

ID: 736955
Sample Name: transferencia bancaria.pdf.exe
Cookbook: default.jbs
Time: 12:28:50
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report transferencia bancaria.pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Lokibot 4
Yara Signatures 4
PCAP (Network Traffic) 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 42
AV Detection 42
Networking 43
System Summary 43
Data Obfuscation 43
Hooking and other Techniques for Hiding and Protection 43
Malware Analysis System Evasion 43
HIPS / PFW / Operating System Protection Evasion 43
Stealing of Sensitive Information 43
Mitre Att&ck Matrix 43
Behavior Graph 44
Screenshots 44
Thumbnails 44
Antivirus, Machine Learning and Genetic Malware Detection 45
Initial Sample 45
Dropped Files 45
Unpacked PE Files 45
Domains 46
URLs 46
Domains and IPs 46
Contacted Domains 46
Contacted URLs 46
URLs from Memory and Binaries 47
World Map of Contacted IPs 48
Public IPs 48
General Information 48
Warnings 49
Simulations 49
Behavior and APIs 49
Joe Sandbox View / Context 49
IPs 49
Domains 49
ASNs 49
JA3 Fingerprints 49
Dropped Files 49
Created / dropped Files 50
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\transferencia bancaria.pdf.exe.log 50
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck 50
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a 50
Static File Info 51
General 51
File Icon 51
Static PE Info 51
General 51
Entrypoint Preview 51
Data Directories 53
Sections 53
Resources 54
Imports 54
Network Behavior 54
Snort IDS Alerts 54
Network Port Distribution 68
TCP Packets 68
UDP Packets 70
DNS Queries 71

Copyright Joe Security LLC 2022

DNS Answers 73
HTTP Request Dependency Graph 74
Statistics 75
Behavior 75
System Behavior 75
Analysis Process: transferencia bancaria.pdf.exePID: 1100, Parent PID: 3452 75
General 75
File Activities 76
File Created 76
File Written 76
File Read 77
Analysis Process: transferencia bancaria.pdf.exePID: 5228, Parent PID: 1100 77
General 77
File Activities 78
File Created 78
File Deleted 78
File Moved 78
File Written 78
File Read 78
Disassembly 78

Copyright Joe Security LLC 2022

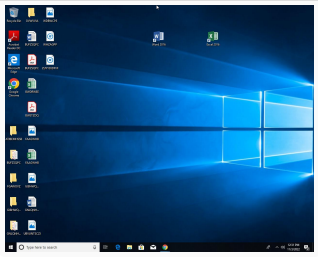
Windows Analysis Report

transferencia bancaria.pdf.exe

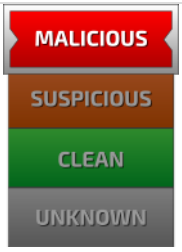
Overview

General Information

Sample Name:	transferencia bancaria.pdf.exe
Analysis ID:	736955
MD5:	355efb2e1f7dd36.
SHA1:	864f8d367c72d3..
SHA256:	cb90ea9b90ccb6..
Tags:	exe Loki
Infos:	



Detection



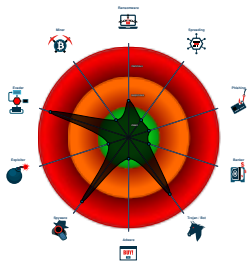
Lokibot

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Lokibot
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Yara detected aPLib compressed bi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- transferencia bancaria.pdf.exe (PID: 1100 cmdline: C:\Users\user\Desktop\transferencia bancaria.pdf.exe MD5: 355EFB2E1F7DD361F8E7CDA449A45EAC)
  - transferencia bancaria.pdf.exe (PID: 5228 cmdline: C:\Users\user\Desktop\transferencia bancaria.pdf.exe MD5: 355EFB2E1F7DD361F8E7CDA449A45EAC)
- **cleanup**

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "http://sempersim.su/gl21/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
00000001.00000000.275125166.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Lokibot_0f421617	unknown	unknown	• 0x43bb:$a: 08 8B CE 0F B6 14 38 D3 E2 83 C1 08 03 F2 48 79 F2 5F 8B C6
00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.transferencia bancaria.pdf.exe.400000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x18074:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13e80:$s2: https:// • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
1.0.transferencia bancaria.pdf.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
1.0.transferencia bancaria.pdf.exe.400000.0.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
1.0.transferencia bancaria.pdf.exe.400000.0.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
1.0.transferencia bancaria.pdf.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x16536:$f1: FileZilla\recentservers.xml • 0x16576:$f2: FileZilla\sitemanager.xml • 0x147e6:$b2: Mozilla\Firefox\Profiles • 0x14550:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x146fa:$s4: logins.json • 0x155a4:$s6: wand.dat • 0x14024:$a1: username_value • 0x14014:$a2: password_value • 0x1465f:$a3: encryptedUsername • 0x146cc:$a3: encryptedUsername • 0x14672:$a4: encryptedPassword • 0x146e0:$a4: encryptedPassword
Click to see the 45 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549712802024318 11/03/22-12:30:22.162497
SID:	2024318
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549727802024313 11/03/22-12:31:01.987085
SID:	2024313
Source Port:	49727
Destination Port:	80

Copyright Joe Security LLC 2022

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549723802825766 11/03/22-12:30:53.367985
SID:	2825766
Source Port:	49723
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549724802021641 11/03/22-12:30:54.913991
SID:	2021641
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:	192.168.2.68.8.8.859881532014169 11/03/22-12:31:01.170102
SID:	2014169
Source Port:	59881
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:	192.168.2.68.8.8.856122532014169 11/03/22-12:30:45.704907
SID:	2014169
Source Port:	56122
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549741802825766 11/03/22-12:31:39.946873
SID:	2825766
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549745802024313 11/03/22-12:31:50.569101
SID:	2024313
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549728802025381 11/03/22-12:31:03.903902
SID:	2025381
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549739802021641 11/03/22-12:31:35.606377
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549738802825766 11/03/22-12:31:33.019427
SID:	2825766
Source Port:	49738
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549713802025381 11/03/22-12:30:25.414440
SID:	2025381
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549731802025381 11/03/22-12:31:09.511791
SID:	2025381
Source Port:	49731
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549737802024318 11/03/22-12:31:31.046497
SID:	2024318
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549713802825766 11/03/22-12:30:25.414440
SID:	2825766
Source Port:	49713
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497182025483 11/03/22-12:30:41.067853
SID:	2025483
Source Port:	80
Destination Port:	49718
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497092025483 11/03/22-12:30:17.656419
SID:	2025483
Source Port:	80
Destination Port:	49709

Copyright Joe Security LLC 2022

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 11/03/22-12:31:05.602892
SID:	2014169
Source Port:	50343
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549717802024318 11/03/22-12:30:35.019960
SID:	2024318
Source Port:	49717
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549717802024313 11/03/22-12:30:35.019960
SID:	2024313
Source Port:	49717
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 11/03/22-12:31:22.519121
SID:	2014169
Source Port:	56569
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497122025483 11/03/22-12:30:23.556931
SID:	2025483
Source Port:	80
Destination Port:	49712
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549729802021641 11/03/22-12:31:05.707382
SID:	2021641
Source Port:	49729
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549742802021641 11/03/22-12:31:41.893270
SID:	2021641
Source Port:	49742
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 11/03/22-12:30:54.819244
SID:	2014169
Source Port:	53943
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549730802024318 11/03/22-12:31:07.626823
SID:	2024318
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497102025483 11/03/22-12:30:19.791139
SID:	2025483
Source Port:	80
Destination Port:	49710
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549735802024313 11/03/22-12:31:27.516452
SID:	2024313
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549721802025381 11/03/22-12:30:48.032802
SID:	2025381
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:	192.168.2.68.8.8.855629532014169 11/03/22-12:31:09.419344
SID:	2014169
Source Port:	55629
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549731802825766 11/03/22-12:31:09.511791
SID:	2825766
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549738802025381 11/03/22-12:31:33.019427
SID:	2025381
Source Port:	49738
Destination Port:	80

Copyright Joe Security LLC 2022

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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549712802024313 11/03/22-12:30:22.162497
SID:	2024313
Source Port:	49712
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497142025483 11/03/22-12:30:29.899760
SID:	2025483
Source Port:	80
Destination Port:	49714
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497162025483 11/03/22-12:30:34.572782
SID:	2025483
Source Port:	80
Destination Port:	49716
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549706802021641 11/03/22-12:30:09.785093
SID:	2021641
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549730802024313 11/03/22-12:31:07.626823
SID:	2024313
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:	192.168.2.68.8.8.861609532014169 11/03/22-12:30:50.734926
SID:	2014169
Source Port:	61609
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:	192.168.2.68.8.8.862958532014169 11/03/22-12:31:41.802948
SID:	2014169
Source Port:	62958
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549735802024318 11/03/22-12:31:27.516452
SID:	2024318
Source Port:	49735
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:	192.168.2.68.8.8.849232532014169 11/03/22-12:31:30.955921
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 11/03/22-12:31:45.492508
SID:	2014169
Source Port:	62848
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549733802025381 11/03/22-12:31:22.614964
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549732802021641 11/03/22-12:31:20.467945
SID:	2021641
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549720802024318 11/03/22-12:30:45.793165
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549718802025381 11/03/22-12:30:37.003049
SID:	2025381
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549721802825766 11/03/22-12:30:48.032802
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549720802024313 11/03/22-12:30:45.793165
SID:	2024313
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549714802024318 11/03/22-12:30:27.432237
SID:	2024318
Source Port:	49714
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549719802024318 11/03/22-12:30:42.564459
SID:	2024318
Source Port:	49719
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549725802024313 11/03/22-12:30:57.918358
SID:	2024313
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549715802825766 11/03/22-12:30:31.132672
SID:	2825766
Source Port:	49715
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549719802024313 11/03/22-12:30:42.564459
SID:	2024313
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549710802825766 11/03/22-12:30:18.297577
SID:	2825766
Source Port:	49710
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549734802021641 11/03/22-12:31:25.377976
SID:	2021641
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:	192.168.2.68.8.8.862910532014169 11/03/22-12:30:27.345778
SID:	2014169
Source Port:	62910
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497352025483 11/03/22-12:31:28.883670
SID:	2025483
Source Port:	80
Destination Port:	49735
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549737802021641 11/03/22-12:31:31.046497
SID:	2021641
Source Port:	49737
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497422025483 11/03/22-12:31:43.475626
SID:	2025483
Source Port:	80
Destination Port:	49742
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549714802024313 11/03/22-12:30:27.432237
SID:	2024313
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549711802025381 11/03/22-12:30:20.264286
SID:	2025381
Source Port:	49711
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549722802024313 11/03/22-12:30:50.822444
SID:	2024313
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:	192.168.2.68.8.8.856331532014169 11/03/22-12:30:13.938466
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 11/03/22-12:30:17.960732
SID:	2014169
Source Port:	49448
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 11/03/22-12:30:15.990659
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 11/03/22-12:31:35.521025
SID:	2014169
Source Port:	59752
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549722802024318 11/03/22-12:30:50.822444
SID:	2024318
Source Port:	49722
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549726802021641 11/03/22-12:30:59.657451
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549741802025381 11/03/22-12:31:39.946873
SID:	2025381
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497392025483 11/03/22-12:31:37.318947
SID:	2025483
Source Port:	80
Destination Port:	49739
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549709802021641 11/03/22-12:30:16.075566
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549727802024318 11/03/22-12:31:01.987085
SID:	2024318
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549728802825766 11/03/22-12:31:03.903902
SID:	2825766
Source Port:	49728
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497312025483 11/03/22-12:31:10.691873
SID:	2025483
Source Port:	80
Destination Port:	49731
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 11/03/22-12:30:25.312645
SID:	2014169
Source Port:	65198
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549721802021641 11/03/22-12:30:48.032802
SID:	2021641
Source Port:	49721
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549715802024318 11/03/22-12:30:31.132672
SID:	2024318
Source Port:	49715
Destination Port:	80

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549726802825766 11/03/22-12:30:59.657451
SID:	2825766
Source Port:	49726
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549724802024313 11/03/22-12:30:54.913991
SID:	2024313
Source Port:	49724
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549710802025381 11/03/22-12:30:18.297577
SID:	2025381
Source Port:	49710
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549712802021641 11/03/22-12:30:22.162497
SID:	2021641
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549735802825766 11/03/22-12:31:27.516452
SID:	2825766
Source Port:	49735
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549744802825766 11/03/22-12:31:45.577786
SID:	2825766
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549740802021641 11/03/22-12:31:37.627027
SID:	2021641
Source Port:	49740
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549743802024318 11/03/22-12:31:43.782645
SID:	2024318
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549743802024313 11/03/22-12:31:43.782645
SID:	2024313
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549707802025381 11/03/22-12:30:11.977904
SID:	2025381
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549726802025381 11/03/22-12:30:59.657451
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549725802024318 11/03/22-12:30:57.918358
SID:	2024318
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549707802825766 11/03/22-12:30:11.977904
SID:	2825766
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497342025483 11/03/22-12:31:27.178865
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549731802021641 11/03/22-12:31:09.511791
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:	192.168.2.68.8.8.852481532014169 11/03/22-12:30:53.275834
SID:	2014169
Source Port:	52481
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549720802025381 11/03/22-12:30:45.793165
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:	192.168.2.68.8.8.864404532014169 11/03/22-12:31:43.694917
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549708802025381 11/03/22-12:30:14.035064
SID:	2025381
Source Port:	49708
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549735802021641 11/03/22-12:31:27.516452
SID:	2021641
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549706802024317 11/03/22-12:30:09.785093
SID:	2024317
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497322025483 11/03/22-12:31:21.820409
SID:	2025483
Source Port:	80
Destination Port:	49732
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 11/03/22-12:31:37.538077
SID:	2014169
Source Port:	52865
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549725802825766 11/03/22-12:30:57.918358
SID:	2825766
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497292025483 11/03/22-12:31:07.339016
SID:	2025483
Source Port:	80
Destination Port:	49729
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549724802024318 11/03/22-12:30:54.913991
SID:	2024318
Source Port:	49724
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549706802024312 11/03/22-12:30:09.785093
SID:	2024312
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497212025483 11/03/22-12:30:50.362964
SID:	2025483
Source Port:	80
Destination Port:	49721
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497232025483 11/03/22-12:30:54.557575
SID:	2025483
Source Port:	80
Destination Port:	49723
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549739802025381 11/03/22-12:31:35.606377
SID:	2025381
Source Port:	49739
Destination Port:	80

Copyright Joe Security LLC 2022

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 11/03/22-12:30:30.240421
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549744802021641 11/03/22-12:31:45.577786
SID:	2021641
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549745802025381 11/03/22-12:31:50.569101
SID:	2025381
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549736802025381 11/03/22-12:31:29.221112
SID:	2025381
Source Port:	49736
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549741802021641 11/03/22-12:31:39.946873
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549742802025381 11/03/22-12:31:41.893270
SID:	2025381
Source Port:	49742
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:	192.168.2.68.8.8.862538532014169 11/03/22-12:30:34.919732
SID:	2014169
Source Port:	62538
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 11/03/22-12:30:11.893252
SID:	2014169
Source Port:	58595
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549716802021641 11/03/22-12:30:32.992651
SID:	2021641
Source Port:	49716
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549728802024313 11/03/22-12:31:03.903902
SID:	2024313
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549725802021641 11/03/22-12:30:57.918358
SID:	2021641
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549728802024318 11/03/22-12:31:03.903902
SID:	2024318
Source Port:	49728
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 11/03/22-12:31:47.481296
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549734802024313 11/03/22-12:31:25.377976
SID:	2024313
Source Port:	49734
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549719802021641 11/03/22-12:30:42.564459
SID:	2021641
Source Port:	49719
Destination Port:	80

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549723802025381 11/03/22-12:30:53.367985
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549737802024313 11/03/22-12:31:31.046497
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549740802024313 11/03/22-12:31:37.627027
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549717802025381 11/03/22-12:30:35.019960
SID:	2025381
Source Port:	49717
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549734802024318 11/03/22-12:31:25.377976
SID:	2024318
Source Port:	49734
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497372025483 11/03/22-12:31:32.671321
SID:	2025483
Source Port:	80
Destination Port:	49737
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549716802825766 11/03/22-12:30:32.992651
SID:	2825766
Source Port:	49716
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549722802825766 11/03/22-12:30:50.822444
SID:	2825766
Source Port:	49722
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549722802021641 11/03/22-12:30:50.822444
SID:	2021641
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549740802024318 11/03/22-12:31:37.627027
SID:	2024318
Source Port:	49740
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497402025483 11/03/22-12:31:39.620076
SID:	2025483
Source Port:	80
Destination Port:	49740
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 11/03/22-12:30:20.174105
SID:	2014169
Source Port:	59082
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:	192.168.2.68.8.8.851530532014169 11/03/22-12:30:41.510499
SID:	2014169
Source Port:	51530
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549709802024313 11/03/22-12:30:16.075566
SID:	2024313
Source Port:	49709
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 11/03/22-12:31:29.125849
SID:	2014169
Source Port:	60032
Destination Port:	53

Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497152025483 11/03/22-12:30:32.611167
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549738802021641 11/03/22-12:31:33.019427
SID:	2021641
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549715802024313 11/03/22-12:30:31.132672
SID:	2024313
Source Port:	49715
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497262025483 11/03/22-12:31:00.653288
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549709802024318 11/03/22-12:30:16.075566
SID:	2024318
Source Port:	49709
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 11/03/22-12:31:03.812359
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549718802024318 11/03/22-12:30:37.003049
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549721802024313 11/03/22-12:30:48.032802
SID:	2024313
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549729802825766 11/03/22-12:31:05.707382
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549719802025381 11/03/22-12:30:42.564459
SID:	2025381
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549721802024318 11/03/22-12:30:48.032802
SID:	2024318
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549718802024313 11/03/22-12:30:37.003049
SID:	2024313
Source Port:	49718
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549714802825766 11/03/22-12:30:27.432237
SID:	2825766
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549736802024313 11/03/22-12:31:29.221112
SID:	2024313
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549732802825766 11/03/22-12:31:20.467945
SID:	2825766
Source Port:	49732
Destination Port:	80

Copyright Joe Security LLC 2022

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549743802021641 11/03/22-12:31:43.782645
SID:	2021641
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549740802025381 11/03/22-12:31:37.627027
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549722802025381 11/03/22-12:30:50.822444
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549742802825766 11/03/22-12:31:41.893270
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549731802024318 11/03/22-12:31:09.511791
SID:	2024318
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497432025483 11/03/22-12:31:45.271881
SID:	2025483
Source Port:	80
Destination Port:	49743
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497452025483 11/03/22-12:31:52.163667
SID:	2025483
Source Port:	80
Destination Port:	49745
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549731802024313 11/03/22-12:31:09.511791
SID:	2024313
Source Port:	49731
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497412025483 11/03/22-12:31:41.587643
SID:	2025483
Source Port:	80
Destination Port:	49741
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549714802025381 11/03/22-12:30:27.432237
SID:	2025381
Source Port:	49714
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549713802024318 11/03/22-12:30:25.414440
SID:	2024318
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549737802025381 11/03/22-12:31:31.046497
SID:	2025381
Source Port:	49737
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549709802025381 11/03/22-12:30:16.075566
SID:	2025381
Source Port:	49709
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549737802825766 11/03/22-12:31:31.046497
SID:	2825766
Source Port:	49737
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549736802024318 11/03/22-12:31:29.221112
SID:	2024318
Source Port:	49736
Destination Port:	80

Copyright Joe Security LLC 2022

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549732802025381 11/03/22-12:31:20.467945
SID:	2025381
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549719802825766 11/03/22-12:30:42.564459
SID:	2825766
Source Port:	49719
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 11/03/22-12:30:32.906943
SID:	2014169
Source Port:	63229
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549741802024318 11/03/22-12:31:39.946873
SID:	2024318
Source Port:	49741
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549744802024318 11/03/22-12:31:45.577786
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:	192.168.2.68.8.8.849786532014169 11/03/22-12:30:06.615613
SID:	2014169
Source Port:	49786
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549730802025381 11/03/22-12:31:07.626823
SID:	2025381
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549744802024313 11/03/22-12:31:45.577786
SID:	2024313
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549738802024318 11/03/22-12:31:33.019427
SID:	2024318
Source Port:	49738
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549727802025381 11/03/22-12:31:01.987085
SID:	2025381
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:	192.168.2.68.8.8.856123532014169 11/03/22-12:31:32.930668
SID:	2014169
Source Port:	56123
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549724802025381 11/03/22-12:30:54.913991
SID:	2025381
Source Port:	49724
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549741802024313 11/03/22-12:31:39.946873
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549716802024313 11/03/22-12:30:32.992651
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549713802021641 11/03/22-12:30:25.414440
SID:	2021641
Source Port:	49713
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549723802021641 11/03/22-12:30:53.367985
SID:	2021641
Source Port:	49723
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549707802021641 11/03/22-12:30:11.977904
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549712802825766 11/03/22-12:30:22.162497
SID:	2825766
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549711802024318 11/03/22-12:30:20.264286
SID:	2024318
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549709802825766 11/03/22-12:30:16.075566
SID:	2825766
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549728802021641 11/03/22-12:31:03.903902
SID:	2021641
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549711802024313 11/03/22-12:30:20.264286
SID:	2024313
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549706802825766 11/03/22-12:30:09.785093
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549708802024313 11/03/22-12:30:14.035064
SID:	2024313
Source Port:	49708
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549729802025381 11/03/22-12:31:05.707382
SID:	2025381
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549708802024318 11/03/22-12:30:14.035064
SID:	2024318
Source Port:	49708
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497172025483 11/03/22-12:30:36.516442
SID:	2025483
Source Port:	80
Destination Port:	49717
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549716802024318 11/03/22-12:30:32.992651
SID:	2024318
Source Port:	49716
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549739802825766 11/03/22-12:31:35.606377
SID:	2825766
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:	192.168.2.68.8.8.865044532014169 11/03/22-12:31:27.427876
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549745802021641 11/03/22-12:31:50.569101
SID:	2021641
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549745802825766 11/03/22-12:31:50.569101
SID:	2825766
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549734802825766 11/03/22-12:31:25.377976
SID:	2825766
Source Port:	49734
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549710802021641 11/03/22-12:30:18.297577
SID:	2021641
Source Port:	49710
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497132025483 11/03/22-12:30:26.998667
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549740802825766 11/03/22-12:31:37.627027
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549733802024313 11/03/22-12:31:22.614964
SID:	2024313
Source Port:	49733
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549738802024313 11/03/22-12:31:33.019427
SID:	2024313
Source Port:	49738
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549715802021641 11/03/22-12:30:31.132672
SID:	2021641
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:	192.168.2.68.8.8.856086532014169 11/03/22-12:30:57.832797
SID:	2014169
Source Port:	56086
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549733802024318 11/03/22-12:31:22.614964
SID:	2024318
Source Port:	49733
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497282025483 11/03/22-12:31:05.359036
SID:	2025483
Source Port:	80
Destination Port:	49728
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497202025483 11/03/22-12:30:47.547245
SID:	2025483
Source Port:	80
Destination Port:	49720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497242025483 11/03/22-12:30:57.636605
SID:	2025483
Source Port:	80
Destination Port:	49724
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549735802025381 11/03/22-12:31:27.516452
SID:	2025381
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549727802021641 11/03/22-12:31:01.987085
SID:	2021641
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549720802825766 11/03/22-12:30:45.793165
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:	192.168.2.68.8.8.854903532014169 11/03/22-12:30:36.914690
SID:	2014169
Source Port:	54903
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549718802021641 11/03/22-12:30:37.003049
SID:	2021641
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549739802024313 11/03/22-12:31:35.606377
SID:	2024313
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549736802021641 11/03/22-12:31:29.221112
SID:	2021641
Source Port:	49736
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549739802024318 11/03/22-12:31:35.606377
SID:	2024318
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549717802825766 11/03/22-12:30:35.019960
SID:	2825766
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549725802025381 11/03/22-12:30:57.918358
SID:	2025381
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:	192.168.2.68.8.8.856547532014169 11/03/22-12:30:59.560048
SID:	2014169
Source Port:	56547
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549734802025381 11/03/22-12:31:25.377976
SID:	2025381
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549716802025381 11/03/22-12:30:32.992651
SID:	2025381
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:	192.168.2.68.8.8.859504532014169 11/03/22-12:30:22.044585
SID:	2014169
Source Port:	59504
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497272025483 11/03/22-12:31:03.547635
SID:	2025483
Source Port:	80
Destination Port:	49727
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497362025483 11/03/22-12:31:30.738262
SID:	2025483
Source Port:	80
Destination Port:	49736

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497382025483 11/03/22-12:31:35.287070
SID:	2025483
Source Port:	80
Destination Port:	49738
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549717802021641 11/03/22-12:30:35.019960
SID:	2021641
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549736802825766 11/03/22-12:31:29.221112
SID:	2825766
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549743802025381 11/03/22-12:31:43.782645
SID:	2025381
Source Port:	49743
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 11/03/22-12:30:47.939957
SID:	2014169
Source Port:	52556
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549723802024313 11/03/22-12:30:53.367985
SID:	2024313
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549715802025381 11/03/22-12:30:31.132672
SID:	2025381
Source Port:	49715
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549708802825766 11/03/22-12:30:14.035064
SID:	2825766
Source Port:	49708
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549742802024313 11/03/22-12:31:41.893270
SID:	2024313
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549744802025381 11/03/22-12:31:45.577786
SID:	2025381
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549729802024318 11/03/22-12:31:05.707382
SID:	2024318
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	−
Timestamp:	91.142.77.45192.168.2.680497302025483 11/03/22-12:31:09.196542
SID:	2025483
Source Port:	80
Destination Port:	49730
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549742802024318 11/03/22-12:31:41.893270
SID:	2024318
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549729802024313 11/03/22-12:31:05.707382
SID:	2024313
Source Port:	49729
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549730802021641 11/03/22-12:31:07.626823
SID:	2021641
Source Port:	49730
Destination Port:	80

Copyright Joe Security LLC 2022

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549743802825766 11/03/22-12:31:43.782645
SID:	2825766
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497252025483 11/03/22-12:30:59.345748
SID:	2025483
Source Port:	80
Destination Port:	49725
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549707802024312 11/03/22-12:30:11.977904
SID:	2024312
Source Port:	49707
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549732802024318 11/03/22-12:31:20.467945
SID:	2024318
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:	192.168.2.68.8.8.862520532014169 11/03/22-12:31:07.541345
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 11/03/22-12:31:39.862228
SID:	2014169
Source Port:	57322
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549707802024317 11/03/22-12:30:11.977904
SID:	2024317
Source Port:	49707
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549732802024313 11/03/22-12:31:20.467945
SID:	2024313
Source Port:	49732
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549713802024313 11/03/22-12:30:25.414440
SID:	2024313
Source Port:	49713
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549726802024318 11/03/22-12:30:59.657451
SID:	2024318
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549724802825766 11/03/22-12:30:54.913991
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549727802825766 11/03/22-12:31:01.987085
SID:	2825766
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549720802021641 11/03/22-12:30:45.793165
SID:	2021641
Source Port:	49720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549718802825766 11/03/22-12:30:37.003049
SID:	2825766
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: 91.142.77.45	−
Timestamp:	192.168.2.691.142.77.4549723802024318 11/03/22-12:30:53.367985
SID:	2024318
Source Port:	49723
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549711802021641 11/03/22-12:30:20.264286
SID:	2021641
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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549730802825766 11/03/22-12:31:07.626823
SID:	2825766
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497442025483 11/03/22-12:31:47.249314
SID:	2025483
Source Port:	80
Destination Port:	49744
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549708802021641 11/03/22-12:30:14.035064
SID:	2021641
Source Port:	49708
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497192025483 11/03/22-12:30:45.376826
SID:	2025483
Source Port:	80
Destination Port:	49719
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497082025483 11/03/22-12:30:15.684954
SID:	2025483
Source Port:	80
Destination Port:	49708
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497332025483 11/03/22-12:31:25.021802
SID:	2025483
Source Port:	80
Destination Port:	49733
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549733802825766 11/03/22-12:31:22.614964
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549714802021641 11/03/22-12:30:27.432237
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549726802024313 11/03/22-12:30:59.657451
SID:	2024313
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6

Timestamp:	91.142.77.45192.168.2.680497112025483 11/03/22-12:30:21.541561
SID:	2025483
Source Port:	80
Destination Port:	49711
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:	192.168.2.68.8.8.852079532014169 11/03/22-12:31:11.161882
SID:	2014169
Source Port:	52079
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549710802024313 11/03/22-12:30:18.297577
SID:	2024313
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549712802025381 11/03/22-12:30:22.162497
SID:	2025381
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: 91.142.77.45

Timestamp:	192.168.2.691.142.77.4549710802024318 11/03/22-12:30:18.297577
SID:	2024318
Source Port:	49710
Destination Port:	80

Copyright Joe Security LLC 2022

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: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549745802024318 11/03/22-12:31:50.569101
SID:	2024318
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:	192.168.2.68.8.8.861833532014169 11/03/22-12:31:25.278309
SID:	2014169
Source Port:	61833
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549733802021641 11/03/22-12:31:22.614964
SID:	2021641
Source Port:	49733
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549706802025381 11/03/22-12:30:09.785093
SID:	2025381
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.2.6 - Destination IP: 91.142.77.45	
Timestamp:	192.168.2.691.142.77.4549711802825766 11/03/22-12:30:20.264286
SID:	2825766
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Fake 404 Response - Source IP: 91.142.77.45 - Destination IP: 192.168.2.6	
Timestamp:	91.142.77.45192.168.2.680497222025483 11/03/22-12:30:53.023996
SID:	2025483
Source Port:	80
Destination Port:	49722
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

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

Data Obfuscation



Yara detected aPLib compressed binary

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection



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

Malware Analysis System Evasion



Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion



Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

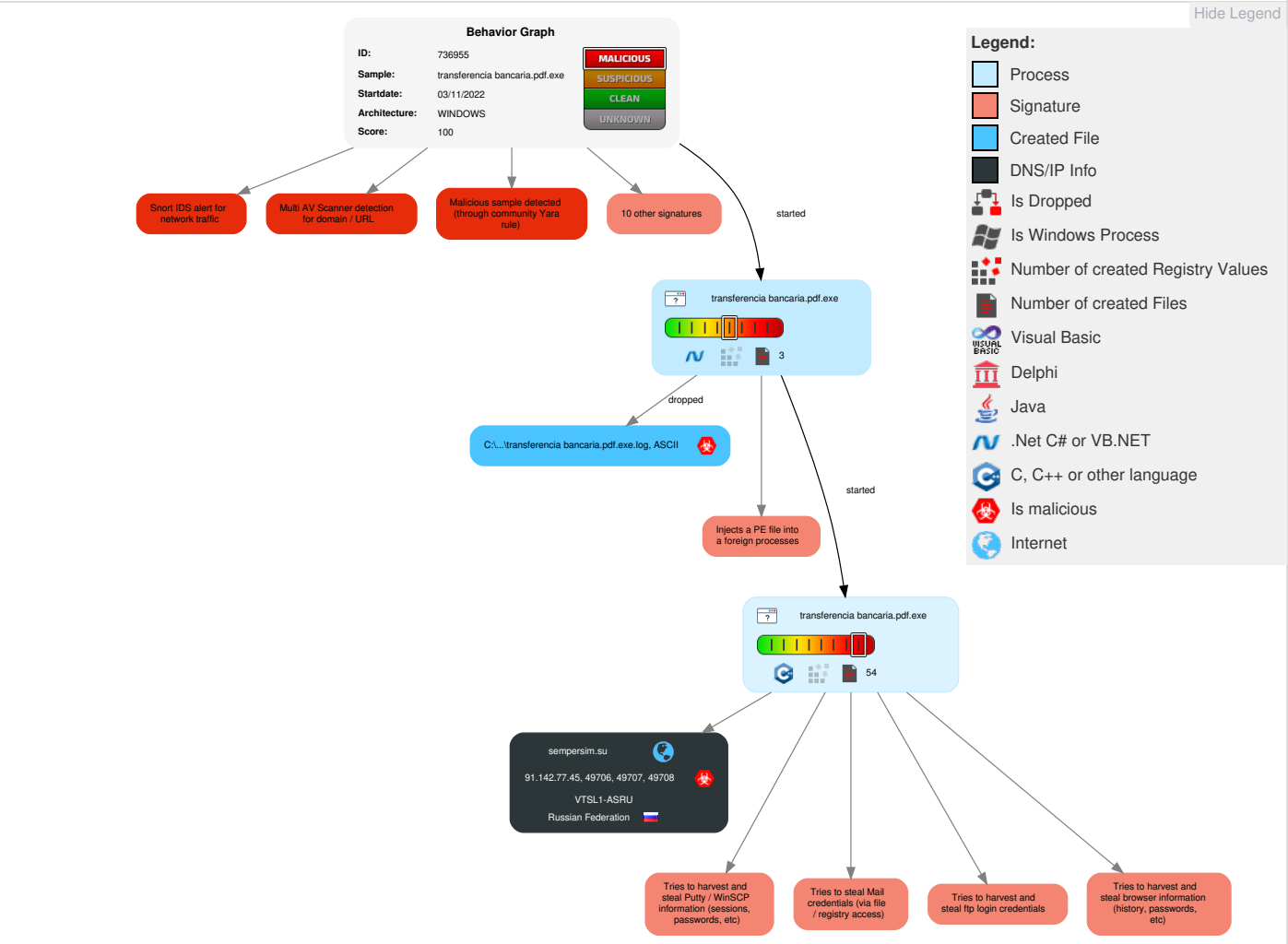
Tries to harvest and steal browser information (history, passwords, etc)

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 1 1 Process Injection	1 1 Masquerading	2 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Credentials in Registry	2 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 1 2 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 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Obfuscated Files or Information	LSA Secrets	Remote System 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	1 3 Software Packing	Cached Domain Credentials	System Owner/User 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	1 Timestomp	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

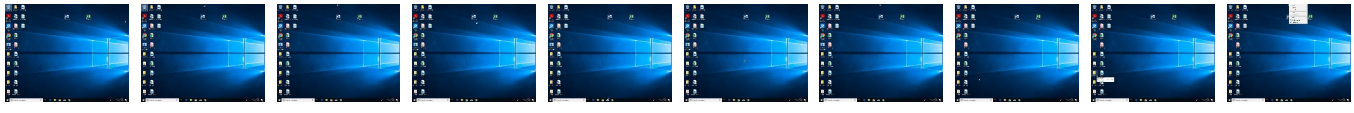
Behavior Graph

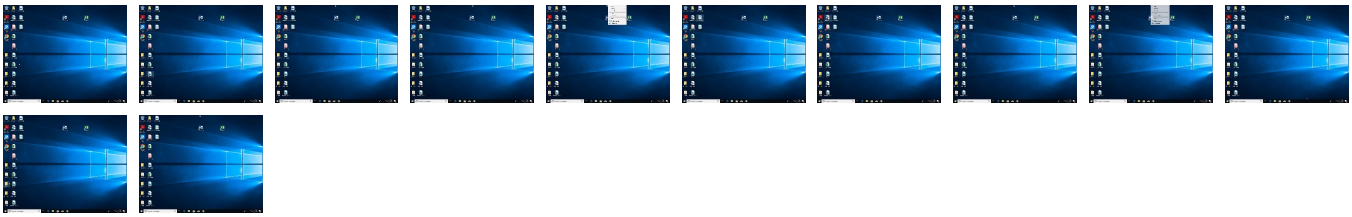


Screenshots

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
transferencia bancaria.pdf.exe	12%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
transferencia bancaria.pdf.exe	21%	Virustotal		Browse
transferencia bancaria.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.transferencia bancaria.pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.transferencia bancaria.pdf.exe.44458b0.13.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.transferencia bancaria.pdf.exe.442b890.12.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
sempersim.su	21%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://alphastand.top/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://www.tiro.com	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://sempersim.su/gl21/fre.php	0%	Avira URL Cloud	safe	
http://sempersim.su/gl21/fre.php	19%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sempersim.su	91.142.77.45	true	true	• 21%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown

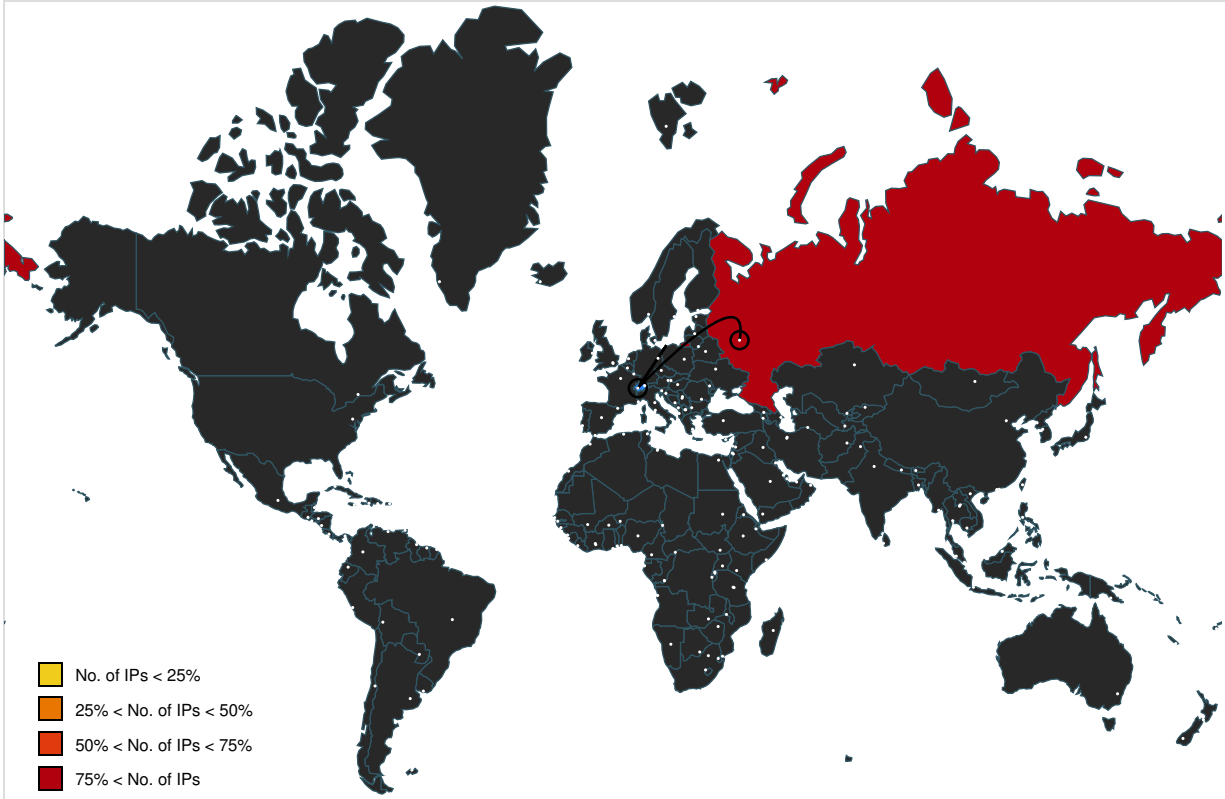
Name	Malicious	Antivirus Detection	Reputation
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://sempersim.su/gl21/fre.php	true	• 19%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ibsensoftware.com/	transferencia bancaria.pdf.exe, 00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp, transferencia bancaria.pdf.exe, 00000000.00000002.290985684.000000000442B000.00000004.00000800.00020000.00000000.sdmp, transferencia bancaria.pdf.exe, 00000000.00000002.291086969.0000000004445000.00000004.00000800.00020000.00000000.sdmp, transferencia bancaria.pdf.exe, 00000001.00000000.275310547.0000000000415000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	transferencia bancaria.pdf.exe, 00000000.00000002.294758334.00000000073E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.142.77.45	sempersim.su	Russian Federation		48720	VTSL1-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736955
Start date and time:	2022-11-03 12:28:50 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 37s
Hypervisor based Inspection enabled:	false
Report type:	light

Copyright Joe Security LLC 2022

Sample file name:	transferencia bancaria.pdf.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:	13
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@3/3@40/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
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, SgrmBroker.exe, conhost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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
12:29:57	API Interceptor	38x Sleep call for process: transferencia bancaria.pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\transferencia bancaria.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\Desktop\transferencia bancaria.pdf.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\Desktop\transferencia bancaria.pdf.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

Reputation:	moderate, very likely benign file
Preview:	.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.908301217464369
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	transferencia bancaria.pdf.exe
File size:	811008
MD5:	355efb2e1f7dd361f8e7cda449a45eac
SHA1:	864f8d367c72d37347e2dc8fa799cc9a2550d66c
SHA256:	cb90ea9b90ccb675d555891bcbfb224edf1bbfe7a650e9600508c93660ec09eb
SHA512:	696a0d695e86094c35abf41001c607fa3df61bbf5cb7bf11feadd4bd434a67ce31628106c71688e8782f4e326e71aaced83b031764c4214832df455329edc8c5
SSDEEP:	12288:dR/AN9w7DTlJ0ycSou3KRdwHDl3tRG/8wSRDfs2sFLTAehm8buS89W:3XXEyycSDAwHNi8TAqbD
TLSH:	8005E00F8AE6460ED66936B865F0EFB75799DC01F44BC35B17CA6E4BB8432308211BD9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....|#.....0..X.....v... .....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c761e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xA9237CA5 [Wed Dec 3 11:06:13 2059 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc75cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x370	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc75b0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc5624	0xc5800	False	0.712665644778481	data	6.915983824184794	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xc8000	0x370	0x400	False	0.365234375	data	2.7841237517285475	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc8058	0x314	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.4549712802024318 11/03/22-12:30:22.162497	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49712	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.4549727802024313 11/03/22-12:31:01.987085	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49727	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.4549723802825766 11/03/22-12:30:53.367985	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49723	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.4549724802021641 11/03/22-12:30:54.913991	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49724	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8.859881532014169 11/03/22-12:31:01.170102	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59881	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8.856122532014169 11/03/22-12:30:45.704907	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56122	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.4549741802825766 11/03/22-12:31:39.946873	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49741	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.4549745802024313 11/03/22-12:31:50.569101	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49745	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.4549728802025381 11/03/22-12:31:03.903902	TCP	2025381	ET TROJAN LokiBot Checkin	49728	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.4549739802021641 11/03/22-12:31:35.606377	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49739	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.4549738802825766 11/03/22-12:31:33.019427	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49738	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.4549713802025381 11/03/22-12:30:25.414440	TCP	2025381	ET TROJAN LokiBot Checkin	49713	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9731802025381 11/03/22-12:31:09.511791	TCP	2025381	ET TROJAN LokiBot Checkin	49731	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9737802024318 11/03/22-12:31:31.046497	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49737	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9713802825766 11/03/22-12:30:25.414440	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49713	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497182025483 11/03/22-12:30:41.067853	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49718	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497092025483 11/03/22-12:30:17.656419	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49709	91.142.77.45	192.168.2.6
192.168.2.68.8.8.8.8503435 32014169 11/03/22-12:31:05.602892	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	50343	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9717802024318 11/03/22-12:30:35.019960	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49717	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9717802024313 11/03/22-12:30:35.019960	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49717	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8.8565695 32014169 11/03/22-12:31:22.519121	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56569	53	192.168.2.6	8.8.8.8
91.142.77.45192.168.2.68 0497122025483 11/03/22-12:30:23.556931	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49712	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9729802021641 11/03/22-12:31:05.707382	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49729	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9742802021641 11/03/22-12:31:41.893270	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49742	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8.8539435 32014169 11/03/22-12:30:54.819244	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	53943	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9730802024318 11/03/22-12:31:07.626823	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49730	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497102025483 11/03/22-12:30:19.791139	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49710	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9735802024313 11/03/22-12:31:27.516452	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49735	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9721802025381 11/03/22-12:30:48.032802	TCP	2025381	ET TROJAN LokiBot Checkin	49721	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8.8556295 32014169 11/03/22-12:31:09.419344	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55629	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9731802825766 11/03/22-12:31:09.511791	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49731	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9738802025381 11/03/22-12:31:33.019427	TCP	2025381	ET TROJAN LokiBot Checkin	49738	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9712802024313 11/03/22-12:30:22.162497	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49712	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497142025483 11/03/22-12:30:29.899760	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49714	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497162025483 11/03/22-12:30:34.572782	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49716	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9706802021641 11/03/22-12:30:09.785093	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49706	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9730802024313 11/03/22-12:31:07.626823	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49730	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8616095 32014169 11/03/22-12:30:50.734926	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61609	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8629585 32014169 11/03/22-12:31:41.802948	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62958	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9735802024318 11/03/22-12:31:27.516452	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49735	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8492325 32014169 11/03/22-12:31:30.955921	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49232	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8628485 32014169 11/03/22-12:31:45.492508	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62848	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9733802025381 11/03/22-12:31:22.614964	TCP	2025381	ET TROJAN LokiBot Checkin	49733	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9732802021641 11/03/22-12:31:20.467945	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49732	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9720802024318 11/03/22-12:30:45.793165	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49720	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9718802025381 11/03/22-12:30:37.003049	TCP	2025381	ET TROJAN LokiBot Checkin	49718	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9721802825766 11/03/22-12:30:48.032802	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49721	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9720802024313 11/03/22-12:30:45.793165	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49720	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9714802024318 11/03/22-12:30:27.432237	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49714	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9719802024318 11/03/22-12:30:42.564459	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49719	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9725802024313 11/03/22-12:30:57.918358	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49725	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9715802825766 11/03/22-12:30:31.132672	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49715	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9719802024313 11/03/22-12:30:42.564459	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49719	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9710802825766 11/03/22-12:30:18.297577	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49710	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9734802021641 11/03/22-12:31:25.377976	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49734	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8629105 32014169 11/03/22-12:30:27.345778	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62910	53	192.168.2.6	8.8.8.8
91.142.77.45192.168.2.68 0497352025483 11/03/22-12:31:28.883670	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49735	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9737802021641 11/03/22-12:31:31.046497	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49737	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497422025483 11/03/22-12:31:43.475626	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49742	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9714802024313 11/03/22-12:30:27.432237	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49714	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9711802025381 11/03/22-12:30:20.264286	TCP	2025381	ET TROJAN LokiBot Checkin	49711	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9722802024313 11/03/22-12:30:50.822444	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49722	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8563315 32014169 11/03/22-12:30:13.938466	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 11/03/22-12:30:17.960732	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49448	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8505065 32014169 11/03/22-12:30:15.990659	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 11/03/22-12:31:35.521025	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59752	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9722802024318 11/03/22-12:30:50.822444	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49722	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9726802021641 11/03/22-12:30:59.657451	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49726	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9741802025381 11/03/22-12:31:39.946873	TCP	2025381	ET TROJAN LokiBot Checkin	49741	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497392025483 11/03/22-12:31:37.318947	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49739	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9709802021641 11/03/22-12:30:16.075566	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49709	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9727802024318 11/03/22-12:31:01.987085	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49727	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9728802825766 11/03/22-12:31:03.903902	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49728	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497312025483 11/03/22-12:31:10.691873	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49731	91.142.77.45	192.168.2.6
192.168.2.68.8.8.8651985 32014169 11/03/22-12:30:25.312645	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	65198	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9721802021641 11/03/22-12:30:48.032802	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49721	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9715802024318 11/03/22-12:30:31.132672	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49715	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9726802825766 11/03/22-12:30:59.657451	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49726	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9724802024313 11/03/22-12:30:54.913991	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49724	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9710802025381 11/03/22-12:30:18.297577	TCP	2025381	ET TROJAN LokiBot Checkin	49710	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9712802021641 11/03/22-12:30:22.162497	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49712	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9735802825766 11/03/22-12:31:27.516452	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49735	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9744802825766 11/03/22-12:31:45.577786	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49744	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9740802021641 11/03/22-12:31:37.627027	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49740	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9743802024318 11/03/22-12:31:43.782645	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49743	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9743802024313 11/03/22-12:31:43.782645	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49743	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9707802025381 11/03/22-12:30:11.977904	TCP	2025381	ET TROJAN LokiBot Checkin	49707	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9726802025381 11/03/22-12:30:59.657451	TCP	2025381	ET TROJAN LokiBot Checkin	49726	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9725802024318 11/03/22-12:30:57.918358	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49725	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9707802825766 11/03/22-12:30:11.977904	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49707	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497342025483 11/03/22-12:31:27.178865	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49734	91.142.77.45	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9731802021641 11/03/22-12:31:09.511791	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49731	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8524815 32014169 11/03/22-12:30:53.275834	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52481	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9720802025381 11/03/22-12:30:45.793165	TCP	2025381	ET TROJAN LokiBot Checkin	49720	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8644045 32014169 11/03/22-12:31:43.694917	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	64404	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9708802025381 11/03/22-12:30:14.035064	TCP	2025381	ET TROJAN LokiBot Checkin	49708	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9735802021641 11/03/22-12:31:27.516452	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49735	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9706802024317 11/03/22-12:30:09.785093	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49706	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497322025483 11/03/22-12:31:21.820409	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49732	91.142.77.45	192.168.2.6
192.168.2.68.8.8.8528655 32014169 11/03/22-12:31:37.538077	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52865	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9725802825766 11/03/22-12:30:57.918358	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49725	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497292025483 11/03/22-12:31:07.339016	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49729	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9724802024318 11/03/22-12:30:54.913991	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49724	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9706802024312 11/03/22-12:30:09.785093	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49706	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497212025483 11/03/22-12:30:50.362964	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49721	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497232025483 11/03/22-12:30:54.557575	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49723	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9739802025381 11/03/22-12:31:35.606377	TCP	2025381	ET TROJAN LokiBot Checkin	49739	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8638635 32014169 11/03/22-12:30:30.240421	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63863	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9744802021641 11/03/22-12:31:45.577786	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9745802025381 11/03/22-12:31:50.569101	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9736802025381 11/03/22-12:31:29.221112	TCP	2025381	ET TROJAN LokiBot Checkin	49736	80	192.168.2.6	91.142.77.45

Copyright Joe Security LLC 2022

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9741802021641 11/03/22-12:31:39.946873	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49741	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9742802025381 11/03/22-12:31:41.893270	TCP	2025381	ET TROJAN LokiBot Checkin	49742	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8625385 32014169 11/03/22-12:30:34.919732	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	62538	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8585955 32014169 11/03/22-12:30:11.893252	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58595	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9716802021641 11/03/22-12:30:32.992651	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49716	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9728802024313 11/03/22-12:31:03.903902	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49728	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9725802021641 11/03/22-12:30:57.918358	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49725	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9728802024318 11/03/22-12:31:03.903902	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49728	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8559565 32014169 11/03/22-12:31:47.481296	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	55956	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9734802024313 11/03/22-12:31:25.377976	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49734	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9719802021641 11/03/22-12:30:42.564459	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49719	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9723802025381 11/03/22-12:30:53.367985	TCP	2025381	ET TROJAN LokiBot Checkin	49723	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9737802024313 11/03/22-12:31:31.046497	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49737	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9740802024313 11/03/22-12:31:37.627027	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49740	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9717802025381 11/03/22-12:30:35.019960	TCP	2025381	ET TROJAN LokiBot Checkin	49717	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9734802024318 11/03/22-12:31:25.377976	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49734	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497372025483 11/03/22-12:31:32.671321	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49737	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9716802825766 11/03/22-12:30:32.992651	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49716	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9722802825766 11/03/22-12:30:50.822444	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49722	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9722802021641 11/03/22-12:30:50.822444	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49722	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9740802024318 11/03/22-12:31:37.627027	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49740	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497402025483 11/03/22-12:31:39.620076	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49740	91.142.77.45	192.168.2.6
192.168.2.68.8.8.8590825 32014169 11/03/22-12:30:20.174105	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59082	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8515305 32014169 11/03/22-12:30:41.510499	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	51530	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9709802024313 11/03/22-12:30:16.075566	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49709	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8600325 32014169 11/03/22-12:31:29.125849	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	60032	53	192.168.2.6	8.8.8.8
91.142.77.45192.168.2.68 0497152025483 11/03/22-12:30:32.611167	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49715	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9738802021641 11/03/22-12:31:33.019427	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49738	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9715802024313 11/03/22-12:30:31.132672	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49715	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497262025483 11/03/22-12:31:00.653288	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49726	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9709802024318 11/03/22-12:30:16.075566	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49709	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8589175 32014169 11/03/22-12:31:03.812359	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	58917	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9718802024318 11/03/22-12:30:37.003049	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49718	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9721802024313 11/03/22-12:30:48.032802	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49721	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9729802825766 11/03/22-12:31:05.707382	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49729	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9719802025381 11/03/22-12:30:42.564459	TCP	2025381	ET TROJAN LokiBot Checkin	49719	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9721802024318 11/03/22-12:30:48.032802	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49721	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9718802024313 11/03/22-12:30:37.003049	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49718	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9714802825766 11/03/22-12:30:27.432237	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49714	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9736802024313 11/03/22-12:31:29.221112	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49736	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9732802825766 11/03/22-12:31:20.467945	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49732	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9743802021641 11/03/22-12:31:43.782645	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9740802025381 11/03/22-12:31:37.627027	TCP	2025381	ET TROJAN LokiBot Checkin	49740	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9722802025381 11/03/22-12:30:50.822444	TCP	2025381	ET TROJAN LokiBot Checkin	49722	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9742802825766 11/03/22-12:31:41.893270	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49742	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9731802024318 11/03/22-12:31:09.511791	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49731	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497432025483 11/03/22-12:31:45.271881	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49743	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497452025483 11/03/22-12:31:52.163667	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49745	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9731802024313 11/03/22-12:31:09.511791	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49731	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497412025483 11/03/22-12:31:41.587643	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49741	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9714802025381 11/03/22-12:30:27.432237	TCP	2025381	ET TROJAN LokiBot Checkin	49714	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9713802024318 11/03/22-12:30:25.414440	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49713	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9737802025381 11/03/22-12:31:31.046497	TCP	2025381	ET TROJAN LokiBot Checkin	49737	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9709802025381 11/03/22-12:30:16.075566	TCP	2025381	ET TROJAN LokiBot Checkin	49709	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9737802825766 11/03/22-12:31:31.046497	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49737	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9736802024318 11/03/22-12:31:29.221112	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49736	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9732802025381 11/03/22-12:31:20.467945	TCP	2025381	ET TROJAN LokiBot Checkin	49732	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9719802825766 11/03/22-12:30:42.564459	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49719	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8632295 32014169 11/03/22-12:30:32.906943	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	63229	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9741802024318 11/03/22-12:31:39.946873	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49741	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9744802024318 11/03/22-12:31:45.577786	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49744	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8497865 32014169 11/03/22-12:30:06.615613	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	49786	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9730802025381 11/03/22-12:31:07.626823	TCP	2025381	ET TROJAN LokiBot Checkin	49730	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9744802024313 11/03/22-12:31:45.577786	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49744	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9738802024318 11/03/22-12:31:33.019427	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49738	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9727802025381 11/03/22-12:31:01.987085	TCP	2025381	ET TROJAN LokiBot Checkin	49727	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8561235 32014169 11/03/22-12:31:32.930668	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56123	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9724802025381 11/03/22-12:30:54.913991	TCP	2025381	ET TROJAN LokiBot Checkin	49724	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9741802024313 11/03/22-12:31:39.946873	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49741	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9716802024313 11/03/22-12:30:32.992651	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49716	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9713802021641 11/03/22-12:30:25.414440	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49713	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9723802021641 11/03/22-12:30:53.367985	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49723	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9707802021641 11/03/22-12:30:11.977904	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49707	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9712802825766 11/03/22-12:30:22.162497	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49712	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9711802024318 11/03/22-12:30:20.264286	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49711	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9709802825766 11/03/22-12:30:16.075566	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49709	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9728802021641 11/03/22-12:31:03.903902	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49728	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9711802024313 11/03/22-12:30:20.264286	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49711	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9706802825766 11/03/22-12:30:09.785093	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49706	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9708802024313 11/03/22-12:30:14.035064	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49708	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9729802025381 11/03/22-12:31:05.707382	TCP	2025381	ET TROJAN LokiBot Checkin	49729	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9708802024318 11/03/22-12:30:14.035064	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49708	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497172025483 11/03/22-12:30:36.516442	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49717	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9716802024318 11/03/22-12:30:32.992651	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49716	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9739802825766 11/03/22-12:31:35.606377	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49739	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8.8650445 32014169 11/03/22-12:31:27.427876	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	65044	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9745802021641 11/03/22-12:31:50.569101	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9745802825766 11/03/22-12:31:50.569101	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49745	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9734802825766 11/03/22-12:31:25.377976	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49734	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9710802021641 11/03/22-12:30:18.297577	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49710	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497132025483 11/03/22-12:30:26.998667	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49713	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9740802825766 11/03/22-12:31:37.627027	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49740	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9733802024313 11/03/22-12:31:22.614964	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49733	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9738802024313 11/03/22-12:31:33.019427	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49738	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9715802021641 11/03/22-12:30:31.132672	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49715	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8.8560865 32014169 11/03/22-12:30:57.832797	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56086	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9733802024318 11/03/22-12:31:22.614964	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49733	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497282025483 11/03/22-12:31:05.359036	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49728	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497202025483 11/03/22-12:30:47.547245	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49720	91.142.77.45	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
91.142.77.45192.168.2.68 0497242025483 11/03/22-12:30:57.636605	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49724	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9735802025381 11/03/22-12:31:27.516452	TCP	2025381	ET TROJAN LokiBot Checkin	49735	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9727802021641 11/03/22-12:31:01.987085	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49727	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9720802825766 11/03/22-12:30:45.793165	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49720	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8549035 32014169 11/03/22-12:30:36.914690	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	54903	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9718802021641 11/03/22-12:30:37.003049	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49718	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9739802024313 11/03/22-12:31:35.606377	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49739	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9736802021641 11/03/22-12:31:29.221112	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49736	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9739802024318 11/03/22-12:31:35.606377	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49739	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9717802825766 11/03/22-12:30:35.019960	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49717	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9725802025381 11/03/22-12:30:57.918358	TCP	2025381	ET TROJAN LokiBot Checkin	49725	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8565475 32014169 11/03/22-12:30:59.560048	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	56547	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9734802025381 11/03/22-12:31:25.377976	TCP	2025381	ET TROJAN LokiBot Checkin	49734	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9716802025381 11/03/22-12:30:32.992651	TCP	2025381	ET TROJAN LokiBot Checkin	49716	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8595045 32014169 11/03/22-12:30:22.044585	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	59504	53	192.168.2.6	8.8.8.8
91.142.77.45192.168.2.68 0497272025483 11/03/22-12:31:03.547635	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49727	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497362025483 11/03/22-12:31:30.738262	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49736	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497382025483 11/03/22-12:31:35.287070	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49738	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9717802021641 11/03/22-12:30:35.019960	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49717	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9736802825766 11/03/22-12:31:29.221112	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49736	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9743802025381 11/03/22-12:31:43.782645	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8525565 32014169 11/03/22-12:30:47.939957	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52556	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9723802024313 11/03/22-12:30:53.367985	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49723	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9715802025381 11/03/22-12:30:31.132672	TCP	2025381	ET TROJAN LokiBot Checkin	49715	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9708802825766 11/03/22-12:30:14.035064	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49708	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9742802024313 11/03/22-12:31:41.893270	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49742	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9744802025381 11/03/22-12:31:45.577786	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9729802024318 11/03/22-12:31:05.707382	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49729	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497302025483 11/03/22-12:31:09.196542	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49730	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9742802024318 11/03/22-12:31:41.893270	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49742	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9729802024313 11/03/22-12:31:05.707382	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49729	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9730802021641 11/03/22-12:31:07.626823	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49730	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9743802825766 11/03/22-12:31:43.782645	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49743	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497252025483 11/03/22-12:30:59.345748	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49725	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9707802024312 11/03/22-12:30:11.977904	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49707	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9732802024318 11/03/22-12:31:20.467945	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49732	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8625205 32014169 11/03/22-12:31:07.541345	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 11/03/22-12:31:39.862228	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57322	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9707802024317 11/03/22-12:30:11.977904	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49707	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9732802024313 11/03/22-12:31:20.467945	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49732	80	192.168.2.6	91.142.77.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9713802024313 11/03/22-12:30:25.414440	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49713	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9726802024318 11/03/22-12:30:59.657451	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49726	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9724802825766 11/03/22-12:30:54.913991	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49724	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9727802825766 11/03/22-12:31:01.987085	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49727	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9720802021641 11/03/22-12:30:45.793165	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49720	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9718802825766 11/03/22-12:30:37.003049	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49718	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9723802024318 11/03/22-12:30:53.367985	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49723	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9711802021641 11/03/22-12:30:20.264286	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49711	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9730802825766 11/03/22-12:31:07.626823	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49730	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497442025483 11/03/22-12:31:47.249314	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49744	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9708802021641 11/03/22-12:30:14.035064	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49708	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497192025483 11/03/22-12:30:45.376826	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49719	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497082025483 11/03/22-12:30:15.684954	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49708	91.142.77.45	192.168.2.6
91.142.77.45192.168.2.68 0497332025483 11/03/22-12:31:25.021802	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49733	91.142.77.45	192.168.2.6
192.168.2.691.142.77.454 9733802825766 11/03/22-12:31:22.614964	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49733	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9714802021641 11/03/22-12:30:27.432237	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49714	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9726802024313 11/03/22-12:30:59.657451	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49726	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497112025483 11/03/22-12:30:21.541561	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49711	91.142.77.45	192.168.2.6
192.168.2.68.8.8.8520795 32014169 11/03/22-12:31:11.161882	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	52079	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.142.77.454 9710802024313 11/03/22-12:30:18.297577	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49710	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9712802025381 11/03/22-12:30:22.162497	TCP	2025381	ET TROJAN LokiBot Checkin	49712	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9710802024318 11/03/22-12:30:18.297577	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49710	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9745802024318 11/03/22-12:31:50.569101	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49745	80	192.168.2.6	91.142.77.45
192.168.2.68.8.8.8618335 32014169 11/03/22-12:31:25.278309	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	61833	53	192.168.2.6	8.8.8.8
192.168.2.691.142.77.454 9733802021641 11/03/22-12:31:22.614964	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49733	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9706802025381 11/03/22-12:30:09.785093	TCP	2025381	ET TROJAN LokiBot Checkin	49706	80	192.168.2.6	91.142.77.45
192.168.2.691.142.77.454 9711802825766 11/03/22-12:30:20.264286	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49711	80	192.168.2.6	91.142.77.45
91.142.77.45192.168.2.68 0497222025483 11/03/22-12:30:53.023996	TCP	2025483	ET TROJAN LokiBot Fake 404 Response	80	49722	91.142.77.45	192.168.2.6

Network Port Distribution



Total Packets: 98

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:30:06.648422003 CET	49706	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:09.705056906 CET	49706	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:09.767577887 CET	80	49706	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:09.767824888 CET	49706	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:09.785093069 CET	49706	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:09.847585917 CET	80	49706	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:09.847696066 CET	49706	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:09.911494017 CET	80	49706	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:11.378333092 CET	80	49706	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:11.378524065 CET	49706	80	192.168.2.6	91.142.77.45

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:30:11.378582001 CET	49706	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:11.441195965 CET	80	49706	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:11.912462950 CET	49707	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:11.974523067 CET	80	49707	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:11.974664927 CET	49707	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:11.977904081 CET	49707	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:12.039987087 CET	80	49707	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:12.040091991 CET	49707	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:12.102111101 CET	80	49707	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:13.686108112 CET	80	49707	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:13.686407089 CET	49707	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:13.689996004 CET	49707	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:13.752177954 CET	80	49707	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:13.960999012 CET	49708	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:14.024719000 CET	80	49708	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:14.024915934 CET	49708	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:14.035063982 CET	49708	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:14.097285032 CET	80	49708	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:14.097431898 CET	49708	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:14.159482002 CET	80	49708	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:15.684953928 CET	80	49708	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:15.685059071 CET	49708	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:15.685152054 CET	49708	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:15.747353077 CET	80	49708	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:16.009772062 CET	49709	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:16.071901083 CET	80	49709	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:16.072161913 CET	49709	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:16.075566053 CET	49709	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:16.137646914 CET	80	49709	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:16.137861967 CET	49709	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:16.199959040 CET	80	49709	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:17.656419039 CET	80	49709	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:17.656625032 CET	49709	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:17.656876087 CET	49709	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:17.718825102 CET	80	49709	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:18.232103109 CET	49710	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:18.294275999 CET	80	49710	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:18.294435978 CET	49710	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:18.297576904 CET	49710	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:18.359631062 CET	80	49710	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:18.359889030 CET	49710	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:18.666949987 CET	49710	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:18.729307890 CET	80	49710	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:19.791138887 CET	80	49710	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:19.791312933 CET	49710	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:19.791399956 CET	49710	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:19.853351116 CET	80	49710	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:20.195004940 CET	49711	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:20.257170916 CET	80	49711	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:20.260675907 CET	49711	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:20.264286041 CET	49711	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:20.326256037 CET	80	49711	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:20.327415943 CET	49711	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:20.389652014 CET	80	49711	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:21.541560888 CET	80	49711	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:21.541733980 CET	49711	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:21.541781902 CET	49711	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:21.854696989 CET	49711	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:22.066165924 CET	49712	80	192.168.2.6	91.142.77.45

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:30:22.128371954 CET	80	49712	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:22.128586054 CET	49712	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:22.162497044 CET	49712	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:22.224786043 CET	80	49712	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:22.224951029 CET	49712	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:22.287046909 CET	80	49712	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:22.464206934 CET	49711	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:22.527188063 CET	80	49711	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:23.556931019 CET	80	49712	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:23.557039022 CET	49712	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:23.557166100 CET	49712	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:23.619096041 CET	80	49712	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:25.335967064 CET	49713	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:25.401177883 CET	80	49713	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:25.401310921 CET	49713	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:25.414439917 CET	49713	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:25.476397991 CET	80	49713	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:25.476478100 CET	49713	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:25.538403988 CET	80	49713	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:26.998667002 CET	80	49713	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:27.002180099 CET	49713	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:27.002180099 CET	49713	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:27.064440012 CET	80	49713	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:27.367080927 CET	49714	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:27.428744078 CET	80	49714	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:27.428901911 CET	49714	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:27.432236910 CET	49714	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:27.493885994 CET	80	49714	91.142.77.45	192.168.2.6
Nov 3, 2022 12:30:27.493982077 CET	49714	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:27.886517048 CET	49714	80	192.168.2.6	91.142.77.45
Nov 3, 2022 12:30:28.386557102 CET	49714	80	192.168.2.6	91.142.77.45

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:30:06.615612984 CET	49786	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:06.635174990 CET	53	49786	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:11.893251896 CET	58595	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:11.910538912 CET	53	58595	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:13.938466072 CET	56331	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:13.958684921 CET	53	56331	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:15.990658998 CET	50506	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:16.008389950 CET	53	50506	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:17.960731983 CET	49448	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:18.222553015 CET	53	49448	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:20.174104929 CET	59082	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:20.193391085 CET	53	59082	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:22.044584990 CET	59504	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:22.064102888 CET	53	59504	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:25.312644958 CET	65198	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:25.332699060 CET	53	65198	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:27.345777988 CET	62910	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:27.365106106 CET	53	62910	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:30.240421057 CET	63863	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:31.064527988 CET	53	63863	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:32.906943083 CET	63229	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:32.924936056 CET	53	63229	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:34.919732094 CET	62538	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:34.938977957 CET	53	62538	8.8.8.8	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:30:36.914690018 CET	54903	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:36.935085058 CET	53	54903	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:41.510499001 CET	51530	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:41.802865028 CET	53	51530	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:45.704906940 CET	56122	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:45.724493027 CET	53	56122	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:47.939956903 CET	52556	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:47.958667994 CET	53	52556	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:50.734925985 CET	61609	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:50.754672050 CET	53	61609	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:53.275834084 CET	52481	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:53.293008089 CET	53	52481	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:54.819243908 CET	53943	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:54.838155985 CET	53	53943	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:57.832797050 CET	56086	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:57.850481033 CET	53	56086	8.8.8.8	192.168.2.6
Nov 3, 2022 12:30:59.560048103 CET	56547	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:30:59.579384089 CET	53	56547	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:01.170101881 CET	59881	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:01.189847946 CET	53	59881	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:03.812359095 CET	58917	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:03.831717968 CET	53	58917	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:05.602891922 CET	50343	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:05.622453928 CET	53	50343	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:07.541344881 CET	62520	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:07.558957100 CET	53	62520	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:09.419343948 CET	55629	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:09.438843966 CET	53	55629	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:11.161881924 CET	52079	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:11.179299116 CET	53	52079	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:22.519120932 CET	56569	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:22.538552046 CET	53	56569	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:25.278309107 CET	61833	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:25.295921087 CET	53	61833	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:27.427875996 CET	65044	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:27.445188999 CET	53	65044	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:29.125849009 CET	60032	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:29.145350933 CET	53	60032	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:30.955920935 CET	49232	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:30.976178885 CET	53	49232	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:32.930668116 CET	56123	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:32.949887991 CET	53	56123	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:35.521024942 CET	59752	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:35.540065050 CET	53	59752	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:37.538077116 CET	52865	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:37.555300951 CET	53	52865	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:39.862227917 CET	57322	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:39.879426956 CET	53	57322	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:41.802947998 CET	62958	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:41.821785927 CET	53	62958	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:43.694916964 CET	64404	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:43.714163065 CET	53	64404	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:45.492507935 CET	62848	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:45.510040045 CET	53	62848	8.8.8.8	192.168.2.6
Nov 3, 2022 12:31:47.481296062 CET	55956	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:31:47.499958038 CET	53	55956	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 3, 2022 12:30:06.615612984 CET	192.168.2.6	8.8.8.8	0x9698	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:11.893251896 CET	192.168.2.6	8.8.8.8	0x836	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:13.938466072 CET	192.168.2.6	8.8.8.8	0x6c7f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:15.990658998 CET	192.168.2.6	8.8.8.8	0x898b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:17.960731983 CET	192.168.2.6	8.8.8.8	0xfd9	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:20.174104929 CET	192.168.2.6	8.8.8.8	0xb2c5	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:22.044584990 CET	192.168.2.6	8.8.8.8	0x3df	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:25.312644958 CET	192.168.2.6	8.8.8.8	0x1b5b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:27.345777988 CET	192.168.2.6	8.8.8.8	0x744c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:30.240421057 CET	192.168.2.6	8.8.8.8	0x679b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:32.906943083 CET	192.168.2.6	8.8.8.8	0x93fc	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:34.919732094 CET	192.168.2.6	8.8.8.8	0xf5b2	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:36.914690018 CET	192.168.2.6	8.8.8.8	0x4e0b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:41.510499001 CET	192.168.2.6	8.8.8.8	0x72f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:45.704906940 CET	192.168.2.6	8.8.8.8	0x2cbb	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:47.939956903 CET	192.168.2.6	8.8.8.8	0x5480	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:50.734925985 CET	192.168.2.6	8.8.8.8	0xeac7	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:53.275834084 CET	192.168.2.6	8.8.8.8	0xa703	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:54.819243908 CET	192.168.2.6	8.8.8.8	0xb2a0	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:57.832797050 CET	192.168.2.6	8.8.8.8	0x101a	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:59.560048103 CET	192.168.2.6	8.8.8.8	0x26c2	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:01.170101881 CET	192.168.2.6	8.8.8.8	0x2de9	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:03.812359095 CET	192.168.2.6	8.8.8.8	0x997d	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:05.602891922 CET	192.168.2.6	8.8.8.8	0xdc66	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:07.541344881 CET	192.168.2.6	8.8.8.8	0x2825	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:09.419343948 CET	192.168.2.6	8.8.8.8	0xa44c	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:11.161881924 CET	192.168.2.6	8.8.8.8	0xbf26	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:22.519120932 CET	192.168.2.6	8.8.8.8	0x8b48	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:25.278309107 CET	192.168.2.6	8.8.8.8	0x6a31	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:27.427875996 CET	192.168.2.6	8.8.8.8	0x81d8	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:29.125849009 CET	192.168.2.6	8.8.8.8	0x5fd	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:30.955920935 CET	192.168.2.6	8.8.8.8	0x984b	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:32.930668116 CET	192.168.2.6	8.8.8.8	0x5c96	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:35.521024942 CET	192.168.2.6	8.8.8.8	0x9f71	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:37.538077116 CET	192.168.2.6	8.8.8.8	0x396f	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:31:39.862227917 CET	192.168.2.6	8.8.8.8	0xc65	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:41.802947998 CET	192.168.2.6	8.8.8.8	0xe860	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:43.694916964 CET	192.168.2.6	8.8.8.8	0x4f0d	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:45.492507935 CET	192.168.2.6	8.8.8.8	0x845a	Standard query (0)	sempersim.su	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:47.481296062 CET	192.168.2.6	8.8.8.8	0xe70	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 3, 2022 12:30:06.635174990 CET	8.8.8.8	192.168.2.6	0x9698	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:11.910538912 CET	8.8.8.8	192.168.2.6	0x836	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:13.958684921 CET	8.8.8.8	192.168.2.6	0x6c7f	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:16.008389950 CET	8.8.8.8	192.168.2.6	0x898b	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:18.222553015 CET	8.8.8.8	192.168.2.6	0xfd9	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:20.193391085 CET	8.8.8.8	192.168.2.6	0xb2c5	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:22.064102888 CET	8.8.8.8	192.168.2.6	0x3df	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:25.332699060 CET	8.8.8.8	192.168.2.6	0x1b5b	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:27.365106106 CET	8.8.8.8	192.168.2.6	0x744c	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:31.064527988 CET	8.8.8.8	192.168.2.6	0x679b	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:32.924936056 CET	8.8.8.8	192.168.2.6	0x93fc	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:34.938977957 CET	8.8.8.8	192.168.2.6	0xf5b2	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:36.935085058 CET	8.8.8.8	192.168.2.6	0x4e0b	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:41.802865028 CET	8.8.8.8	192.168.2.6	0x72f	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:45.724493027 CET	8.8.8.8	192.168.2.6	0x2cbb	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:47.958667994 CET	8.8.8.8	192.168.2.6	0x5480	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:50.754672050 CET	8.8.8.8	192.168.2.6	0xeac7	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:53.293008089 CET	8.8.8.8	192.168.2.6	0xa703	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:54.838155985 CET	8.8.8.8	192.168.2.6	0xb2a0	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

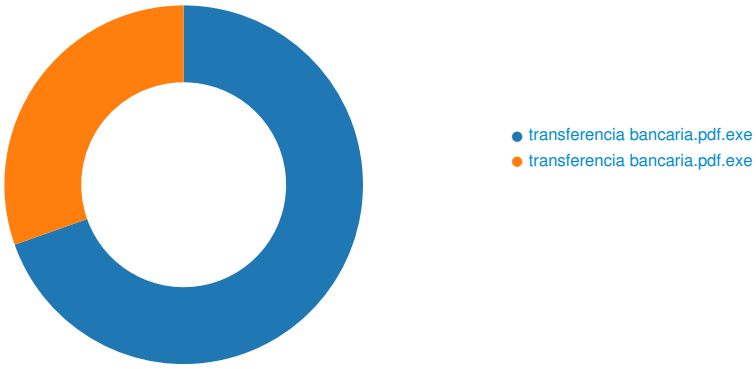
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:30:57.850481033 CET	8.8.8.8	192.168.2.6	0x101a	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:30:59.579384089 CET	8.8.8.8	192.168.2.6	0x26c2	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:01.189847946 CET	8.8.8.8	192.168.2.6	0x2de9	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:03.831717968 CET	8.8.8.8	192.168.2.6	0x997d	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:05.622453928 CET	8.8.8.8	192.168.2.6	0xdc66	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:07.558957100 CET	8.8.8.8	192.168.2.6	0x2825	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:09.438843966 CET	8.8.8.8	192.168.2.6	0xa44c	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:11.179299116 CET	8.8.8.8	192.168.2.6	0xbf26	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:22.538552046 CET	8.8.8.8	192.168.2.6	0x8b48	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:25.295921087 CET	8.8.8.8	192.168.2.6	0x6a31	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:27.445188999 CET	8.8.8.8	192.168.2.6	0x81d8	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:29.145350933 CET	8.8.8.8	192.168.2.6	0x5fd	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:30.976178885 CET	8.8.8.8	192.168.2.6	0x984b	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:32.949887991 CET	8.8.8.8	192.168.2.6	0x5c96	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:35.540065050 CET	8.8.8.8	192.168.2.6	0x9f71	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:37.555300951 CET	8.8.8.8	192.168.2.6	0x396f	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:39.879426956 CET	8.8.8.8	192.168.2.6	0xc65	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:41.821785927 CET	8.8.8.8	192.168.2.6	0xe860	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:43.714163065 CET	8.8.8.8	192.168.2.6	0x4f0d	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:45.510040045 CET	8.8.8.8	192.168.2.6	0x845a	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:31:47.499958038 CET	8.8.8.8	192.168.2.6	0xe70	No error (0)	sempersim.su		91.142.77.45	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- sempersim.su

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: transferencia bancaria.pdf.exe PID: **1100**, Parent PID: **3452**

General

Target ID:	0
Start time:	12:29:47
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\transferencia bancaria.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\transferencia bancaria.pdf.exe
Imagebase:	0xf40000
File size:	811008 bytes
MD5 hash:	355EFB2E1F7DD361F8E7CDA449A45EAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.277908890.0000000003356000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.290985684.000000000442B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.290985684.000000000442B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.290985684.000000000442B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.290985684.000000000442B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.290985684.000000000442B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.290985684.000000000442B000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.289674735.0000000003592000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.291086969.0000000004445000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.291086969.0000000004445000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.291086969.0000000004445000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000000.00000002.291086969.0000000004445000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000000.00000002.291086969.0000000004445000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.291086969.0000000004445000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D65CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D65CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\transferencia bancaria.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\transferencia bancaria.pdf.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D96C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile

Analysis Process: transferencia bancaria.pdf.exe PID: **5228**, Parent PID: **1100**

General

Target ID:	1
Start time:	12:29:59
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\transferencia bancaria.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\transferencia bancaria.pdf.exe
Imagebase:	0x5f0000
File size:	811008 bytes
MD5 hash:	355EFB2E1F7DD361F8E7CDA449A45EAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000001.00000000.275125166.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 00000001.00000002.513741442.0000000000CF8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.275310547.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000000.275310547.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000000.275310547.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000001.00000000.275310547.0000000000415000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

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

File Deleted

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

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\transferencia bancaria.pdf.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
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	40415C	ReadFile

Disassembly

No disassembly