ID: 753423
Sample Name:
Payment_copy28476450.exe
Cookbook: default.jbs
Time: 19:53:07
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

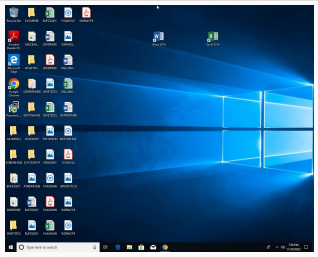
Windows Analysis Report

Payment_copy28476450.exe

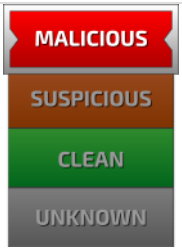
Overview

General Information

Sample Name:	Payment_copy28476450.exe
Analysis ID:	753423
MD5:	70e90926399154.
SHA1:	0eaff8f1cde17a3..
SHA256:	c36de6d07a8ce4..
Tags:	exe loki
Infos:	



Detection



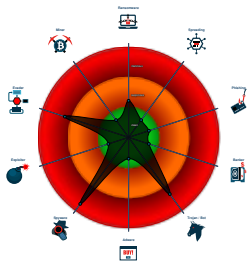
Lokibot

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Yara detected aPLib compressed bi…

Classification



Process Tree

- **System is w10x64**
- Payment_copy28476450.exe (PID: 160 cmdline: C:\Users\user\Desktop\Payment_copy28476450.exe MD5: 70E90926399154C2708801A73CF53D99)
  - wcycejenv.exe (PID: 588 cmdline: "C:\Users\user\AppData\Local\Temp\wcycejenv.exe" C:\Users\user\AppData\Local\Temp\stvrrcrc.d MD5: 3182BEF520A1E9F52BE3755C25E4C3B0)
    - conhost.exe (PID: 584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - wcycejenv.exe (PID: 5332 cmdline: "C:\Users\user\AppData\Local\Temp\wcycejenv.exe" C:\Users\user\AppData\Local\Temp\stvrrcrc.d MD5: 3182BEF520A1E9F52BE3755C25E4C3B0)
- **cleanup**

Malware Configuration

Threatname: Lokibot


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


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword
00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x187f0:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk

Click to see the 24 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.wcycejenv.exe.400000.4.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x18074:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0
3.2.wcycejenv.exe.400000.0.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
3.2.wcycejenv.exe.400000.0.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
3.2.wcycejenv.exe.400000.0.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
3.2.wcycejenv.exe.400000.0.raw.unpack	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword

Click to see the 35 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202

Timestamp:	192.168.2.695.213.216.20249737802025381 11/24/22-19:55:31.199874
SID:	2025381
Source Port:	49737
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249748802021641 11/24/22-19:55:53.130311
SID:	2021641
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249750802825766 11/24/22-19:55:57.329298
SID:	2825766
Source Port:	49750
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249751802021641 11/24/22-19:55:59.376338
SID:	2021641
Source Port:	49751
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:	192.168.2.68.8.8.859881532014169 11/24/22-19:55:09.708351
SID:	2014169
Source Port:	59881
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497332025483 11/24/22-19:55:24.906100
SID:	2025483
Source Port:	80
Destination Port:	49733
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497352025483 11/24/22-19:55:28.867256
SID:	2025483
Source Port:	80
Destination Port:	49735
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249736802024318 11/24/22-19:55:29.163584
SID:	2024318
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497372025483 11/24/22-19:55:32.908191
SID:	2025483
Source Port:	80

Destination Port:	49737
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	−
Timestamp:	95.213.216.202192.168.2.680497392025483 11/24/22-19:55:36.924861
SID:	2025483
Source Port:	80
Destination Port:	49739
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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249754802024318 11/24/22-19:56:04.818902
SID:	2024318
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249736802024313 11/24/22-19:55:29.163584
SID:	2024313
Source Port:	49736
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:	192.168.2.68.8.8.856122532014169 11/24/22-19:54:54.866804
SID:	2014169
Source Port:	56122
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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249754802024313 11/24/22-19:56:04.818902
SID:	2024313
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249711802024313 11/24/22-19:54:38.624655
SID:	2024313
Source Port:	49711
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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249705802021641 11/24/22-19:54:27.228813
SID:	2021641
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249719802025381 11/24/22-19:54:53.033944
SID:	2025381
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249729802825766 11/24/22-19:55:13.852615
SID:	2825766
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249722802025381 11/24/22-19:54:59.769485
SID:	2025381
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249747802825766 11/24/22-19:55:51.131718
SID:	2825766
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249711802024318 11/24/22-19:54:38.624655
SID:	2024318
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249740802025381 11/24/22-19:55:37.776321
SID:	2025381
Source Port:	49740
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249750802025381 11/24/22-19:55:57.329298
SID:	2025381
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249737802825766 11/24/22-19:55:31.199874
SID:	2825766
Source Port:	49737

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

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249714802825766 11/24/22-19:54:45.091814
SID:	2825766
Source Port:	49714
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:	192.168.2.68.8.8.850343532014169 11/24/22-19:55:13.761219
SID:	2014169
Source Port:	50343
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249741802021641 11/24/22-19:55:39.990050
SID:	2021641
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249709802025381 11/24/22-19:54:33.518227
SID:	2025381
Source Port:	49709
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249723802021641 11/24/22-19:55:01.692450
SID:	2021641
Source Port:	49723
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249727802025381 11/24/22-19:55:09.788187
SID:	2025381
Source Port:	49727
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249700802021641 11/24/22-19:54:18.249997
SID:	2021641
Source Port:	49700
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:	192.168.2.68.8.8.856569532014169 11/24/22-19:55:23.105213
SID:	2014169
Source Port:	56569
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249719802825766 11/24/22-19:54:53.033944
SID:	2825766
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249732802825766 11/24/22-19:55:21.169470
SID:	2825766
Source Port:	49732
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:	192.168.2.68.8.8.853943532014169 11/24/22-19:55:03.645658
SID:	2014169
Source Port:	53943
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249755802025381 11/24/22-19:56:06.881877
SID:	2025381
Source Port:	49755
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:	192.168.2.68.8.8.855629532014169 11/24/22-19:55:19.049102
SID:	2014169
Source Port:	55629
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497312025483 11/24/22-19:55:20.867899
SID:	2025483
Source Port:	80
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249755802825766 11/24/22-19:56:06.881877
SID:	2825766
Source Port:	49755

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

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249701802024313 11/24/22-19:54:22.087876
SID:	2024313
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249732802025381 11/24/22-19:55:21.169470
SID:	2025381
Source Port:	49732
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:	192.168.2.68.8.8.860130532014169 11/24/22-19:55:57.225226
SID:	2014169
Source Port:	60130
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249718802024313 11/24/22-19:54:50.807735
SID:	2024313
Source Port:	49718
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249701802024318 11/24/22-19:54:22.087876
SID:	2024318
Source Port:	49701
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249699802024318 11/24/22-19:54:15.956073
SID:	2024318
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497402025483 11/24/22-19:55:39.709470
SID:	2025483
Source Port:	80
Destination Port:	49740
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497422025483 11/24/22-19:55:42.590814
SID:	2025483
Source Port:	80
Destination Port:	49742
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249718802024318 11/24/22-19:54:50.807735
SID:	2024318
Source Port:	49718
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249699802024313 11/24/22-19:54:15.956073
SID:	2024313
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249702802025381 11/24/22-19:54:25.054966
SID:	2025381
Source Port:	49702
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:	192.168.2.68.8.8.861609532014169 11/24/22-19:54:59.613442
SID:	2014169
Source Port:	61609
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497282025483 11/24/22-19:55:13.560423
SID:	2025483
Source Port:	80
Destination Port:	49728
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249710802021641 11/24/22-19:54:35.914327
SID:	2021641
Source Port:	49710
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249716802024318 11/24/22-19:54:48.704817
SID:	2024318
Source Port:	49716

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:	192.168.2.68.8.8.862958532014169 11/24/22-19:55:40.875534
SID:	2014169
Source Port:	62958
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:	192.168.2.68.8.8.864382532014169 11/24/22-19:54:15.835585
SID:	2014169
Source Port:	64382
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249716802024313 11/24/22-19:54:48.704817
SID:	2024313
Source Port:	49716
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249707802021641 11/24/22-19:54:31.276699
SID:	2021641
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249739802825766 11/24/22-19:55:35.259290
SID:	2825766
Source Port:	49739
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497242025483 11/24/22-19:55:05.403255
SID:	2025483
Source Port:	80
Destination Port:	49724
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:	192.168.2.68.8.8.849232532014169 11/24/22-19:55:31.114753
SID:	2014169
Source Port:	49232
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:	192.168.2.68.8.8.862848532014169 11/24/22-19:55:44.925533
SID:	2014169
Source Port:	62848
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249713802021641 11/24/22-19:54:43.021097
SID:	2021641
Source Port:	49713
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249745802825766 11/24/22-19:55:47.082758
SID:	2825766
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249731802024318 11/24/22-19:55:19.158567
SID:	2024318
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249706802825766 11/24/22-19:54:29.062049
SID:	2825766
Source Port:	49706
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249749802024313 11/24/22-19:55:55.139215
SID:	2024313
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249709802825766 11/24/22-19:54:33.518227
SID:	2825766
Source Port:	49709
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249731802024313 11/24/22-19:55:19.158567
SID:	2024313
Source Port:	49731

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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249746802024313 11/24/22-19:55:49.078874
SID:	2024313
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249742802825766 11/24/22-19:55:40.973542
SID:	2825766
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249749802024318 11/24/22-19:55:55.139215
SID:	2024318
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497072025483 11/24/22-19:54:33.040572
SID:	2025483
Source Port:	80
Destination Port:	49707
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249712802825766 11/24/22-19:54:40.926341
SID:	2825766
Source Port:	49712
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249752802024313 11/24/22-19:56:01.434635
SID:	2024313
Source Port:	49752
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249746802024318 11/24/22-19:55:49.078874
SID:	2024318
Source Port:	49746
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249752802024318 11/24/22-19:56:01.434635
SID:	2024318
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249728802021641 11/24/22-19:55:11.780324
SID:	2021641
Source Port:	49728
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249743802021641 11/24/22-19:55:42.875605
SID:	2021641
Source Port:	49743
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249738802024313 11/24/22-19:55:33.192742
SID:	2024313
Source Port:	49738
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:	192.168.2.68.8.8.862910532014169 11/24/22-19:54:44.985895
SID:	2014169
Source Port:	62910
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249724802025381 11/24/22-19:55:03.741584
SID:	2025381
Source Port:	49724
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249738802024318 11/24/22-19:55:33.192742
SID:	2024318
Source Port:	49738
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249740802825766 11/24/22-19:55:37.776321
SID:	2825766
Source Port:	49740

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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249744802024313 11/24/22-19:55:45.028740
SID:	2024313
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249697802825766 11/24/22-19:54:11.348011
SID:	2825766
Source Port:	49697
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:	192.168.2.68.8.8.856331532014169 11/24/22-19:54:31.195563
SID:	2014169
Source Port:	56331
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:	192.168.2.68.8.8.849448532014169 11/24/22-19:54:35.800639
SID:	2014169
Source Port:	49448
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249744802024318 11/24/22-19:55:45.028740
SID:	2024318
Source Port:	49744
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:	192.168.2.68.8.8.856750532014169 11/24/22-19:56:03.361289
SID:	2014169
Source Port:	56750
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:	192.168.2.68.8.8.850506532014169 11/24/22-19:54:33.429766
SID:	2014169
Source Port:	50506
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:	192.168.2.68.8.8.859752532014169 11/24/22-19:55:35.135406
SID:	2014169
Source Port:	59752
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249721802021641 11/24/22-19:54:56.896268
SID:	2021641
Source Port:	49721
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249729802025381 11/24/22-19:55:13.852615
SID:	2025381
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249698802025381 11/24/22-19:54:13.981663
SID:	2025381
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249730802025381 11/24/22-19:55:16.067382
SID:	2025381
Source Port:	49730
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:	192.168.2.68.8.8.862732532014169 11/24/22-19:55:59.286288
SID:	2014169
Source Port:	62732
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:	192.168.2.68.8.8.859336532014169 11/24/22-19:56:04.733170
SID:	2014169
Source Port:	59336
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249734802825766 11/24/22-19:55:25.189583
SID:	2825766
Source Port:	49734

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:	192.168.2.68.8.8.865198532014169 11/24/22-19:54:42.928676
SID:	2014169
Source Port:	65198
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249735802025381 11/24/22-19:55:27.170416
SID:	2025381
Source Port:	49735
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	−
Timestamp:	95.213.216.202192.168.2.680497542025483 11/24/22-19:56:06.628427
SID:	2025483
Source Port:	80
Destination Port:	49754
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249715802021641 11/24/22-19:54:47.405096
SID:	2021641
Source Port:	49715
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	−
Timestamp:	95.213.216.202192.168.2.680497192025483 11/24/22-19:54:54.654090
SID:	2025483
Source Port:	80
Destination Port:	49719
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	−
Timestamp:	95.213.216.202192.168.2.680497522025483 11/24/22-19:56:03.175717
SID:	2025483
Source Port:	80
Destination Port:	49752
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249753802825766 11/24/22-19:56:03.443038
SID:	2825766
Source Port:	49753
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:	192.168.2.68.8.8.851321532014169 11/24/22-19:55:51.025349
SID:	2014169
Source Port:	51321
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249697802025381 11/24/22-19:54:11.348011
SID:	2025381
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249707802825766 11/24/22-19:54:31.276699
SID:	2825766
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249744802825766 11/24/22-19:55:45.028740
SID:	2825766
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249749802025381 11/24/22-19:55:55.139215
SID:	2025381
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497162025483 11/24/22-19:54:50.512832
SID:	2025483
Source Port:	80
Destination Port:	49716
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497142025483 11/24/22-19:54:46.656019
SID:	2025483
Source Port:	80
Destination Port:	49714
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249754802021641 11/24/22-19:56:04.818902
SID:	2021641
Source Port:	49754

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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249705802024318 11/24/22-19:54:27.228813
SID:	2024318
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249710802025381 11/24/22-19:54:35.914327
SID:	2025381
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497112025483 11/24/22-19:54:39.580169
SID:	2025483
Source Port:	80
Destination Port:	49711
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497132025483 11/24/22-19:54:44.610304
SID:	2025483
Source Port:	80
Destination Port:	49713
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249735802825766 11/24/22-19:55:27.170416
SID:	2825766
Source Port:	49735
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249752802025381 11/24/22-19:56:01.434635
SID:	2025381
Source Port:	49752
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:	192.168.2.68.8.8.862766532014169 11/24/22-19:55:55.046216
SID:	2014169
Source Port:	62766
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249705802024313 11/24/22-19:54:27.228813
SID:	2024313
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249710802825766 11/24/22-19:54:35.914327
SID:	2825766
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249707802025381 11/24/22-19:54:31.276699
SID:	2025381
Source Port:	49707
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:	192.168.2.68.8.8.864601532014169 11/24/22-19:54:24.912578
SID:	2014169
Source Port:	64601
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249706802024313 11/24/22-19:54:29.062049
SID:	2024313
Source Port:	49706
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249735802021641 11/24/22-19:55:27.170416
SID:	2021641
Source Port:	49735
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249706802024318 11/24/22-19:54:29.062049
SID:	2024318
Source Port:	49706
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:	192.168.2.68.8.8.852481532014169 11/24/22-19:55:01.607307
SID:	2014169
Source Port:	52481

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

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249726802825766 11/24/22-19:55:07.738200
SID:	2825766
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249754802825766 11/24/22-19:56:04.818902
SID:	2825766
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249733802025381 11/24/22-19:55:23.201569
SID:	2025381
Source Port:	49733
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249753802021641 11/24/22-19:56:03.443038
SID:	2021641
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249724802024313 11/24/22-19:55:03.741584
SID:	2024313
Source Port:	49724
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:	192.168.2.68.8.8.864404532014169 11/24/22-19:55:42.774058
SID:	2014169
Source Port:	64404
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249726802025381 11/24/22-19:55:07.738200
SID:	2025381
Source Port:	49726
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249747802024318 11/24/22-19:55:51.131718
SID:	2024318
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249725802825766 11/24/22-19:55:05.694279
SID:	2825766
Source Port:	49725
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249712802021641 11/24/22-19:54:40.926341
SID:	2021641
Source Port:	49712
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249747802024313 11/24/22-19:55:51.131718
SID:	2024313
Source Port:	49747
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:	192.168.2.68.8.8.852865532014169 11/24/22-19:55:37.629169
SID:	2014169
Source Port:	52865
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497462025483 11/24/22-19:55:50.859980
SID:	2025483
Source Port:	80
Destination Port:	49746
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249699802021641 11/24/22-19:54:15.956073
SID:	2021641
Source Port:	49699
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249724802024318 11/24/22-19:55:03.741584
SID:	2024318
Source Port:	49724

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

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497552025483 11/24/22-19:56:08.689068
SID:	2025483
Source Port:	80
Destination Port:	49755
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249719802021641 11/24/22-19:54:53.033944
SID:	2021641
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497442025483 11/24/22-19:55:46.796463
SID:	2025483
Source Port:	80
Destination Port:	49744
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497272025483 11/24/22-19:55:11.470809
SID:	2025483
Source Port:	80
Destination Port:	49727
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:	192.168.2.68.8.8.863863532014169 11/24/22-19:54:46.995919
SID:	2014169
Source Port:	63863
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249716802021641 11/24/22-19:54:48.704817
SID:	2021641
Source Port:	49716
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249751802025381 11/24/22-19:55:59.376338
SID:	2025381
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249714802025381 11/24/22-19:54:45.091814
SID:	2025381
Source Port:	49714
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249722802021641 11/24/22-19:54:59.769485
SID:	2021641
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497222025483 11/24/22-19:55:01.407205
SID:	2025483
Source Port:	80
Destination Port:	49722
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249720802025381 11/24/22-19:54:54.960633
SID:	2025381
Source Port:	49720
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:	192.168.2.68.8.8.853203532014169 11/24/22-19:54:18.123294
SID:	2014169
Source Port:	53203
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249700802825766 11/24/22-19:54:18.249997
SID:	2825766
Source Port:	49700
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249737802024318 11/24/22-19:55:31.199874
SID:	2024318
Source Port:	49737
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249740802024313 11/24/22-19:55:37.776321
SID:	2024313
Source Port:	49740

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

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249742802025381 11/24/22-19:55:40.973542
SID:	2025381
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	▬
Timestamp:	95.213.216.202192.168.2.680497052025483 11/24/22-19:54:28.634655
SID:	2025483
Source Port:	80
Destination Port:	49705
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249731802021641 11/24/22-19:55:19.158567
SID:	2021641
Source Port:	49731
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:	192.168.2.68.8.8.857686532014169 11/24/22-19:54:13.553924
SID:	2014169
Source Port:	57686
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:	192.168.2.68.8.8.858595532014169 11/24/22-19:54:28.961973
SID:	2014169
Source Port:	58595
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249736802025381 11/24/22-19:55:29.163584
SID:	2025381
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249745802025381 11/24/22-19:55:47.082758
SID:	2025381
Source Port:	49745
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:	192.168.2.68.8.8.857515532014169 11/24/22-19:55:48.986225
SID:	2014169
Source Port:	57515
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249734802024318 11/24/22-19:55:25.189583
SID:	2024318
Source Port:	49734
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497002025483 11/24/22-19:54:20.029122
SID:	2025483
Source Port:	80
Destination Port:	49700
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249725802021641 11/24/22-19:55:05.694279
SID:	2021641
Source Port:	49725
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249734802024313 11/24/22-19:55:25.189583
SID:	2024313
Source Port:	49734
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249743802024318 11/24/22-19:55:42.875605
SID:	2024318
Source Port:	49743
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249728802024318 11/24/22-19:55:11.780324
SID:	2024318
Source Port:	49728
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249737802024313 11/24/22-19:55:31.199874
SID:	2024313
Source Port:	49737

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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249728802024313 11/24/22-19:55:11.780324
SID:	2024313
Source Port:	49728
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249739802025381 11/24/22-19:55:35.259290
SID:	2025381
Source Port:	49739
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:	192.168.2.68.8.8.855956532014169 11/24/22-19:55:46.990731
SID:	2014169
Source Port:	55956
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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249743802024313 11/24/22-19:55:42.875605
SID:	2024313
Source Port:	49743
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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249709802024313 11/24/22-19:54:33.518227
SID:	2024313
Source Port:	49709
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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249738802021641 11/24/22-19:55:33.192742
SID:	2021641
Source Port:	49738
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:	192.168.2.68.8.8.859082532014169 11/24/22-19:54:38.013432
SID:	2014169
Source Port:	59082
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249740802024318 11/24/22-19:55:37.776321
SID:	2024318
Source Port:	49740
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249722802825766 11/24/22-19:54:59.769485
SID:	2825766
Source Port:	49722
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:	192.168.2.68.8.8.851530532014169 11/24/22-19:54:52.685795
SID:	2014169
Source Port:	51530
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249701802025381 11/24/22-19:54:22.087876
SID:	2025381
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249723802025381 11/24/22-19:55:01.692450
SID:	2025381
Source Port:	49723
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249721802024313 11/24/22-19:54:56.896268
SID:	2024313
Source Port:	49721
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249750802021641 11/24/22-19:55:57.329298
SID:	2021641
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249715802024318 11/24/22-19:54:47.405096
SID:	2024318
Source Port:	49715

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

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	−
Timestamp:	95.213.216.202192.168.2.680497302025483 11/24/22-19:55:17.735946
SID:	2025483
Source Port:	80
Destination Port:	49730
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249716802825766 11/24/22-19:54:48.704817
SID:	2825766
Source Port:	49716
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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249721802024318 11/24/22-19:54:56.896268
SID:	2024318
Source Port:	49721
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:	192.168.2.68.8.8.860032532014169 11/24/22-19:55:29.068969
SID:	2014169
Source Port:	60032
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249744802021641 11/24/22-19:55:45.028740
SID:	2021641
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	−
Timestamp:	95.213.216.202192.168.2.680497412025483 11/24/22-19:55:40.700457
SID:	2025483
Source Port:	80
Destination Port:	49741
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	−
Timestamp:	95.213.216.202192.168.2.680497492025483 11/24/22-19:55:57.050677
SID:	2025483
Source Port:	80
Destination Port:	49749
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249709802024318 11/24/22-19:54:33.518227
SID:	2024318
Source Port:	49709
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249715802024313 11/24/22-19:54:47.405096
SID:	2024313
Source Port:	49715
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:	192.168.2.68.8.8.858917532014169 11/24/22-19:55:11.700175
SID:	2014169
Source Port:	58917
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249745802024318 11/24/22-19:55:47.082758
SID:	2024318
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497342025483 11/24/22-19:55:26.886961
SID:	2025483
Source Port:	80
Destination Port:	49734
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249742802021641 11/24/22-19:55:40.973542
SID:	2021641
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497362025483 11/24/22-19:55:30.902353
SID:	2025483
Source Port:	80
Destination Port:	49736
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497382025483 11/24/22-19:55:34.897313
SID:	2025483
Source Port:	80

Destination Port:	49738
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	−
Timestamp:	95.213.216.202192.168.2.680497322025483 11/24/22-19:55:22.836179
SID:	2025483
Source Port:	80
Destination Port:	49732
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249739802021641 11/24/22-19:55:35.259290
SID:	2021641
Source Port:	49739
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249741802825766 11/24/22-19:55:39.990050
SID:	2825766
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249728802025381 11/24/22-19:55:11.780324
SID:	2025381
Source Port:	49728
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: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249745802024313 11/24/22-19:55:47.082758
SID:	2024313
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249713802825766 11/24/22-19:54:43.021097
SID:	2825766
Source Port:	49713
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	−
Timestamp:	192.168.2.695.213.216.20249746802025381 11/24/22-19:55:49.078874
SID:	2025381
Source Port:	49746
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:	192.168.2.68.8.8.853731532014169 11/24/22-19:54:11.254500
SID:	2014169
Source Port:	53731
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249702802024318 11/24/22-19:54:25.054966
SID:	2024318
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249713802025381 11/24/22-19:54:43.021097
SID:	2025381
Source Port:	49713
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249738802825766 11/24/22-19:55:33.192742
SID:	2825766
Source Port:	49738
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:	192.168.2.68.8.8.861089532014169 11/24/22-19:55:53.045222
SID:	2014169
Source Port:	61089
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249714802021641 11/24/22-19:54:45.091814
SID:	2021641
Source Port:	49714
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249720802024313 11/24/22-19:54:54.960633
SID:	2024313
Source Port:	49720
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249702802024313 11/24/22-19:54:25.054966
SID:	2024313
Source Port:	49702

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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249720802024318 11/24/22-19:54:54.960633
SID:	2024318
Source Port:	49720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249731802025381 11/24/22-19:55:19.158567
SID:	2025381
Source Port:	49731
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249735802024313 11/24/22-19:55:27.170416
SID:	2024313
Source Port:	49735
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249698802024317 11/24/22-19:54:13.981663
SID:	2024317
Source Port:	49698
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249698802024312 11/24/22-19:54:13.981663
SID:	2024312
Source Port:	49698
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249729802021641 11/24/22-19:55:13.852615
SID:	2021641
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249721802025381 11/24/22-19:54:56.896268
SID:	2025381
Source Port:	49721
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249731802825766 11/24/22-19:55:19.158567
SID:	2825766
Source Port:	49731
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249712802024313 11/24/22-19:54:40.926341
SID:	2024313
Source Port:	49712
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249712802024318 11/24/22-19:54:40.926341
SID:	2024318
Source Port:	49712
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249735802024318 11/24/22-19:55:27.170416
SID:	2024318
Source Port:	49735
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249724802021641 11/24/22-19:55:03.741584
SID:	2021641
Source Port:	49724
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249748802825766 11/24/22-19:55:53.130311
SID:	2825766
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249753802024318 11/24/22-19:56:03.443038
SID:	2024318
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249753802024313 11/24/22-19:56:03.443038
SID:	2024313
Source Port:	49753

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

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249730802024318 11/24/22-19:55:16.067382
SID:	2024318
Source Port:	49730
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249747802021641 11/24/22-19:55:51.131718
SID:	2021641
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249738802025381 11/24/22-19:55:33.192742
SID:	2025381
Source Port:	49738
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249730802024313 11/24/22-19:55:16.067382
SID:	2024313
Source Port:	49730
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249706802021641 11/24/22-19:54:29.062049
SID:	2021641
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249705802025381 11/24/22-19:54:27.228813
SID:	2025381
Source Port:	49705
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:	192.168.2.68.8.8.863229532014169 11/24/22-19:54:48.619009
SID:	2014169
Source Port:	63229
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249721802825766 11/24/22-19:54:56.896268
SID:	2825766
Source Port:	49721
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249722802024313 11/24/22-19:54:59.769485
SID:	2024313
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497432025483 11/24/22-19:55:44.744520
SID:	2025483
Source Port:	80
Destination Port:	49743
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:	192.168.2.68.8.8.849786532014169 11/24/22-19:54:27.135932
SID:	2014169
Source Port:	49786
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249725802024313 11/24/22-19:55:05.694279
SID:	2024313
Source Port:	49725
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249719802024318 11/24/22-19:54:53.033944
SID:	2024318
Source Port:	49719
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249722802024318 11/24/22-19:54:59.769485
SID:	2024318
Source Port:	49722
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249725802024318 11/24/22-19:55:05.694279
SID:	2024318
Source Port:	49725

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:	192.168.2.68.8.8.856123532014169 11/24/22-19:55:33.111651
SID:	2014169
Source Port:	56123
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249697802021641 11/24/22-19:54:11.348011
SID:	2021641
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249711802025381 11/24/22-19:54:38.624655
SID:	2025381
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249736802825766 11/24/22-19:55:29.163584
SID:	2825766
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497292025483 11/24/22-19:55:15.362841
SID:	2025483
Source Port:	80
Destination Port:	49729
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497252025483 11/24/22-19:55:07.447890
SID:	2025483
Source Port:	80
Destination Port:	49725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497212025483 11/24/22-19:54:58.247548
SID:	2025483
Source Port:	80
Destination Port:	49721
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249750802024318 11/24/22-19:55:57.329298
SID:	2024318
Source Port:	49750
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249737802021641 11/24/22-19:55:31.199874
SID:	2021641
Source Port:	49737
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249751802825766 11/24/22-19:55:59.376338
SID:	2825766
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249740802021641 11/24/22-19:55:37.776321
SID:	2021641
Source Port:	49740
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497022025483 11/24/22-19:54:26.773719
SID:	2025483
Source Port:	80
Destination Port:	49702
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497062025483 11/24/22-19:54:30.867234
SID:	2025483
Source Port:	80
Destination Port:	49706
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249754802025381 11/24/22-19:56:04.818902
SID:	2025381
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249699802825766 11/24/22-19:54:15.956073
SID:	2825766
Source Port:	49699

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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249719802024313 11/24/22-19:54:53.033944
SID:	2024313
Source Port:	49719
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249734802021641 11/24/22-19:55:25.189583
SID:	2021641
Source Port:	49734
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249748802025381 11/24/22-19:55:53.130311
SID:	2025381
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249715802825766 11/24/22-19:54:47.405096
SID:	2825766
Source Port:	49715
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249732802021641 11/24/22-19:55:21.169470
SID:	2021641
Source Port:	49732
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249709802021641 11/24/22-19:54:33.518227
SID:	2021641
Source Port:	49709
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249755802024318 11/24/22-19:56:06.881877
SID:	2024318
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249741802025381 11/24/22-19:55:39.990050
SID:	2025381
Source Port:	49741
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249755802024313 11/24/22-19:56:06.881877
SID:	2024313
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249723802825766 11/24/22-19:55:01.692450
SID:	2825766
Source Port:	49723
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:	192.168.2.68.8.8.865044532014169 11/24/22-19:55:27.077654
SID:	2014169
Source Port:	65044
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249726802021641 11/24/22-19:55:07.738200
SID:	2021641
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249718802025381 11/24/22-19:54:50.807735
SID:	2025381
Source Port:	49718
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249727802024313 11/24/22-19:55:09.788187
SID:	2024313
Source Port:	49727
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249750802024313 11/24/22-19:55:57.329298
SID:	2024313
Source Port:	49750

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

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249727802024318 11/24/22-19:55:09.788187
SID:	2024318
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249700802025381 11/24/22-19:54:18.249997
SID:	2025381
Source Port:	49700
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249733802024313 11/24/22-19:55:23.201569
SID:	2024313
Source Port:	49733
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497472025483 11/24/22-19:55:52.860690
SID:	2025483
Source Port:	80
Destination Port:	49747
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:	192.168.2.68.8.8.856086532014169 11/24/22-19:55:05.605111
SID:	2014169
Source Port:	56086
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249728802825766 11/24/22-19:55:11.780324
SID:	2825766
Source Port:	49728
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249733802024318 11/24/22-19:55:23.201569
SID:	2024318
Source Port:	49733
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497502025483 11/24/22-19:55:59.104900
SID:	2025483
Source Port:	80
Destination Port:	49750
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249734802025381 11/24/22-19:55:25.189583
SID:	2025381
Source Port:	49734
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249742802024318 11/24/22-19:55:40.973542
SID:	2024318
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497532025483 11/24/22-19:56:04.545301
SID:	2025483
Source Port:	80
Destination Port:	49753
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497182025483 11/24/22-19:54:52.477982
SID:	2025483
Source Port:	80
Destination Port:	49718
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249751802024313 11/24/22-19:55:59.376338
SID:	2024313
Source Port:	49751
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:	192.168.2.68.8.8.860690532014169 11/24/22-19:56:01.353337
SID:	2014169
Source Port:	60690
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249748802024313 11/24/22-19:55:53.130311
SID:	2024313
Source Port:	49748

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

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249701802825766 11/24/22-19:54:22.087876
SID:	2825766
Source Port:	49701
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:	192.168.2.68.8.8.854903532014169 11/24/22-19:54:50.721248
SID:	2014169
Source Port:	54903
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249743802025381 11/24/22-19:55:42.875605
SID:	2025381
Source Port:	49743
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249742802024313 11/24/22-19:55:40.973542
SID:	2024313
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497152025483 11/24/22-19:54:48.216785
SID:	2025483
Source Port:	80
Destination Port:	49715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249736802021641 11/24/22-19:55:29.163584
SID:	2021641
Source Port:	49736
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249739802024313 11/24/22-19:55:35.259290
SID:	2024313
Source Port:	49739
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249739802024318 11/24/22-19:55:35.259290
SID:	2024318
Source Port:	49739
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249745802021641 11/24/22-19:55:47.082758
SID:	2021641
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249748802024318 11/24/22-19:55:53.130311
SID:	2024318
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680496992025483 11/24/22-19:54:17.569674
SID:	2025483
Source Port:	80
Destination Port:	49699
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497102025483 11/24/22-19:54:37.501776
SID:	2025483
Source Port:	80
Destination Port:	49710
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497122025483 11/24/22-19:54:42.610242
SID:	2025483
Source Port:	80
Destination Port:	49712
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:	192.168.2.68.8.8.856547532014169 11/24/22-19:55:07.655761
SID:	2014169
Source Port:	56547
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249714802024313 11/24/22-19:54:45.091814
SID:	2024313
Source Port:	49714

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: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249720802021641 11/24/22-19:54:54.960633
SID:	2021641
Source Port:	49720
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: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249714802024318 11/24/22-19:54:45.091814
SID:	2024318
Source Port:	49714
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249725802025381 11/24/22-19:55:05.694279
SID:	2025381
Source Port:	49725
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: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249702802021641 11/24/22-19:54:25.054966
SID:	2021641
Source Port:	49702
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: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249711802021641 11/24/22-19:54:38.624655
SID:	2021641
Source Port:	49711
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:	192.168.2.68.8.8.859504532014169 11/24/22-19:54:40.838615
SID:	2014169
Source Port:	59504
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	▬
Timestamp:	192.168.2.695.213.216.20249716802025381 11/24/22-19:54:48.704817
SID:	2025381
Source Port:	49716
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249698802021641 11/24/22-19:54:13.981663
SID:	2021641
Source Port:	49698
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249729802024318 11/24/22-19:55:13.852615
SID:	2024318
Source Port:	49729
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249700802024318 11/24/22-19:54:18.249997
SID:	2024318
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249715802025381 11/24/22-19:54:47.405096
SID:	2025381
Source Port:	49715
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249723802024318 11/24/22-19:55:01.692450
SID:	2024318
Source Port:	49723
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249729802024313 11/24/22-19:55:13.852615
SID:	2024313
Source Port:	49729
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249723802024313 11/24/22-19:55:01.692450
SID:	2024313
Source Port:	49723
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:	192.168.2.68.8.8.852556532014169 11/24/22-19:54:56.722023
SID:	2014169
Source Port:	52556

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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249741802024318 11/24/22-19:55:39.990050
SID:	2024318
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249749802825766 11/24/22-19:55:55.139215
SID:	2825766
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249741802024313 11/24/22-19:55:39.990050
SID:	2024313
Source Port:	49741
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249700802024313 11/24/22-19:54:18.249997
SID:	2024313
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497202025483 11/24/22-19:54:56.488535
SID:	2025483
Source Port:	80
Destination Port:	49720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249718802021641 11/24/22-19:54:50.807735
SID:	2021641
Source Port:	49718
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249701802021641 11/24/22-19:54:22.087876
SID:	2021641
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497482025483 11/24/22-19:55:54.888388
SID:	2025483
Source Port:	80
Destination Port:	49748
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249720802825766 11/24/22-19:54:54.960633
SID:	2825766
Source Port:	49720
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:	192.168.2.68.8.8.853107532014169 11/24/22-19:54:21.991089
SID:	2014169
Source Port:	53107
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249702802825766 11/24/22-19:54:25.054966
SID:	2825766
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249744802025381 11/24/22-19:55:45.028740
SID:	2025381
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497512025483 11/24/22-19:56:01.147373
SID:	2025483
Source Port:	80
Destination Port:	49751
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249730802021641 11/24/22-19:55:16.067382
SID:	2021641
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249743802825766 11/24/22-19:55:42.875605
SID:	2825766
Source Port:	49743

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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249710802024318 11/24/22-19:54:35.914327
SID:	2024318
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249724802825766 11/24/22-19:55:03.741584
SID:	2825766
Source Port:	49724
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249727802825766 11/24/22-19:55:09.788187
SID:	2825766
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497452025483 11/24/22-19:55:48.824554
SID:	2025483
Source Port:	80
Destination Port:	49745
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249713802024318 11/24/22-19:54:43.021097
SID:	2024318
Source Port:	49713
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249710802024313 11/24/22-19:54:35.914327
SID:	2024313
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249718802825766 11/24/22-19:54:50.807735
SID:	2825766
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497092025483 11/24/22-19:54:35.412652
SID:	2025483
Source Port:	80
Destination Port:	49709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497232025483 11/24/22-19:55:03.460307
SID:	2025483
Source Port:	80
Destination Port:	49723
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249697802024312 11/24/22-19:54:11.348011
SID:	2024312
Source Port:	49697
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249707802024313 11/24/22-19:54:31.276699
SID:	2024313
Source Port:	49707
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:	192.168.2.68.8.8.862520532014169 11/24/22-19:55:15.969759
SID:	2014169
Source Port:	62520
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:	192.168.2.68.8.8.857322532014169 11/24/22-19:55:39.901358
SID:	2014169
Source Port:	57322
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249713802024313 11/24/22-19:54:43.021097
SID:	2024313
Source Port:	49713
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249697802024317 11/24/22-19:54:11.348011
SID:	2024317
Source Port:	49697

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

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497262025483 11/24/22-19:55:09.535230
SID:	2025483
Source Port:	80
Destination Port:	49726
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249707802024318 11/24/22-19:54:31.276699
SID:	2024318
Source Port:	49707
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249746802021641 11/24/22-19:55:49.078874
SID:	2021641
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 95.213.216.202 - Destination IP: 192.168.2.6	
Timestamp:	95.213.216.202192.168.2.680497012025483 11/24/22-19:54:23.783923
SID:	2025483
Source Port:	80
Destination Port:	49701
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249733802825766 11/24/22-19:55:23.201569
SID:	2825766
Source Port:	49733
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249752802021641 11/24/22-19:56:01.434635
SID:	2021641
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249730802825766 11/24/22-19:55:16.067382
SID:	2825766
Source Port:	49730
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249732802024313 11/24/22-19:55:21.169470
SID:	2024313
Source Port:	49732
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249726802024318 11/24/22-19:55:07.738200
SID:	2024318
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249753802025381 11/24/22-19:56:03.443038
SID:	2025381
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249732802024318 11/24/22-19:55:21.169470
SID:	2024318
Source Port:	49732
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249705802825766 11/24/22-19:54:27.228813
SID:	2825766
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249746802825766 11/24/22-19:55:49.078874
SID:	2825766
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249755802021641 11/24/22-19:56:06.881877
SID:	2021641
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249747802025381 11/24/22-19:55:51.131718
SID:	2025381
Source Port:	49747

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

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249699802025381 11/24/22-19:54:15.956073
SID:	2025381
Source Port:	49699
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249726802024313 11/24/22-19:55:07.738200
SID:	2024313
Source Port:	49726
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249749802021641 11/24/22-19:55:55.139215
SID:	2021641
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249698802825766 11/24/22-19:54:13.981663
SID:	2825766
Source Port:	49698
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249727802021641 11/24/22-19:55:09.788187
SID:	2021641
Source Port:	49727
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:	192.168.2.68.8.8.852715532014169 11/24/22-19:56:06.802187
SID:	2014169
Source Port:	52715
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:	192.168.2.68.8.8.852079532014169 11/24/22-19:55:21.075805
SID:	2014169
Source Port:	52079
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:	192.168.2.68.8.8.861833532014169 11/24/22-19:55:25.100624
SID:	2014169
Source Port:	61833
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249706802025381 11/24/22-19:54:29.062049
SID:	2025381
Source Port:	49706
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249733802021641 11/24/22-19:55:23.201569
SID:	2021641
Source Port:	49733
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: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249751802024318 11/24/22-19:55:59.376338
SID:	2024318
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249752802825766 11/24/22-19:56:01.434635
SID:	2825766
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249712802025381 11/24/22-19:54:40.926341
SID:	2025381
Source Port:	49712
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 95.213.216.202	
Timestamp:	192.168.2.695.213.216.20249711802825766 11/24/22-19:54:38.624655
SID:	2825766
Source Port:	49711
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

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Yara detected aPLib compressed binary

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

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)

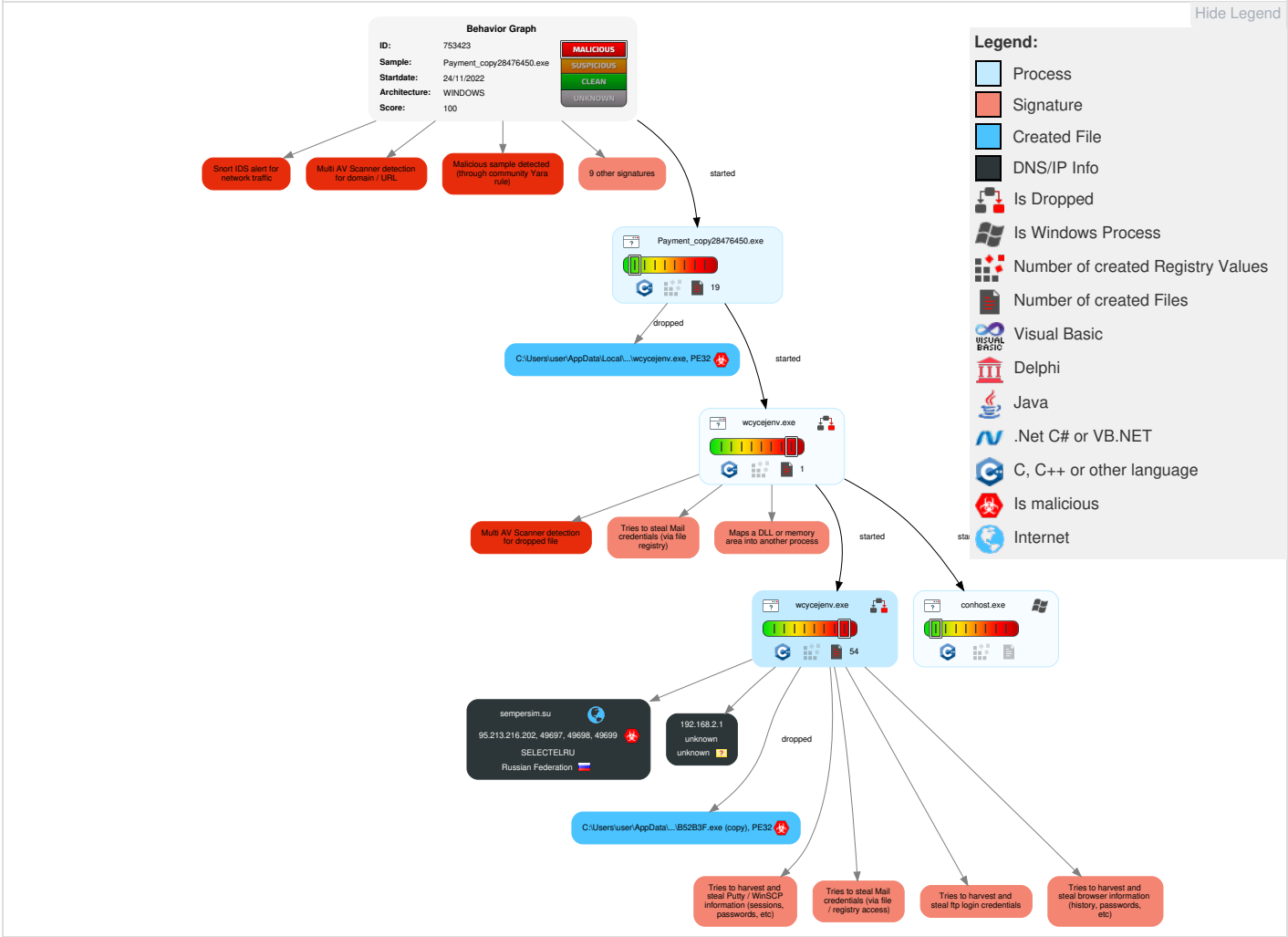
Tries to harvest and steal browser information (history, passwords, etc)

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 Masquerading	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	2 Credentials in Registry	1 2 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Account Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Owner/User 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 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	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	Compile After Delivery	DCSync	2 File and Directory 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	Indicator Removal from Tools	Proc Filesystem	2 6 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

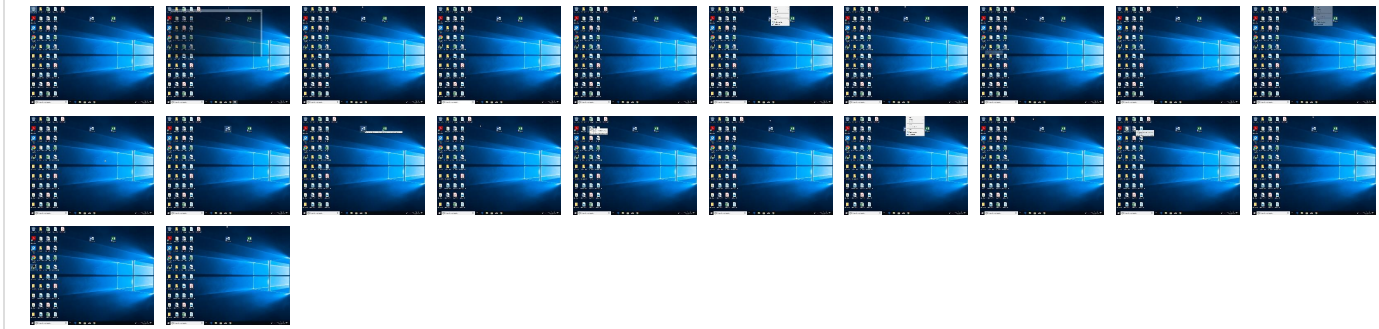
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Payment_copy28476450.exe	35%	ReversingLabs	Win32.Trojan.FormBook	
Payment_copy28476450.exe	42%	Virustotal		Browse
Payment_copy28476450.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\wcycejenv.exe	50%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\wcycejenv.exe	23%	Virustotal		Browse
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe (copy)	50%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe (copy)	23%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.wcycejenv.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.Payment_copy28476450.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
1.2.wcycejenv.exe.610000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Payment_copy28476450.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

Source	Detection	Scanner	Label	Link
sempersim.su	25%	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/gl20/fre.php	100%	Avira URL Cloud	malware	
http://sempersim.su/gl20/fre.php	26%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sempersim.su	95.213.216.202	true	true	• 25%, Virustotal, Browse	unknown

Contacted URLs

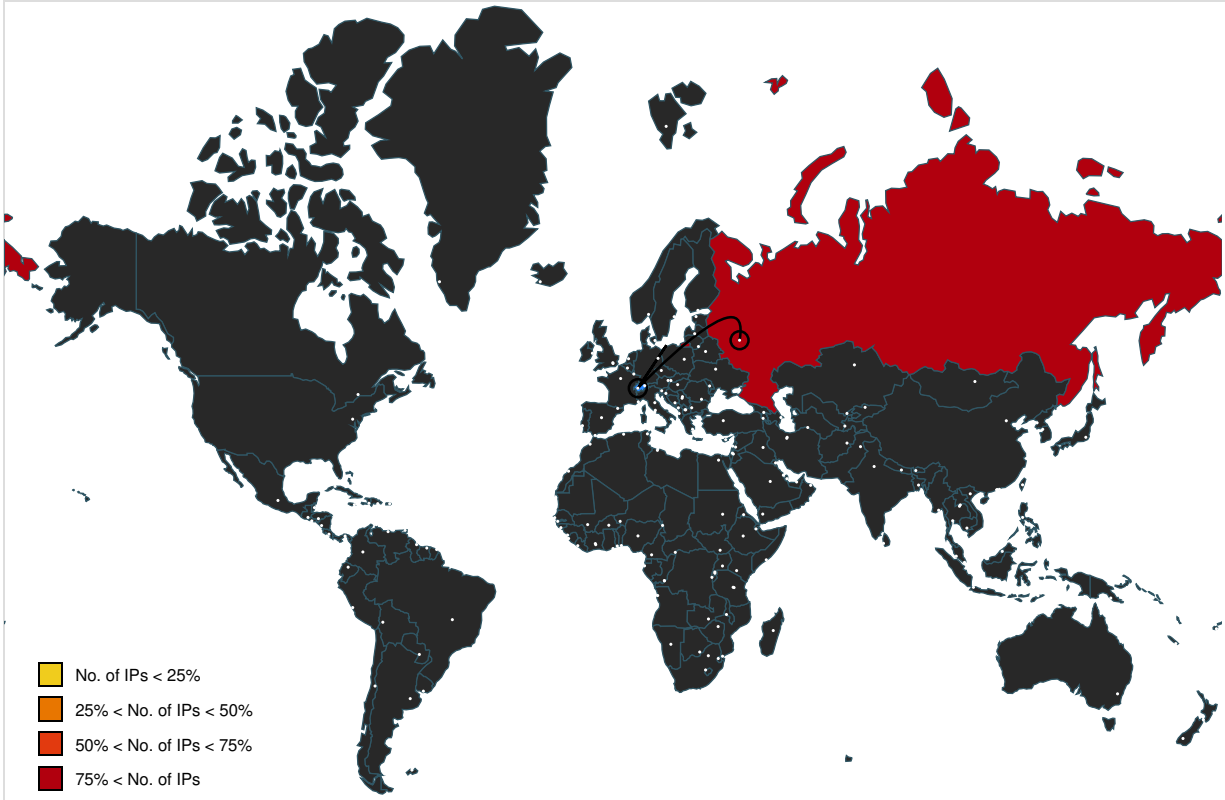
Name	Malicious	Antivirus Detection	Reputation
http://sempersim.su/gl20/fre.php	true	• 26%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	Payment_copy28476450.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Payment_copy28476450.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ibsensoftware.com/	wcycejenv.exe, wcycejenv.exe, 00000003.0 0000000.253960864.0000000000400000.00000 040.80000000.00040000.00000000.sdmp, wcy cejenv.exe, 00000003.00000002.510096240. 0000000000400000.00000040.80000000.00040 000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.213.216.202	sempersim.su	Russian Federation		49505	SELECTELRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753423
Start date and time:	2022-11-24 19:53:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment_copy28476450.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/7@55/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.6% (good quality ratio 96%) • Quality average: 86.2% • Quality standard deviation: 25%
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:54:17	API Interceptor	52x Sleep call for process: wcycejenv.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\Temp\nsg6B4D.tmp	
Process:	C:\Users\user\Desktop\Payment_copy28476450.exe
File Type:	data
Category:	dropped
Size (bytes):	459450
Entropy (8bit):	7.057848521690541
Encrypted:	false
SSDEEP:	12288:JxcTxTkKZ9roe9deAwRxFMCgRlXXLRLh7mgb1xuuu9toBdmqQGMZRUuJ5:ATxTkQEweAwbqD7vb1xuuu9Edmdl
MD5:	DAEA903CE6FBB92BF4BE14AEC7489613
SHA1:	21872C93628D5B4715A9876332090C3D0EE03E66
SHA-256:	97CE6EB441A34EBEE7864B4B0E99939D7D773AC7FC416B27F1F72413061944B3
SHA-512:	9D6B3DAEC38C534A73F91BD26D71D77E3FAD8A21CED7817D9A9CDC5F991503AE348B728D6D9E1257D2D85B9137D33E59D2592EE1E9CABD920BB64FFE8F88D 3D5
Malicious:	false
Reputation:	low
Preview:	.....,.....N...d..... .....J.....Y...j.....I..... ....

C:\Users\user\AppData\Local\Temp\ntwcyphb.r	
Process:	C:\Users\user\Desktop\Payment_copy28476450.exe
File Type:	data
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	7.955523846750811
Encrypted:	false
SSDEEP:	3072:wjajJkiH9OPjfkivvicRevZjOqhaMltCzjriqZTa5apaaaaaaaaaaaaaaaaaaaal:Q7fk2evZCqhadZqZ1
MD5:	B12381A247D8454C152B69D13B35EC05
SHA1:	347BDD9D8F6E96C6912DC56198BD5038969C41AC
SHA-256:	1B9C40C7751E34B3A3DD0658B3F1DAC5AA39D85D50D3F02CDAA555220228193E
SHA-512:	AD79AC16823D14CD07EF1C74C2933B3D1FB15D4C1F22416FCBC0F25E6C087E8C5F3BBD63E393D9B07DCAD185A51D3457F818C56B95CAD074365D8B2CA11D6 D8
Malicious:	false
Reputation:	low
Preview:	....{T(...|Y*..<.(ak.5....C..."... .I4.....~.....-..xN..z.....B.....3O....'...U6..0%.]*..9.[QPN.....{..u!...G.....P..WX...{.Z~.Fr.....>Zx.....[6... ?q.e.4..d.k....X.1..F....."u.U..(v.....!.jy~ ...Z.h...+...M.....d.F...x.]@6jc#.b.c..-T.....Y1y.<...ak.5.....C...".1. .Q4....@~.Z.....-..x..4z.....Be.K.D...N...`c.u..x.v.n....Y..9u.9..xub.{c.s..R.....cL.....G.z..w..\1^.....|...g.. d.q...5-.....M(:.....M.B....xj.z.....X.p....3....II..x..QH..U-.....B..x....\>c..b.c...T(...|Y.h.\.V...5..U..C..."6.. ..4.....~.....-p{.}N;z.I..Bn.K.B...}M|..Ic....x.....{..z.9u...xu....,s..:..... .QcL.....G.z..w..\1^.....|...g..d.q...5-.....M(:.....M.B....xj.:.N..X.p....3....II..x..QH.....F.xD..{.>c#.b.c...T(...|Y1h.<.(ak.5.~...C..."... .I4.....~.....-..xN.4z.....B..K.D...N|..Ic....x ...n....Y..z.9u.9..xub...,s.R.....cL.....G.z..w..\1^.....|...g..d.q...5-.....M(:.....M.B....xj.:.N..X.p....3....II..x..QH

C:\Users\user\AppData\Local\Temp\stvrrcrc.d	
Process:	C:\Users\user\Desktop\Payment_copy28476450.exe
File Type:	data
Category:	dropped
Size (bytes):	5655
Entropy (8bit):	6.234833362351721
Encrypted:	false
SSDEEP:	96:4HXF/taUEVYCVmNFHILHl95DTMQUTPENeG2O3VyKbaj9XPIP:w1/tNECRKZTtkG2W8fP
MD5:	8C23AB33C072F31910D8126FE29420D7
SHA1:	19752AC35C502F4CD5BB55D3DB4ACE8FD00C0767
SHA-256:	0C6033793464A7C0D79F2A402CC4DCF821B8C633371B4D676BA18F21FCB3376F
SHA-512:	612E97ABC1D02F74E9334D2D37A0193C974D6BEFB86E3A578AC2BE71AA6B56331F3F24F69EC9953B525AAD39EFE6376563C8BDAFAA552A936582613BDBCC70 99
Malicious:	false
Reputation:	low
Preview:	.*.<<`.,<<<.|..|..<.<.|.K...`.,<<<<...|..t....q..~,.=<<..pr.>c.q.;....$...J.<.....q...+<<...2M.....sD.W.M..F.J..q....J.<....`.,<<<.|..|..<.<.|.d.X.....<<<<..p.....R..L.T..+..EK;.EK.....p....Zp...y ...p..L.:.....=q....J.<.....y.;...8..4t.O..\..._.. .g.|..W.....p...O.....c..p.....cq.z.;....EJ.<.....l...O.....`.,<<<.|..|..<.<.|.dp.^...q....y..T.....[.q....[c.qR.a.<..[..p.....O.....4....JR.....\.. ..J.nc2...R.....\.LncV.K..Lnc_q..y.....O...y.....cT...z.;..;.|...EJ.<.....q...+<<...2M.....~.sD.W.M..F.J..q....J.<....<<O..=<<<.....HN..cN..)N..N..zN..{.aT<.a.<Rv.n...Rp.n...R. .n...Rk.n...Ru.n...Rl.n...Rd.n...Rj.n...R6.n...Rz.n..J;.n..@.....dn.^..q.....d+>..q.....d.z...q..r.....dY....q.."....d|...q.....d..^..q.....d.....q..2.....dt....q.....;.|S.<N...;.|..<N ...;.|M.N...);.|S..N....;.|...N...}..T..H.a.<....|....y..{ ...;ZR.....H.....;D.....W;.|S.<.....;E}SE<....c.qn;.|..<.....;E}..<....c.q.;.|M.....;E}M.....

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

Process:	C:\Users\user\Desktop\Payment_copy28476450.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	340992
Entropy (8bit):	6.549726242729774
Encrypted:	false
SSDEEP:	6144:Qoe9deNmwPG6xFMCgRlXXLRLh7mzMb1iRWuuu9toDVdmqQL17EMRvM/gRUuJ5dX:Qoe9deAwRxFMCgRlXXLRLh7mgb1xuuuz
MD5:	3182BEF520A1E9F52BE3755C25E4C3B0
SHA1:	1829DD90A63BF67DCEB3F6CC41C8AACE8E7E31AD
SHA-256:	E7ECA366A9467420BA42645AAC451E02D0F009C6F6DFE3A47349510DE0BBFB96
SHA-512:	BDC8E908D5BCDD52CCF880D11D863D76EE28D9201C51972CD547E94887E32BA986329D5C7615FBB1F01E8E2AF5123E419A411DFAADD8B9B5A2D8E586C947E62
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50% • Antivirus: Virustotal, Detection: 23%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.).-.G.-.G.-.G.v.D.'.G.v.B...G.v.C.?.G...../.G...B...G...C.>.G...D.8.G.v.F.4.G.-.F...G...C.,.G.....,.G...E.,.G.Rich-.G.....PE..L.....~c.....!.x.....z.....@.....P.....D.....@.....0...@.....text....v.....x..... ..`.rdata.....|.....@..@.data.....0.....@....rsrc.....@.....2.....@..@.....

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\wcycejenv.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	340992
Entropy (8bit):	6.549726242729774
Encrypted:	false
SSDEEP:	6144:Qoe9deNmwPG6xFMCgRlXXLRLh7mzMb1iRWuuu9toDVdmqQL17EMRvM/gRUuJ5dX:Qoe9deAwRxFMCgRlXXLRLh7mgb1xuuuz
MD5:	3182BEF520A1E9F52BE3755C25E4C3B0
SHA1:	1829DD90A63BF67DCEB3F6CC41C8AACE8E7E31AD
SHA-256:	E7ECA366A9467420BA42645AAC451E02D0F009C6F6DFE3A47349510DE0BBFB96
SHA-512:	BDC8E908D5BCDD52CCF880D11D863D76EE28D9201C51972CD547E94887E32BA986329D5C7615FBB1F01E8E2AF5123E419A411DFAADD8B9B5A2D8E586C947E62
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50% • Antivirus: Virustotal, Detection: 23%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.).-.G.-.G.-.G.v.D.'.G.v.B...G.v.C.?.G...../.G...B...G...C.>.G...D.8.G.v.F.4.G.-.F...G...C.,.G.....,.G...E.,.G.Rich-.G.....PE..L.....~c.....!.x.....z.....@.....P.....D.....@.....0...@.....text....v.....x..... ..`.rdata.....|.....@..@.data.....0.....@....rsrc.....@.....2.....@..@.....

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

Process:	C:\Users\user\AppData\Local\Temp\wcycejenv.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:\Users\user\AppData\Local\Temp\wcycejenv.exe
File Type:	data
Category:	dropped
Size (bytes):	49
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	884BB48A55DA67B4812805CB8905277D
SHA1:	6B3D33E00F5B9DEAE2826F80644CB4F6E78B7401
SHA-256:	78877FA898F0B4C45C9C33AE941E40617AD7C8657A307DB62BC5691F92F4F60E
SHA-512:	989A38778FC961EB2C79E70621EABFB4B22D6537F08A71359B27AF495646E304EE252A523769F66B75BC2FAF546ACB22A71B358B51221174AC0D964DA7A62821
Malicious:	false
Preview:	.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.918853891717431
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Payment_copy28476450.exe
File size:	247655
MD5:	70e90926399154c2708801a73cf53d99
SHA1:	0eaff8f1cde17a392d9e7935bae96f21c91acc3c
SHA256:	c36de6d07a8ce4407cb59a275dbf8c04d05844903bb6d566f295ccd13a2d4ce6
SHA512:	a6256e11df089a3063738ca0e36eca4ca89ed89ac7530a83394aa1864ba392e87318270529d04b1c72fa0d2cb392ba8c66ebedca335af82ec8fe124814ec9cab
SSDEEP:	6144:QBn1WN747c5LFA0rw3gw8QXRq+/lp7q76lS:gWZ4wa8QXRq+/Pe76lS
TLSH:	F434126B32F09476F961057099B3A657EBFA9300455813474BC7CFBBADB06C2CE8A172
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3(..RF..RF..RF.*]...RF..RG.pRF.*]...RF..qv..RF..T@..RF.Rich.RF.....PE..L...ly.V.....^.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40324f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x567F796C [Sun Dec 27 05:38:52 2015 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:	ab6770b0a8635b9d92a5838920cfe770

Entrypoint Preview
Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+1Ch], ebx
mov dword ptr [esp+14h], 00409130h
xor esi, esi
mov byte ptr [esp+18h], 00000020h
call dword ptr [004070B8h]
call dword ptr [004070B4h]
cmp ax, 00000006h
je 00007FDE449C9A73h
push ebx
call 00007FDE449CC861h
cmp eax, ebx
je 00007FDE449C9A69h
push 00000C00h
call eax
push 004091E0h
call 00007FDE449CC7E2h
push 004091D8h
call 00007FDE449CC7D8h
push 004091CCh
call 00007FDE449CC7CEh
push 0000000Dh
call 00007FDE449CC831h
push 0000000Bh
call 00007FDE449CC82Ah
mov dword ptr [00423F84h], eax
call dword ptr [00407034h]
push ebx
call dword ptr [00407270h]
mov dword ptr [00424038h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F538h
call dword ptr [00407160h]
push 004091C0h
push 00423780h
call 00007FDE449CC461h
call dword ptr [004070B0h]
mov ebp, 0042A000h
push eax
push ebp
call 00007FDE449CC44Fh
push ebx
call dword ptr [00407144h]

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73cc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x9e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c4a	0x5e00	False	0.659906914893617	data	6.410763775060762	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x115e	0x1200	False	0.4466145833333333	data	5.142548180775325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b078	0x600	False	0.455078125	data	4.2252195571372315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2d000	0x9e0	0xa00	False	0.45625	data	4.509328731926377	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d190	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x2d478	0x100	data	English	United States
RT_DIALOG	0x2d578	0x11c	data	English	United States
RT_DIALOG	0x2d698	0x60	data	English	United States
RT_GROUP_ICON	0x2d6f8	0x14	data	English	United States
RT_MANIFEST	0x2d710	0x2cc	XML 1.0 document, ASCII text, with very long lines (716), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileAttributesA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CompareFileTime, SearchPathA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, CreateDirectoryA, lstrcmpiA, GetTempPathA, GetCommandLineA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, LoadLibraryA, SetFileTime, CloseHandle, GlobalFree, lstrcmpA, ExpandEnvironmentStringsA, GetExitCodeProcess, GlobalAlloc, WaitForSingleObject, ExitProcess, GetWindowsDirectoryA, GetProcAddress, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, ReadFile, FindClose, GetPrivateProfileStringA, WritePrivateProfileStringA, WriteFile, MulDiv, LoadLibraryExA, GetModuleHandleA, MultiByteToWideChar, FreeLibrary

DLL	Import
USER32.dll	GetWindowRect, EnableMenuItem, GetSystemMenu, ScreenToClient, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetForegroundWindow, PostQuitMessage, RegisterClassA, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, DestroyWindow, OpenClipboard, TrackPopupMenu, SendMessageTimeoutA, GetDC, LoadImageA, GetDlgItem, FindWindowExA, IsWindow, SetClipboardData, SetWindowLongA, EmptyClipboard, SetTimer, CreateDialogParamA, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteValueA, SetFileSecurityA, RegOpenKeyExA, RegDeleteKeyA, RegEnumValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249737802025381 11/24/22-19:55:31.199874	TCP	2025381	ET TROJAN LokiBot Checkin	49737	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249748802021641 11/24/22-19:55:53.130311	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249750802825766 11/24/22-19:55:57.329298	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49750	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249751802021641 11/24/22-19:55:59.376338	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8.859881532014169 11/24/22-19:55:09.708351	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59881	53	192.168.2.6	8.8.8.8
95.213.216.202192.168.2.680497332025483 11/24/22-19:55:24.906100	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49733	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497352025483 11/24/22-19:55:28.867256	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49735	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249736802024318 11/24/22-19:55:29.163584	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49736	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497372025483 11/24/22-19:55:32.908191	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49737	95.213.216.202	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
95.213.216.202192.168.2.680497392025483 11/24/22-19:55:36.924861	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49739	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249754802024318 11/24/22-19:56:04.818902	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49754	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249736802024313 11/24/22-19:55:29.163584	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49736	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8.856122532014169 11/24/22-19:54:54.866804	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56122	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249754802024313 11/24/22-19:56:04.818902	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49754	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249711802024313 11/24/22-19:54:38.624655	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49711	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249705802021641 11/24/22-19:54:27.228813	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49705	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249719802025381 11/24/22-19:54:53.033944	TCP	2025381	ET TROJAN LokiBot Checkin	49719	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249729802825766 11/24/22-19:55:13.852615	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49729	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249722802025381 11/24/22-19:54:59.769485	TCP	2025381	ET TROJAN LokiBot Checkin	49722	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249747802825766 11/24/22-19:55:51.131718	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49747	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249711802024318 11/24/22-19:54:38.624655	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49711	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249740802025381 11/24/22-19:55:37.776321	TCP	2025381	ET TROJAN LokiBot Checkin	49740	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249750802025381 11/24/22-19:55:57.329298	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249737802825766 11/24/22-19:55:31.199874	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49737	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249714802825766 11/24/22-19:54:45.091814	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49714	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8.850343532014169 11/24/22-19:55:13.761219	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50343	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249741802021641 11/24/22-19:55:39.990050	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49741	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249709802025381 11/24/22-19:54:33.518227	TCP	2025381	ET TROJAN LokiBot Checkin	49709	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249723802021641 11/24/22-19:55:01.692450	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49723	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249727802025381 11/24/22-19:55:09.788187	TCP	2025381	ET TROJAN LokiBot Checkin	49727	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249700802021641 11/24/22-19:54:18.249997	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49700	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.856569532014169 11/24/22-19:55:23.105213	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56569	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249719802825766 11/24/22-19:54:53.033944	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49719	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249732802825766 11/24/22-19:55:21.169470	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49732	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.853943532014169 11/24/22-19:55:03.645658	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53943	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249755802025381 11/24/22-19:56:06.881877	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.855629532014169 11/24/22-19:55:19.049102	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55629	53	192.168.2.6	8.8.8.8
95.213.216.202192.168.2.680497312025483 11/24/22-19:55:20.867899	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49731	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249755802825766 11/24/22-19:56:06.881877	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49755	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249701802024313 11/24/22-19:54:22.087876	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49701	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249732802025381 11/24/22-19:55:21.169470	TCP	2025381	ET TROJAN LokiBot Checkin	49732	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.860130532014169 11/24/22-19:55:57.225226	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60130	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249718802024313 11/24/22-19:54:50.807735	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49718	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249701802024318 11/24/22-19:54:22.087876	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49701	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249699802024318 11/24/22-19:54:15.956073	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49699	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497402025483 11/24/22-19:55:39.709470	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49740	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497422025483 11/24/22-19:55:42.590814	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49742	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249718802024318 11/24/22-19:54:50.807735	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49718	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249699802024313 11/24/22-19:54:15.956073	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49699	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249702802025381 11/24/22-19:54:25.054966	TCP	2025381	ET TROJAN LokiBot Checkin	49702	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.861609532014169 11/24/22-19:54:59.613442	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61609	53	192.168.2.6	8.8.8.8
95.213.216.202192.168.2.680497282025483 11/24/22-19:55:13.560423	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49728	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249710802021641 11/24/22-19:54:35.914327	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49710	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249716802024318 11/24/22-19:54:48.704817	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49716	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.862958532014169 11/24/22-19:55:40.875534	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62958	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.864382532014169 11/24/22-19:54:15.835585	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64382	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249716802024313 11/24/22-19:54:48.704817	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49716	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249707802021641 11/24/22-19:54:31.276699	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49707	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249739802825766 11/24/22-19:55:35.259290	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49739	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497242025483 11/24/22-19:55:05.403255	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49724	95.213.216.202	192.168.2.6
192.168.2.68.8.8.849232532014169 11/24/22-19:55:31.114753	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49232	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.862848532014169 11/24/22-19:55:44.925533	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62848	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249713802021641 11/24/22-19:54:43.021097	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49713	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249745802825766 11/24/22-19:55:47.082758	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49745	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249731802024318 11/24/22-19:55:19.158567	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49731	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249706802825766 11/24/22-19:54:29.062049	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49706	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249749802024313 11/24/22-19:55:55.139215	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249709802825766 11/24/22-19:54:33.518227	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49709	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249731802024313 11/24/22-19:55:19.158567	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49731	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249746802024313 11/24/22-19:55:49.078874	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49746	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249742802825766 11/24/22-19:55:40.973542	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49742	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249749802024318 11/24/22-19:55:55.139215	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49749	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497072025483 11/24/22-19:54:33.040572	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49707	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249712802825766 11/24/22-19:54:40.926341	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49712	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249752802024313 11/24/22-19:56:01.434635	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249746802024318 11/24/22-19:55:49.078874	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49746	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249752802024318 11/24/22-19:56:01.434635	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49752	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249728802021641 11/24/22-19:55:11.780324	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49728	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249743802021641 11/24/22-19:55:42.875605	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249738802024313 11/24/22-19:55:33.192742	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49738	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8629105 32014169 11/24/22-19:54:44.985895	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62910	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249724802025381 11/24/22-19:55:03.741584	TCP	2025381	ET TROJAN LokiBot Checkin	49724	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249738802024318 11/24/22-19:55:33.192742	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49738	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249740802825766 11/24/22-19:55:37.776321	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49740	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249744802024313 11/24/22-19:55:45.028740	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49744	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249697802825766 11/24/22-19:54:11.348011	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49697	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8563315 32014169 11/24/22-19:54:31.195563	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56331	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8494485 32014169 11/24/22-19:54:35.800639	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49448	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249744802024318 11/24/22-19:55:45.028740	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49744	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8567505 32014169 11/24/22-19:56:03.361289	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56750	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8505065 32014169 11/24/22-19:54:33.429766	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50506	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8597525 32014169 11/24/22-19:55:35.135406	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59752	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249721802021641 11/24/22-19:54:56.896268	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49721	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249729802025381 11/24/22-19:55:13.852615	TCP	2025381	ET TROJAN LokiBot Checkin	49729	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249698802025381 11/24/22-19:54:13.981663	TCP	2025381	ET TROJAN LokiBot Checkin	49698	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249730802025381 11/24/22-19:55:16.067382	TCP	2025381	ET TROJAN LokiBot Checkin	49730	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8627325 32014169 11/24/22-19:55:59.286288	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62732	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8593365 32014169 11/24/22-19:56:04.733170	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59336	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249734802825766 11/24/22-19:55:25.189583	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49734	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8651985 32014169 11/24/22-19:54:42.928676	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	65198	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249735802025381 11/24/22-19:55:27.170416	TCP	2025381	ET TROJAN LokiBot Checkin	49735	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497542025483 11/24/22-19:56:06.628427	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49754	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249715802021641 11/24/22-19:54:47.405096	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49715	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497192025483 11/24/22-19:54:54.654090	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49719	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497522025483 11/24/22-19:56:03.175717	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49752	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249753802825766 11/24/22-19:56:03.443038	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49753	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8513215 32014169 11/24/22-19:55:51.025349	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51321	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249697802025381 11/24/22-19:54:11.348011	TCP	2025381	ET TROJAN LokiBot Checkin	49697	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249707802825766 11/24/22-19:54:31.276699	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49707	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249744802825766 11/24/22-19:55:45.028740	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49744	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249749802025381 11/24/22-19:55:55.139215	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497160250483 11/24/22-19:54:50.512832	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49716	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497140250483 11/24/22-19:54:46.656019	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49714	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249754802021641 11/24/22-19:56:04.818902	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49754	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249705802024318 11/24/22-19:54:27.228813	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49705	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249710802025381 11/24/22-19:54:35.914327	TCP	2025381	ET TROJAN LokiBot Checkin	49710	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497110250483 11/24/22-19:54:39.580169	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49711	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497130250483 11/24/22-19:54:44.610304	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49713	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249735802825766 11/24/22-19:55:27.170416	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49735	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249752802025381 11/24/22-19:56:01.434635	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8627665 32014169 11/24/22-19:55:55.046216	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62766	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249705802024313 11/24/22-19:54:27.228813	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49705	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249710802825766 11/24/22-19:54:35.914327	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49710	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249707802025381 11/24/22-19:54:31.276699	TCP	2025381	ET TROJAN LokiBot Checkin	49707	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8646015 32014169 11/24/22-19:54:24.912578	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64601	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249706802024313 11/24/22-19:54:29.062049	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49706	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249735802021641 11/24/22-19:55:27.170416	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49735	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249706802024318 11/24/22-19:54:29.062049	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49706	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8524815 32014169 11/24/22-19:55:01.607307	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52481	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249726802825766 11/24/22-19:55:07.738200	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49726	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249754802825766 11/24/22-19:56:04.818902	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49754	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249733802025381 11/24/22-19:55:23.201569	TCP	2025381	ET TROJAN LokiBot Checkin	49733	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249753802021641 11/24/22-19:56:03.443038	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49753	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249724802024313 11/24/22-19:55:03.741584	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49724	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8644045 32014169 11/24/22-19:55:42.774058	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64404	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249726802025381 11/24/22-19:55:07.738200	TCP	2025381	ET TROJAN LokiBot Checkin	49726	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249747802024318 11/24/22-19:55:51.131718	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49747	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249725802825766 11/24/22-19:55:05.694279	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49725	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249712802021641 11/24/22-19:54:40.926341	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49712	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249747802024313 11/24/22-19:55:51.131718	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49747	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8528655 32014169 11/24/22-19:55:37.629169	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52865	53	192.168.2.6	8.8.8.8
95.213.216.202192.168.2.680497462025483 11/24/22-19:55:50.859980	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49746	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249699802021641 11/24/22-19:54:15.956073	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49699	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249724802024318 11/24/22-19:55:03.741584	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49724	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497552025483 11/24/22-19:56:08.689068	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49755	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249719802021641 11/24/22-19:54:53.033944	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49719	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497442025483 11/24/22-19:55:46.796463	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49744	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497272025483 11/24/22-19:55:11.470809	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49727	95.213.216.202	192.168.2.6
192.168.2.68.8.8.8638635 32014169 11/24/22-19:54:46.995919	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63863	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249716802021641 11/24/22-19:54:48.704817	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49716	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249751802025381 11/24/22-19:55:59.376338	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249714802025381 11/24/22-19:54:45.091814	TCP	2025381	ET TROJAN LokiBot Checkin	49714	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249722802021641 11/24/22-19:54:59.769485	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49722	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497222025483 11/24/22-19:55:01.407205	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49722	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249720802025381 11/24/22-19:54:54.960633	TCP	2025381	ET TROJAN LokiBot Checkin	49720	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8532035 32014169 11/24/22-19:54:18.123294	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53203	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249700802825766 11/24/22-19:54:18.249997	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49700	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249737802024318 11/24/22-19:55:31.199874	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49737	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249740802024313 11/24/22-19:55:37.776321	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49740	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249742802025381 11/24/22-19:55:40.973542	TCP	2025381	ET TROJAN LokiBot Checkin	49742	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497052025483 11/24/22-19:54:28.634655	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49705	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249731802021641 11/24/22-19:55:19.158567	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49731	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8576865 32014169 11/24/22-19:54:13.553924	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57686	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8585955 32014169 11/24/22-19:54:28.961973	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58595	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249736802025381 11/24/22-19:55:29.163584	TCP	2025381	ET TROJAN LokiBot Checkin	49736	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249745802025381 11/24/22-19:55:47.082758	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8575155 32014169 11/24/22-19:55:48.986225	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57515	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249734802024318 11/24/22-19:55:25.189583	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49734	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497002025483 11/24/22-19:54:20.029122	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49700	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249725802021641 11/24/22-19:55:05.694279	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49725	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249734802024313 11/24/22-19:55:25.189583	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49734	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249743802024318 11/24/22-19:55:42.875605	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49743	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249728802024318 11/24/22-19:55:11.780324	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49728	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249737802024313 11/24/22-19:55:31.199874	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49737	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249728802024313 11/24/22-19:55:11.780324	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49728	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249739802025381 11/24/22-19:55:35.259290	TCP	2025381	ET TROJAN LokiBot Checkin	49739	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8.855956532014169 11/24/22-19:55:46.990731	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55956	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249743802024313 11/24/22-19:55:42.875605	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49743	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249709802024313 11/24/22-19:54:33.518227	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49709	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249738802021641 11/24/22-19:55:33.192742	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49738	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8.859082532014169 11/24/22-19:54:38.013432	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59082	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249740802024318 11/24/22-19:55:37.776321	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49740	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249722802825766 11/24/22-19:54:59.769485	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49722	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8.851530532014169 11/24/22-19:54:52.685795	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51530	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249701802025381 11/24/22-19:54:22.087876	TCP	2025381	ET TROJAN LokiBot Checkin	49701	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249723802025381 11/24/22-19:55:01.692450	TCP	2025381	ET TROJAN LokiBot Checkin	49723	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249721802024313 11/24/22-19:54:56.896268	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49721	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249750802021641 11/24/22-19:55:57.329298	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249715802024318 11/24/22-19:54:47.405096	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49715	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497302025483 11/24/22-19:55:17.735946	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49730	95.213.216.202	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249716802825766 11/24/22-19:54:48.704817	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49716	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249721802024318 11/24/22-19:54:56.896268	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49721	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8600325 32014169 11/24/22-19:55:29.068969	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60032	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249744802021641 11/24/22-19:55:45.028740	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497412025483 11/24/22-19:55:40.700457	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49741	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497492025483 11/24/22-19:55:57.050677	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49749	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249709802024318 11/24/22-19:54:33.518227	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49709	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249715802024313 11/24/22-19:54:47.405096	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49715	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8589175 32014169 11/24/22-19:55:11.700175	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58917	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249745802024318 11/24/22-19:55:47.082758	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49745	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497342025483 11/24/22-19:55:26.886961	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49734	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249742802021641 11/24/22-19:55:40.973542	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49742	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497362025483 11/24/22-19:55:30.902353	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49736	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497382025483 11/24/22-19:55:34.897313	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49738	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497322025483 11/24/22-19:55:22.836179	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49732	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249739802021641 11/24/22-19:55:35.259290	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49739	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249741802825766 11/24/22-19:55:39.990050	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49741	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249728802025381 11/24/22-19:55:11.780324	TCP	2025381	ET TROJAN LokiBot Checkin	49728	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249745802024313 11/24/22-19:55:47.082758	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49745	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249713802825766 11/24/22-19:54:43.021097	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49713	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20 249746802025381 11/24/22-19:55:49.078874	TCP	2025381	ET TROJAN LokiBot Checkin	49746	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8537315 32014169 11/24/22-19:54:11.254500	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53731	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20 249702802024318 11/24/22-19:54:25.054966	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49702	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249713802025381 11/24/22-19:54:43.021097	TCP	2025381	ET TROJAN LokiBot Checkin	49713	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249738802825766 11/24/22-19:55:33.192742	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49738	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8610895 32014169 11/24/22-19:55:53.045222	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61089	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20 249714802021641 11/24/22-19:54:45.091814	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49714	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249720802024313 11/24/22-19:54:54.960633	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49720	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249702802024313 11/24/22-19:54:25.054966	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49702	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249720802024318 11/24/22-19:54:54.960633	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49720	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249731802025381 11/24/22-19:55:19.158567	TCP	2025381	ET TROJAN LokiBot Checkin	49731	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249735802024313 11/24/22-19:55:27.170416	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49735	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249698802024317 11/24/22-19:54:13.981663	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49698	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249698802024312 11/24/22-19:54:13.981663	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49698	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249729802021641 11/24/22-19:55:13.852615	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49729	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249721802025381 11/24/22-19:54:56.896268	TCP	2025381	ET TROJAN LokiBot Checkin	49721	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249731802825766 11/24/22-19:55:19.158567	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49731	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249712802024313 11/24/22-19:54:40.926341	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49712	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249712802024318 11/24/22-19:54:40.926341	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49712	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20 249735802024318 11/24/22-19:55:27.170416	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49735	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249724802021641 11/24/22-19:55:03.741584	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49724	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249748802825766 11/24/22-19:55:53.130311	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49748	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249753802024318 11/24/22-19:56:03.443038	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49753	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249753802024313 11/24/22-19:56:03.443038	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49753	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249730802024318 11/24/22-19:55:16.067382	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49730	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249747802021641 11/24/22-19:55:51.131718	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49747	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249738802025381 11/24/22-19:55:33.192742	TCP	2025381	ET TROJAN LokiBot Checkin	49738	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249730802024313 11/24/22-19:55:16.067382	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49730	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249706802021641 11/24/22-19:54:29.062049	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49706	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249705802025381 11/24/22-19:54:27.228813	TCP	2025381	ET TROJAN LokiBot Checkin	49705	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8632295 32014169 11/24/22-19:54:48.619009	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63229	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249721802825766 11/24/22-19:54:56.896268	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49721	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249722802024313 11/24/22-19:54:59.769485	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49722	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497432025483 11/24/22-19:55:44.744520	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49743	95.213.216.202	192.168.2.6
192.168.2.68.8.8.8497865 32014169 11/24/22-19:54:27.135932	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49786	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249725802024313 11/24/22-19:55:05.694279	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49725	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249719802024318 11/24/22-19:54:53.033944	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49719	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249722802024318 11/24/22-19:54:59.769485	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49722	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249725802024318 11/24/22-19:55:05.694279	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49725	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8561235 32014169 11/24/22-19:55:33.111651	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56123	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249697802021641 11/24/22-19:54:11.348011	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49697	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249711802025381 11/24/22-19:54:38.624655	TCP	2025381	ET TROJAN LokiBot Checkin	49711	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249736802825766 11/24/22-19:55:29.163584	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49736	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497292025483 11/24/22-19:55:15.362841	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49729	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497252025483 11/24/22-19:55:07.447890	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49725	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497212025483 11/24/22-19:54:58.247548	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49721	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249750802024318 11/24/22-19:55:57.329298	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49750	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249737802021641 11/24/22-19:55:31.199874	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49737	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249751802825766 11/24/22-19:55:59.376338	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49751	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249740802021641 11/24/22-19:55:37.776321	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49740	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497022025483 11/24/22-19:54:26.773719	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49702	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497062025483 11/24/22-19:54:30.867234	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49706	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249754802025381 11/24/22-19:56:04.818902	TCP	2025381	ET TROJAN LokiBot Checkin	49754	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249699802825766 11/24/22-19:54:15.956073	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49699	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249719802024313 11/24/22-19:54:53.033944	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49719	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249734802021641 11/24/22-19:55:25.189583	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49734	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249748802025381 11/24/22-19:55:53.130311	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249715802825766 11/24/22-19:54:47.405096	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49715	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249732802021641 11/24/22-19:55:21.169470	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49732	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249709802021641 11/24/22-19:54:33.518227	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49709	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249755802024318 11/24/22-19:56:06.881877	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49755	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249741802025381 11/24/22-19:55:39.990050	TCP	2025381	ET TROJAN LokiBot Checkin	49741	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249755802024313 11/24/22-19:56:06.881877	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49755	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249723802825766 11/24/22-19:55:01.692450	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49723	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8650445 32014169 11/24/22-19:55:27.077654	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	65044	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249726802021641 11/24/22-19:55:07.738200	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49726	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249718802025381 11/24/22-19:54:50.807735	TCP	2025381	ET TROJAN LokiBot Checkin	49718	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249727802024313 11/24/22-19:55:09.788187	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49727	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249750802024313 11/24/22-19:55:57.329298	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249727802024318 11/24/22-19:55:09.788187	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49727	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249700802025381 11/24/22-19:54:18.249997	TCP	2025381	ET TROJAN LokiBot Checkin	49700	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249733802024313 11/24/22-19:55:23.201569	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49733	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497472025483 11/24/22-19:55:52.860690	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49747	95.213.216.202	192.168.2.6
192.168.2.68.8.8.8560865 32014169 11/24/22-19:55:05.605111	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56086	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249728802825766 11/24/22-19:55:11.780324	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49728	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249733802024318 11/24/22-19:55:23.201569	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49733	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497502025483 11/24/22-19:55:59.104900	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49750	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249734802025381 11/24/22-19:55:25.189583	TCP	2025381	ET TROJAN LokiBot Checkin	49734	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249742802024318 11/24/22-19:55:40.973542	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49742	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
95.213.216.202192.168.2.680497532025483 11/24/22-19:56:04.545301	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49753	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497182025483 11/24/22-19:54:52.477982	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49718	95.213.216.202	192.168.2.6
192.168.2.695.213.216.202497518020243131 1/24/22-19:55:59.376338	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8606905 32014169 11/24/22-19:56:01.353337	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60690	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.202497488020243131 1/24/22-19:55:53.130311	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49748	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.202497018028257666 11/24/22-19:54:22.087876	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49701	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8549035 32014169 11/24/22-19:54:50.721248	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	54903	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.202497438020253811 1/24/22-19:55:42.875605	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.202497428020243131 1/24/22-19:55:40.973542	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49742	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497152025483 11/24/22-19:54:48.216785	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49715	95.213.216.202	192.168.2.6
192.168.2.695.213.216.202497368020216411 1/24/22-19:55:29.163584	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49736	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.202497398020243131 1/24/22-19:55:35.259290	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49739	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.202497398020243188 1/24/22-19:55:35.259290	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49739	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.202497458020216411 1/24/22-19:55:47.082758	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.202497488020243188 1/24/22-19:55:53.130311	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49748	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680496992025483 11/24/22-19:54:17.569674	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49699	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497102025483 11/24/22-19:54:37.501776	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49710	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497122025483 11/24/22-19:54:42.610242	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49712	95.213.216.202	192.168.2.6
192.168.2.68.8.8.8565475 32014169 11/24/22-19:55:07.655761	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56547	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.202497148020243131 1/24/22-19:54:45.091814	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49714	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249720802021641 11/24/22-19:54:54.960633	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49720	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249714802024318 11/24/22-19:54:45.091814	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49714	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249725802025381 11/24/22-19:55:05.694279	TCP	2025381	ET TROJAN LokiBot Checkin	49725	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249702802021641 11/24/22-19:54:25.054966	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49702	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249711802021641 11/24/22-19:54:38.624655	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49711	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8595045 32014169 11/24/22-19:54:40.838615	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59504	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249716802025381 11/24/22-19:54:48.704817	TCP	2025381	ET TROJAN LokiBot Checkin	49716	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249698802021641 11/24/22-19:54:13.981663	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49698	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249729802024318 11/24/22-19:55:13.852615	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49729	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249700802024318 11/24/22-19:54:18.249997	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49700	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249715802025381 11/24/22-19:54:47.405096	TCP	2025381	ET TROJAN LokiBot Checkin	49715	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249723802024318 11/24/22-19:55:01.692450	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49723	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249729802024313 11/24/22-19:55:13.852615	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49729	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249723802024313 11/24/22-19:55:01.692450	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49723	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8525565 32014169 11/24/22-19:54:56.722023	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52556	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249741802024318 11/24/22-19:55:39.990050	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49741	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249749802825766 11/24/22-19:55:55.139215	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49749	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249741802024313 11/24/22-19:55:39.990050	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49741	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249700802024313 11/24/22-19:54:18.249997	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49700	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497202025483 11/24/22-19:54:56.488535	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49720	95.213.216.202	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249718802021641 11/24/22-19:54:50.807735	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49718	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249701802021641 11/24/22-19:54:22.087876	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49701	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497482025483 11/24/22-19:55:54.888388	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49748	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249720802825766 11/24/22-19:54:54.960633	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49720	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8.853107532014169 11/24/22-19:54:21.991089	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53107	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249702802825766 11/24/22-19:54:25.054966	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49702	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249744802025381 11/24/22-19:55:45.028740	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497512025483 11/24/22-19:56:01.147373	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49751	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249730802021641 11/24/22-19:55:16.067382	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49730	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249743802825766 11/24/22-19:55:42.875605	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49743	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249710802024318 11/24/22-19:54:35.914327	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49710	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249724802825766 11/24/22-19:55:03.741584	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49724	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249727802825766 11/24/22-19:55:09.788187	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49727	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497452025483 11/24/22-19:55:48.824554	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49745	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249713802024318 11/24/22-19:54:43.021097	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49713	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249710802024313 11/24/22-19:54:35.914327	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49710	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249718802825766 11/24/22-19:54:50.807735	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49718	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497092025483 11/24/22-19:54:35.412652	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49709	95.213.216.202	192.168.2.6
95.213.216.202192.168.2.680497232025483 11/24/22-19:55:03.460307	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49723	95.213.216.202	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249697802024312 11/24/22-19:54:11.348011	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49697	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249707802024313 11/24/22-19:54:31.276699	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49707	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8625205 32014169 11/24/22-19:55:15.969759	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62520	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8573225 32014169 11/24/22-19:55:39.901358	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57322	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249713802024313 11/24/22-19:54:43.021097	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49713	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249697802024317 11/24/22-19:54:11.348011	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49697	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497262025483 11/24/22-19:55:09.535230	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49726	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249707802024318 11/24/22-19:54:31.276699	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49707	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249746802021641 11/24/22-19:55:49.078874	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49746	80	192.168.2.6	95.213.216.202
95.213.216.202192.168.2.680497012025483 11/24/22-19:54:23.783923	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49701	95.213.216.202	192.168.2.6
192.168.2.695.213.216.20249733802825766 11/24/22-19:55:23.201569	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49733	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249752802021641 11/24/22-19:56:01.434635	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249730802825766 11/24/22-19:55:16.067382	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49730	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249732802024313 11/24/22-19:55:21.169470	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49732	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249726802024318 11/24/22-19:55:07.738200	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49726	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249753802025381 11/24/22-19:56:03.443038	TCP	2025381	ET TROJAN LokiBot Checkin	49753	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249732802024318 11/24/22-19:55:21.169470	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49732	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249705802825766 11/24/22-19:54:27.228813	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49705	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249746802825766 11/24/22-19:55:49.078874	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49746	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249755802021641 11/24/22-19:56:06.881877	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.6	95.213.216.202

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.695.213.216.20249747802025381 11/24/22-19:55:51.131718	TCP	2025381	ET TROJAN LokiBot Checkin	49747	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249699802025381 11/24/22-19:54:15.956073	TCP	2025381	ET TROJAN LokiBot Checkin	49699	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249726802024313 11/24/22-19:55:07.738200	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49726	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249749802021641 11/24/22-19:55:55.139215	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249698802825766 11/24/22-19:54:13.981663	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49698	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249727802021641 11/24/22-19:55:09.788187	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49727	80	192.168.2.6	95.213.216.202
192.168.2.68.8.8.8527155 32014169 11/24/22-19:56:06.802187	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52715	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8520795 32014169 11/24/22-19:55:21.075805	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52079	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8618335 32014169 11/24/22-19:55:25.100624	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61833	53	192.168.2.6	8.8.8.8
192.168.2.695.213.216.20249706802025381 11/24/22-19:54:29.062049	TCP	2025381	ET TROJAN LokiBot Checkin	49706	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249733802021641 11/24/22-19:55:23.201569	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49733	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249751802024318 11/24/22-19:55:59.376338	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49751	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249752802825766 11/24/22-19:56:01.434635	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49752	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249712802025381 11/24/22-19:54:40.926341	TCP	2025381	ET TROJAN LokiBot Checkin	49712	80	192.168.2.6	95.213.216.202
192.168.2.695.213.216.20249711802825766 11/24/22-19:54:38.624655	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49711	80	192.168.2.6	95.213.216.202

Network Port Distribution

Total Packets: 110

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:54:11.286669970 CET	49697	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:11.345004082 CET	80	49697	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:11.345129967 CET	49697	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:11.348011017 CET	49697	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:11.404728889 CET	80	49697	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:11.404869080 CET	49697	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:11.463299036 CET	80	49697	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:13.168977976 CET	80	49697	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:13.169079065 CET	49697	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:13.169225931 CET	49697	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:13.225949049 CET	80	49697	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:13.894681931 CET	49698	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:13.958650112 CET	80	49698	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:13.958801985 CET	49698	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:13.981662989 CET	49698	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:14.045726061 CET	80	49698	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:14.045902014 CET	49698	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:14.110209942 CET	80	49698	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:15.576119900 CET	80	49698	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:15.576334953 CET	49698	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:15.576581955 CET	49698	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:15.640427113 CET	80	49698	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:15.856637001 CET	49699	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:15.927886963 CET	80	49699	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:15.928071022 CET	49699	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:15.956073046 CET	49699	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:16.027493954 CET	80	49699	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:16.027601004 CET	49699	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:16.098913908 CET	80	49699	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:17.569674015 CET	80	49699	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:17.569780111 CET	49699	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:17.569870949 CET	49699	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:17.640960932 CET	80	49699	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:18.143421888 CET	49700	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:18.200618029 CET	80	49700	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:18.200839043 CET	49700	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:18.249996901 CET	49700	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:18.306715012 CET	80	49700	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:18.306893110 CET	49700	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:18.363512039 CET	80	49700	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:20.029122114 CET	80	49700	95.213.216.202	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:54:20.029288054 CET	49700	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:20.981195927 CET	49700	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:21.037904978 CET	80	49700	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:22.019980907 CET	49701	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:22.083102942 CET	80	49701	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:22.083247900 CET	49701	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:22.087876081 CET	49701	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:22.151021957 CET	80	49701	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:22.151093006 CET	49701	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:22.215147972 CET	80	49701	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:23.783922911 CET	80	49701	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:23.784240961 CET	49701	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:23.784240961 CET	49701	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:23.848484039 CET	80	49701	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:24.987267971 CET	49702	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:25.051772118 CET	80	49702	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:25.051894903 CET	49702	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:25.054965973 CET	49702	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:25.119350910 CET	80	49702	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:25.119462013 CET	49702	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:25.185128927 CET	80	49702	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:26.773719072 CET	80	49702	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:26.773926020 CET	49702	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:26.774003983 CET	49702	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:26.838639975 CET	80	49702	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:27.158658981 CET	49705	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:27.225601912 CET	80	49705	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:27.225811958 CET	49705	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:27.228812933 CET	49705	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:27.296253920 CET	80	49705	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:27.296644926 CET	49705	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:27.363353968 CET	80	49705	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:28.634654999 CET	80	49705	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:28.634825945 CET	49705	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:28.634994030 CET	49705	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:28.701540947 CET	80	49705	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:28.980576992 CET	49706	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:29.043751955 CET	80	49706	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:29.043917894 CET	49706	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:29.062048912 CET	49706	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:29.125628948 CET	80	49706	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:29.125740051 CET	49706	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:29.189388037 CET	80	49706	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:30.867233992 CET	80	49706	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:30.867374897 CET	49706	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:30.867445946 CET	49706	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:30.930533886 CET	80	49706	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:31.216176033 CET	49707	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:31.272813082 CET	80	49707	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:31.273060083 CET	49707	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:31.276699066 CET	49707	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:31.333493948 CET	80	49707	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:31.333655119 CET	49707	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:31.390275955 CET	80	49707	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:33.040571928 CET	80	49707	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:33.045016050 CET	49707	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:33.045016050 CET	49707	80	192.168.2.6	95.213.216.202
Nov 24, 2022 19:54:33.101850033 CET	80	49707	95.213.216.202	192.168.2.6
Nov 24, 2022 19:54:33.449861050 CET	49709	80	192.168.2.6	95.213.216.202

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:54:11.254499912 CET	53731	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:11.273976088 CET	53	53731	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:13.553924084 CET	57686	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:13.892705917 CET	53	57686	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:15.835585117 CET	64382	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:15.854994059 CET	53	64382	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:18.123294115 CET	53203	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:18.140840054 CET	53	53203	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:21.991089106 CET	53107	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:22.012207031 CET	53	53107	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:24.912578106 CET	64601	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:24.931736946 CET	53	64601	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:27.135931969 CET	49786	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:27.153167009 CET	53	49786	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:28.961972952 CET	58595	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:28.979187965 CET	53	58595	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:31.195563078 CET	56331	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:31.213350058 CET	53	56331	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:33.429765940 CET	50506	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:33.448172092 CET	53	50506	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:35.800638914 CET	49448	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:35.820136070 CET	53	49448	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:38.013432026 CET	59082	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:38.032367945 CET	53	59082	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:40.838614941 CET	59504	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:40.860896111 CET	53	59504	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:42.928675890 CET	65198	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:42.948046923 CET	53	65198	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:44.985894918 CET	62910	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:45.005995035 CET	53	62910	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:46.995918989 CET	63863	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:47.343003035 CET	53	63863	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:48.619009018 CET	63229	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:48.638283968 CET	53	63229	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:50.721247911 CET	54903	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:50.739190102 CET	53	54903	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:52.685795069 CET	51530	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:52.959728956 CET	53	51530	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:54.866803885 CET	56122	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:54.884646893 CET	53	56122	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:56.722023010 CET	52556	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:56.741736889 CET	53	52556	8.8.8.8	192.168.2.6
Nov 24, 2022 19:54:59.613441944 CET	61609	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:54:59.633409977 CET	53	61609	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:01.607306957 CET	52481	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:01.624758959 CET	53	52481	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:03.645658016 CET	53943	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:03.665380001 CET	53	53943	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:05.605110884 CET	56086	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:05.624840975 CET	53	56086	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:07.655761003 CET	56547	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:07.675786018 CET	53	56547	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:09.708350897 CET	59881	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:09.725904942 CET	53	59881	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:11.700175047 CET	58917	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:11.717746019 CET	53	58917	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:13.761219025 CET	50343	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:55:13.780757904 CET	53	50343	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:15.969758987 CET	62520	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:15.987411976 CET	53	62520	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:19.049102068 CET	55629	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:19.068536043 CET	53	55629	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:21.075804949 CET	52079	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:21.095380068 CET	53	52079	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:23.105212927 CET	56569	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:23.122698069 CET	53	56569	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:25.100624084 CET	61833	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:25.119568110 CET	53	61833	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:27.077653885 CET	65044	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:27.096754074 CET	53	65044	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:29.068969011 CET	60032	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:29.090148926 CET	53	60032	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:31.114753008 CET	49232	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:31.132338047 CET	53	49232	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:33.111650944 CET	56123	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:33.130673885 CET	53	56123	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:35.135406017 CET	59752	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:35.155647993 CET	53	59752	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:37.629168987 CET	52865	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:37.651962996 CET	53	52865	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:39.901357889 CET	57322	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:39.918622017 CET	53	57322	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:40.875534058 CET	62958	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:40.892956972 CET	53	62958	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:42.774058104 CET	64404	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:42.793642044 CET	53	64404	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:44.925533056 CET	62848	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:44.944977045 CET	53	62848	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:46.990731001 CET	55956	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:47.007882118 CET	53	55956	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:48.986224890 CET	57515	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:49.005459070 CET	53	57515	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:51.025348902 CET	51321	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:51.042560101 CET	53	51321	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:53.045222044 CET	61089	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:53.064853907 CET	53	61089	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:55.046216011 CET	62766	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:55.065582991 CET	53	62766	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:57.225225925 CET	60130	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:57.242645979 CET	53	60130	8.8.8.8	192.168.2.6
Nov 24, 2022 19:55:59.286288023 CET	62732	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:55:59.304116011 CET	53	62732	8.8.8.8	192.168.2.6
Nov 24, 2022 19:56:01.353337049 CET	60690	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:56:01.372248888 CET	53	60690	8.8.8.8	192.168.2.6
Nov 24, 2022 19:56:03.361289024 CET	56750	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:56:03.381324053 CET	53	56750	8.8.8.8	192.168.2.6
Nov 24, 2022 19:56:04.733170033 CET	59336	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:56:04.750690937 CET	53	59336	8.8.8.8	192.168.2.6
Nov 24, 2022 19:56:06.802186966 CET	52715	53	192.168.2.6	8.8.8.8
Nov 24, 2022 19:56:06.820142984 CET	53	52715	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:54:11.254499912 CET	192.168.2.6	8.8.8.8	0x9d33	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:54:13.553924084 CET	192.168.2.6	8.8.8.8	0xec24	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:15.835585117 CET	192.168.2.6	8.8.8.8	0x6c3f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:18.123294115 CET	192.168.2.6	8.8.8.8	0x9e45	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:21.991089106 CET	192.168.2.6	8.8.8.8	0x913b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:24.912578106 CET	192.168.2.6	8.8.8.8	0xf13b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:27.135931969 CET	192.168.2.6	8.8.8.8	0x3278	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:28.961972952 CET	192.168.2.6	8.8.8.8	0x88c4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:31.195563078 CET	192.168.2.6	8.8.8.8	0x811e	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:33.429765940 CET	192.168.2.6	8.8.8.8	0x5dea	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:35.800638914 CET	192.168.2.6	8.8.8.8	0x3818	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:38.013432026 CET	192.168.2.6	8.8.8.8	0xbc15	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:40.838614941 CET	192.168.2.6	8.8.8.8	0xdfe4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:42.928675890 CET	192.168.2.6	8.8.8.8	0x467c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:44.985894918 CET	192.168.2.6	8.8.8.8	0x8e71	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:46.995918989 CET	192.168.2.6	8.8.8.8	0xdce6	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:48.619009018 CET	192.168.2.6	8.8.8.8	0x64a9	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:50.721247911 CET	192.168.2.6	8.8.8.8	0x44bb	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:52.685795069 CET	192.168.2.6	8.8.8.8	0x15bd	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:54.866803885 CET	192.168.2.6	8.8.8.8	0xaf57	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:56.722023010 CET	192.168.2.6	8.8.8.8	0x428c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:59.613441944 CET	192.168.2.6	8.8.8.8	0x5781	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:01.607306957 CET	192.168.2.6	8.8.8.8	0x5577	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:03.645658016 CET	192.168.2.6	8.8.8.8	0xe821	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:05.605110884 CET	192.168.2.6	8.8.8.8	0x78c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:07.655761003 CET	192.168.2.6	8.8.8.8	0x88bf	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:09.708350897 CET	192.168.2.6	8.8.8.8	0x41dd	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:11.700175047 CET	192.168.2.6	8.8.8.8	0x6184	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:13.761219025 CET	192.168.2.6	8.8.8.8	0x6a56	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:15.969758987 CET	192.168.2.6	8.8.8.8	0x5414	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:19.049102068 CET	192.168.2.6	8.8.8.8	0x7518	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:21.075804949 CET	192.168.2.6	8.8.8.8	0x4df8	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:23.105212927 CET	192.168.2.6	8.8.8.8	0xcd7f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:25.100624084 CET	192.168.2.6	8.8.8.8	0x1c89	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:27.077653885 CET	192.168.2.6	8.8.8.8	0xc1ed	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:29.068969011 CET	192.168.2.6	8.8.8.8	0x72e9	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:55:31.114753008 CET	192.168.2.6	8.8.8.8	0x3b2b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:33.111650944 CET	192.168.2.6	8.8.8.8	0xaf95	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:35.135406017 CET	192.168.2.6	8.8.8.8	0x83f0	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:37.629168987 CET	192.168.2.6	8.8.8.8	0x7648	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:39.901357889 CET	192.168.2.6	8.8.8.8	0x44d4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:40.875534058 CET	192.168.2.6	8.8.8.8	0x10a4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:42.774058104 CET	192.168.2.6	8.8.8.8	0x8c97	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:44.925533056 CET	192.168.2.6	8.8.8.8	0xd56b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:46.990731001 CET	192.168.2.6	8.8.8.8	0xa25f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:48.986224890 CET	192.168.2.6	8.8.8.8	0x70ee	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:51.025348902 CET	192.168.2.6	8.8.8.8	0x4c51	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:53.045222044 CET	192.168.2.6	8.8.8.8	0xf711	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:55.046216011 CET	192.168.2.6	8.8.8.8	0x6cf7	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:57.225225925 CET	192.168.2.6	8.8.8.8	0x84b4	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:59.286288023 CET	192.168.2.6	8.8.8.8	0xe37	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:56:01.353337049 CET	192.168.2.6	8.8.8.8	0x9b9f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:56:03.361289024 CET	192.168.2.6	8.8.8.8	0x8ac8	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:56:04.733170033 CET	192.168.2.6	8.8.8.8	0xb980	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:56:06.802186966 CET	192.168.2.6	8.8.8.8	0xdf9	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 19:54:11.273976088 CET	8.8.8.8	192.168.2.6	0x9d33	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:13.892705917 CET	8.8.8.8	192.168.2.6	0xec24	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:15.854994059 CET	8.8.8.8	192.168.2.6	0x6c3f	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:18.140840054 CET	8.8.8.8	192.168.2.6	0x9e45	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:22.012207031 CET	8.8.8.8	192.168.2.6	0x913b	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:24.931736946 CET	8.8.8.8	192.168.2.6	0xf13b	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:27.153167009 CET	8.8.8.8	192.168.2.6	0x3278	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:28.979187965 CET	8.8.8.8	192.168.2.6	0x88c4	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:31.213350058 CET	8.8.8.8	192.168.2.6	0x811e	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 19:54:33.448172092 CET	8.8.8.8	192.168.2.6	0x5dea	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:35.820136070 CET	8.8.8.8	192.168.2.6	0x3818	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:38.032367945 CET	8.8.8.8	192.168.2.6	0xbc15	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:40.860896111 CET	8.8.8.8	192.168.2.6	0xdfe4	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:42.948046923 CET	8.8.8.8	192.168.2.6	0x467c	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:45.005995035 CET	8.8.8.8	192.168.2.6	0x8e71	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:47.343003035 CET	8.8.8.8	192.168.2.6	0xdce6	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:48.638283968 CET	8.8.8.8	192.168.2.6	0x64a9	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:50.739190102 CET	8.8.8.8	192.168.2.6	0x44bb	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:52.959728956 CET	8.8.8.8	192.168.2.6	0x15bd	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:54.884646893 CET	8.8.8.8	192.168.2.6	0xaf57	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:56.741736889 CET	8.8.8.8	192.168.2.6	0x428c	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:54:59.633409977 CET	8.8.8.8	192.168.2.6	0x5781	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:01.624758959 CET	8.8.8.8	192.168.2.6	0x5577	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:03.665380001 CET	8.8.8.8	192.168.2.6	0xe821	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:05.624840975 CET	8.8.8.8	192.168.2.6	0x78c	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:07.675786018 CET	8.8.8.8	192.168.2.6	0x88bf	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:09.725904942 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:11.717746019 CET	8.8.8.8	192.168.2.6	0x6184	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:13.780757904 CET	8.8.8.8	192.168.2.6	0x6a56	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:15.987411976 CET	8.8.8.8	192.168.2.6	0x5414	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:19.068536043 CET	8.8.8.8	192.168.2.6	0x7518	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:21.095380068 CET	8.8.8.8	192.168.2.6	0x4df8	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:23.122698069 CET	8.8.8.8	192.168.2.6	0xcd7f	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:25.119568110 CET	8.8.8.8	192.168.2.6	0x1c89	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false

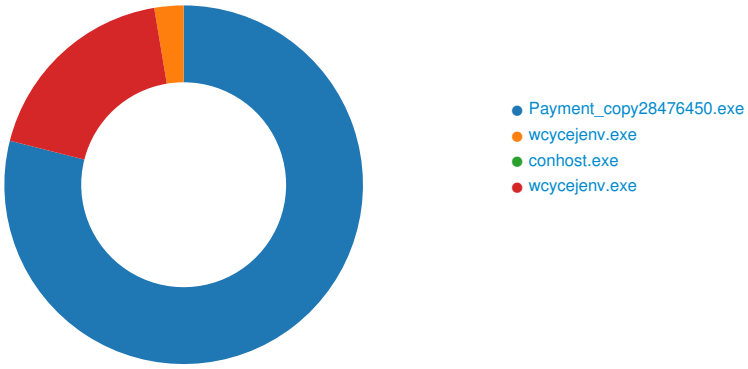
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 19:55:27.096754074 CET	8.8.8.8	192.168.2.6	0xc1ed	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:29.090148926 CET	8.8.8.8	192.168.2.6	0x72e9	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:31.132338047 CET	8.8.8.8	192.168.2.6	0x3b2b	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:33.130673885 CET	8.8.8.8	192.168.2.6	0xaf95	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:35.155647993 CET	8.8.8.8	192.168.2.6	0x83f0	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:37.651962996 CET	8.8.8.8	192.168.2.6	0x7648	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:39.918622017 CET	8.8.8.8	192.168.2.6	0x44d4	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:40.892956972 CET	8.8.8.8	192.168.2.6	0x10a4	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:42.793642044 CET	8.8.8.8	192.168.2.6	0x8c97	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:44.944977045 CET	8.8.8.8	192.168.2.6	0xd56b	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:47.007882118 CET	8.8.8.8	192.168.2.6	0xa25f	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:49.005459070 CET	8.8.8.8	192.168.2.6	0x70ee	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:51.042560101 CET	8.8.8.8	192.168.2.6	0x4c51	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:53.064853907 CET	8.8.8.8	192.168.2.6	0xf711	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:55.065582991 CET	8.8.8.8	192.168.2.6	0x6cf7	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:57.242645979 CET	8.8.8.8	192.168.2.6	0x84b4	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:55:59.304116011 CET	8.8.8.8	192.168.2.6	0xe37	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:56:01.372248888 CET	8.8.8.8	192.168.2.6	0x9b9f	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:56:03.381324053 CET	8.8.8.8	192.168.2.6	0x8ac8	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:56:04.750690937 CET	8.8.8.8	192.168.2.6	0xb980	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:56:06.820142984 CET	8.8.8.8	192.168.2.6	0xdf9	No error (0)	sempersim.su		95.213.216.202	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- sempersim.su

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Payment_copy28476450.exe PID: **160**, Parent PID: **3452**

General

Target ID:	0
Start time:	19:54:02
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\Payment_copy28476450.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment_copy28476450.exe
Imagebase:	0x400000
File size:	247655 bytes
MD5 hash:	70E90926399154C2708801A73CF53D99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405532	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg6B4C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405A34	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsg6B4D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405A34	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsg6B4E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405A34	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg6B4E.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ntwcyphb.r	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4059FE	CreateFileA
C:\Users\user\AppData\Local\Temp\stvrrcrc.d	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4059FE	CreateFileA
C:\Users\user\AppData\Local\Temp\wcycejenv.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4059FE	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg6B4C.tmp	success or wait	1	40340A	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg6B4E.tmp	success or wait	1	405644	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg6B4D.tmp	0	22137	fd 18 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 09 00 00 4e 00 00 00 64 12 00 00 00 00 00 00 fd 17 00 00 01 00 00 00 fd 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	,Nd	success or wait	23	403161	WriteFile
C:\Users\user\AppData\Local\Temp\ntwcyphb.r	0	16384	18 08 fd 0d 7b 54 28 0a fd 01 7c 59 2a fd 09 3c fd 28 61 6b fd 35 fd 9a 1d fd 43 fd 1b fd 22 fd fd 04 20 fd 49 34 fd fd 1c fd fd fd 7e fd 14 fd fd 02 fd fd 2d fd fd 78 4e fd fd 7a a8 fd fd fd fd 42 0d fd fd fd fd 33 4f fd fd fd 06 fd 27 04 fd 03 55 36 fd fd 30 25 fd 5d 2a 0c fd 39 fd 5b 51 50 4e 0a 1a 0c 15 03 fd fd fd fd 7b 19 fd 75 21 fd fd fd 47 fd a0 fd fd fd fd fd 1d fd fd 50 2e 06 57 58 fd fd fd 7b 10 5a 7e fd 46 72 0e fd fd fd fd 3e 5a 78 fd fd 12 fd fd fd 1f fd fd 5b 36 00 fd 02 20 3f 71 fd 65 fd 34 fd fd 64 fd 6b fd fd fd 02 58 fd 31 fd fd 46 fd 16 fd fd 09 22 75 fd 55 fd fd 28 76 fd fd fd 09 fd 3a 6c 04 6a 79 7e 17 e4 01 5a fd 68 fd 14 fd 2b fd fd fd 4d fd 16 fd fd fd fd fd 19 64 fd 46 fd 1e fd 78 fd 5d 40 36 6a 63 23 fd	{T(|Y*<(ak5C" I4~-xNzB3O'U60%] *9[QPN{u!GP.WX{Z~Fr> Zx[6 ?qe4d kX1F"uU(v:ljy~Zh+MdFx] @6jc#	success or wait	7	402FFA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\stvrrcrc.d	0	5655	fd 2a fd 3c 3c 60 fd 2c 3c 3c 3c fd 7c fd fd 7c fd fd 3c fd 3c fd 7c fd 4b fd fd fd 60 fd 2c 3c 3c 3c fd fd fd 7c fd fd 74 fd fd fd 07 71 fd 07 7e 2c fd 3d 3c 3c 01 fd 70 72 fd 3e 63 fd 71 fd 3b fd cb fd fd 24 fd fd fd 4a fd 3c fd fd fd fd fd 71 fd fd 2e 2b 3c 3c fd d6 fd 32 4d fd fd 1d fd fd 73 44 fd 57 fd 4d fd fd 46 fd 4a 01 07 71 fd fd fd fd 4a fd 3c fd fd fd fd 60 fd 2c 3c 3c 3c fd 7c fd fd 7c fd fd 3c fd 3c fd 7c fd 64 0f 58 fd 07 fd fd fd 3c 3c 3c 01 fd 70 fd 09 fd fd fd 52 07 07 4c fd 54 fd fd 2b fd fd 45 4b 3b fd 45 4b fd fd fd fd fd fd fd fd 01 fd 70 fd fd 48 01 5a 70 fd fd fd 79 fd 01 07 70 fd 13 4c fd 3a 04 fd fd 0b fd 3d 71 fd fd fd fd 4a fd 3c fd fd fd fd fd fd fd fd fd 79 fd 3b fd fd fd 38 fd fd 34 74 fd 4f fd fd 5c fd fd	*<<`,<<<||<<|K`,<<<|tq~,=<<pr>cq;$J<q.+<<2MsDWMFJqJ<`,<<<|| <<|dX<<<pRLT+EK;EKpZ pypL:=qJ<y;84tO\	success or wait	1	402FFA	WriteFile
C:\Users\user\AppData\Local\Temp\wcycejenv.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 fd 29 fd 2d fd 47 fd 2d fd 47 fd 2d fd 47 fd 76 fd 44 fd 27 fd 47 fd 76 fd 42 fd fd fd 47 fd 76 fd 43 fd 3f fd 47 fd fd fd fd fd 2f fd 47 fd fd fd 42 fd 08 fd 47 fd fd fd 43 fd 3e fd 47 fd fd fd 44 fd 38 fd 47 fd 76 fd 46 fd 34 fd 47 fd 2d fd 46 fd fd fd 47 fd fd fd 43 fd 2c fd 47 fd fd fd fd fd 2c fd 47 fd fd fd 45 fd 2c fd 47 fd 52 69 63 68 2d fd 47 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$i)-G-G-GvD'GvB GvC? G/GBGC>GD8GvF4G-FGC,G,GE,GRich-G	success or wait	21	402FFA	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Payment_copy28476450.exe	unknown	512	success or wait	67	4031F2	ReadFile
C:\Users\user\Desktop\Payment_copy28476450.exe	unknown	16384	success or wait	14	4031F2	ReadFile
C:\Users\user\AppData\Local\Temp\nsg6B4D.tmp	unknown	4	success or wait	1	402F84	ReadFile
C:\Users\user\AppData\Local\Temp\nsg6B4D.tmp	unknown	6291	success or wait	1	40303A	ReadFile
C:\Users\user\AppData\Local\Temp\nsg6B4D.tmp	unknown	4	success or wait	3	402F84	ReadFile
C:\Users\user\AppData\Local\Temp\nsg6B4D.tmp	unknown	16384	success or wait	29	402FDE	ReadFile

Analysis Process: wcycejenv.exe PID: **588**, Parent PID: **160**

General

Target ID:	1
Start time:	19:54:03
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\wcycejenv.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Local\Temp\wcycejenv.exe" C:\Users\user\AppData\Local\Temp\stvrrcrc.d
Imagebase:	0x400000
File size:	340992 bytes
MD5 hash:	3182BEF520A1E9F52BE3755C25E4C3B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.259864404.0000000000610000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 50%, ReversingLabs • Detection: 23%, Virustotal, Browse
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\stvrrcrc.d	unknown	5655	success or wait	1	4065A2	ReadFile

Analysis Process: conhost.exe PID: 584, Parent PID: 588

General

Target ID:	2
Start time:	19:54:03
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: wcycejenv.exe PID: 5332, Parent PID: 588

General

Target ID:	3
Start time:	19:54:04
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\wcycejenv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\wcycejenv.exe" C:\Users\user\AppData\Local\Temp\stvrrcrc.d

Imagebase:	0x400000
File size:	340992 bytes
MD5 hash:	3182BEF520A1E9F52BE3755C25E4C3B0
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: 00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000000.253960864.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000003.00000002.510358180.0000000000737000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.510096240.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000002.510096240.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000002.510096240.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000002.510096240.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000003.00000002.510096240.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000002.510096240.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000002.510096240.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000002.510096240.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\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:\Users\user\AppData\Local\Temp\wcycejenv.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	49152	success or wait	1	40415C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	40415C	ReadFile

Disassembly

No disassembly