ID: 635076
Sample Name: qFhgp7xLT7
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 12:30:06
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

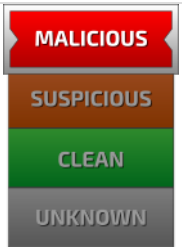
qFhgp7xLT7

Overview

General Information

Sample Name:	qFhgp7xLT7
Analysis ID:	635076
MD5:	60c16bbdea70d0..
SHA1:	333cc469a02c21..
SHA256:	3d8b14056393a4.
Tags:	32 elf intel mirai
Infos:	

Detection



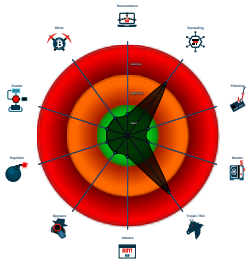
Mirai

Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Uses known network protocols on n…
- Machine Learning detection for sam…
- Sample tries to kill multiple process…
- Sample has stripped symbol table
- HTTP GET or POST without a user …
- Enumerates processes within the "p…
- Detected TCP or UDP traffic on non…
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely that the sample will exhibit less behavior.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635076
Start date and time: 27/05/202212:30:06	2022-05-27 12:30:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qFhgp7xLT7
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal76.spre.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/qFhgp7xLT7
PID:	6237
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected By Cult
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- qFhgp7xLT7 (PID: 6237, Parent: 6125, MD5: 60c16bbdea70d058618c85e3e7d5a7c5) Arguments: /tmp/qFhgp7xLT7
  - qFhgp7xLT7 New Fork (PID: 6238, Parent: 6237)
  - qFhgp7xLT7 New Fork (PID: 6239, Parent: 6237)
  - qFhgp7xLT7 New Fork (PID: 6240, Parent: 6237)
    - qFhgp7xLT7 New Fork (PID: 6241, Parent: 6240)
    - qFhgp7xLT7 New Fork (PID: 6242, Parent: 6240)
    - qFhgp7xLT7 New Fork (PID: 6244, Parent: 6240)
    - qFhgp7xLT7 New Fork (PID: 6245, Parent: 6240)
    - qFhgp7xLT7 New Fork (PID: 6246, Parent: 6240)
    - qFhgp7xLT7 New Fork (PID: 6247, Parent: 6240)
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Snort Signatures

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.202.70

Timestamp:	192.168.2.23112.72.202.7037234802839471 05/27/22-12:33:25.144916
SID:	2839471
Source Port:	37234
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.248.3.12

Timestamp:	192.168.2.2388.248.3.1233844802839471 05/27/22-12:32:09.515172
SID:	2839471
Source Port:	33844
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.67.128

Timestamp:	192.168.2.2388.221.67.12845550802839471 05/27/22-12:31:17.612604
SID:	2839471
Source Port:	45550
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.95.58

Timestamp:	192.168.2.2388.198.95.5834904802839471 05/27/22-12:33:19.894224
SID:	2839471
Source Port:	34904
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.157.135

Timestamp:	192.168.2.2395.216.157.13536388802839471 05/27/22-12:31:45.532082

SID:	2839471
Source Port:	36388
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.80.187.20

Timestamp:	192.168.2.2388.80.187.2054684802839471 05/27/22-12:31:48.571853
SID:	2839471
Source Port:	54684
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.186.20.38

Timestamp:	192.168.2.23112.186.20.3843052802839471 05/27/22-12:32:37.328412
SID:	2839471
Source Port:	43052
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.142.154.35

Timestamp:	192.168.2.2395.142.154.3538450802839471 05/27/22-12:33:45.996466
SID:	2839471
Source Port:	38450
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.119.176.78

Timestamp:	192.168.2.2388.119.176.7846082802839471 05/27/22-12:31:17.602521
SID:	2839471
Source Port:	46082
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.202.185.34

Timestamp:	192.168.2.2388.202.185.3443256802839471 05/27/22-12:31:48.544252
SID:	2839471
Source Port:	43256
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.213.144.234

Timestamp:	192.168.2.2395.213.144.23458586802839471 05/27/22-12:31:56.949860
SID:	2839471
Source Port:	58586
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.55.52

Timestamp:	192.168.2.23112.72.55.5240524802839471 05/27/22-12:33:51.607828
SID:	2839471
Source Port:	40524
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.182.104

Timestamp:	192.168.2.2388.221.182.10450788802839471 05/27/22-12:32:43.974254
SID:	2839471
Source Port:	50788
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.181.216.188

Timestamp:	192.168.2.2395.181.216.18845576802839471 05/27/22-12:31:45.532015
SID:	2839471
Source Port:	45576
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.46.56

Timestamp:	192.168.2.2395.216.46.5638706802839471 05/27/22-12:30:59.349797
SID:	2839471
Source Port:	38706
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.197.186.69

Timestamp:	192.168.2.23112.197.186.6934248802839471 05/27/22-12:34:15.486204
SID:	2839471
Source Port:	34248
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.85.49.125

Timestamp:	192.168.2.2395.85.49.12557494802839471 05/27/22-12:31:01.042653
SID:	2839471
Source Port:	57494
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.51.178

Timestamp:	192.168.2.2395.101.51.17833806802839471 05/27/22-12:34:11.712649
SID:	2839471
Source Port:	33806
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.248.97.42

Timestamp:	192.168.2.2388.248.97.4251404802839471 05/27/22-12:31:19.756383
SID:	2839471
Source Port:	51404
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.211.86.222

Timestamp:	192.168.2.23112.211.86.22251576802839471 05/27/22-12:31:28.539011
SID:	2839471
Source Port:	51576
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.234.59.49

Timestamp:	192.168.2.23197.234.59.4957624372152835222 05/27/22-12:33:52.815817
SID:	2835222
Source Port:	57624
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.223.88

Timestamp:	192.168.2.2395.217.223.8845340802839471 05/27/22-12:31:01.059678
SID:	2839471
Source Port:	45340
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.80.109.205

Timestamp:	192.168.2.2395.80.109.20545624802839471 05/27/22-12:33:44.241244
SID:	2839471
Source Port:	45624
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.183.11.60

Timestamp:	192.168.2.2395.183.11.6060636802839471 05/27/22-12:31:33.291681
SID:	2839471
Source Port:	60636
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.153.193.105

Timestamp:	192.168.2.2388.153.193.10557226802839471 05/27/22-12:33:32.506696
SID:	2839471
Source Port:	57226
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.186.70.80

Timestamp:	192.168.2.23112.186.70.8049836802839471 05/27/22-12:31:46.023807
SID:	2839471
Source Port:	49836
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.110.179.229

Timestamp:	192.168.2.2395.110.179.22947442802839471 05/27/22-12:32:12.681029
SID:	2839471
Source Port:	47442
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.166.221.94

Timestamp:	192.168.2.23112.166.221.9432838802839471 05/27/22-12:32:39.180234
SID:	2839471
Source Port:	32838
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.212.1.166

Timestamp:	192.168.2.2388.212.1.16633040802839471 05/27/22-12:32:16.185110
SID:	2839471
Source Port:	33040
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.14.86.198

Timestamp:	192.168.2.2395.14.86.19846290802839471 05/27/22-12:31:33.281866
SID:	2839471
Source Port:	46290
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.167.174.105

Timestamp:	192.168.2.23112.167.174.10546562802839471 05/27/22-12:31:50.944811
SID:	2839471
Source Port:	46562
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.186.20.38

Timestamp:	192.168.2.23112.186.20.3843220802839471 05/27/22-12:32:47.374861
SID:	2839471
Source Port:	43220
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.119.146.26

Timestamp:	192.168.2.2388.119.146.2644976802839471 05/27/22-12:33:27.528059
SID:	2839471
Source Port:	44976
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.225.227.244

Timestamp:	192.168.2.2388.225.227.24433820802839471 05/27/22-12:31:06.463207
SID:	2839471
Source Port:	33820
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.81.130.67

Timestamp:	192.168.2.23112.81.130.6753396802839471 05/27/22-12:31:51.424495
SID:	2839471
Source Port:	53396
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.56.61.3

Timestamp:	192.168.2.2395.56.61.339992802839471 05/27/22-12:31:33.483422
SID:	2839471
Source Port:	39992
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.175.41.180

Timestamp:	192.168.2.23112.175.41.18034328802839471 05/27/22-12:32:13.340256
SID:	2839471
Source Port:	34328
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.74.93.134

Timestamp:	192.168.2.23112.74.93.13439556802839471 05/27/22-12:32:02.442088
SID:	2839471
Source Port:	39556
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.40.188

Timestamp:	192.168.2.2388.221.40.18858726802839471 05/27/22-12:31:54.763991
SID:	2839471
Source Port:	58726
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.56.210.231

Timestamp:	192.168.2.2395.56.210.23144612802839471 05/27/22-12:31:00.444715
SID:	2839471
Source Port:	44612
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.211.24.216

Timestamp:	192.168.2.2395.211.24.21636048802839471 05/27/22-12:34:29.393344
SID:	2839471
Source Port:	36048
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.163.202.34

Timestamp:	192.168.2.2395.163.202.3455820802839471 05/27/22-12:31:35.237352
SID:	2839471
Source Port:	55820
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.218.28.73

Timestamp:	192.168.2.2388.218.28.7358892802839471 05/27/22-12:32:18.783163
SID:	2839471
Source Port:	58892
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.7.134

Timestamp:	192.168.2.2395.100.7.13456148802839471 05/27/22-12:33:06.960464
SID:	2839471
Source Port:	56148
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.174.197.184

Timestamp:	192.168.2.2395.174.197.18435646802839471 05/27/22-12:31:11.849947
SID:	2839471
Source Port:	35646
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.74.79.44

Timestamp:	192.168.2.23112.74.79.4439520802839471 05/27/22-12:31:50.936841
SID:	2839471
Source Port:	39520
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.149.226.201

Timestamp:	192.168.2.23112.149.226.20155834802839471 05/27/22-12:32:37.572523
SID:	2839471
Source Port:	55834
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.186.20.38

Timestamp:	192.168.2.23112.186.20.3843104802839471 05/27/22-12:32:41.687023
SID:	2839471
Source Port:	43104
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.168.210.33

Timestamp:	192.168.2.2395.168.210.3346156802839471 05/27/22-12:32:06.984091
SID:	2839471
Source Port:	46156
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.211.152.137

Timestamp:	192.168.2.2395.211.152.13753944802839471 05/27/22-12:32:18.728402
SID:	2839471
Source Port:	53944
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.142.205.212

Timestamp:	192.168.2.2395.142.205.21235762802839471 05/27/22-12:31:34.926249
SID:	2839471
Source Port:	35762
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.238.152.223

Timestamp:	192.168.2.2395.238.152.22358532802839471 05/27/22-12:32:22.621176
SID:	2839471
Source Port:	58532
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.70.247

Timestamp:	192.168.2.2395.100.70.24736802802839471 05/27/22-12:32:30.210014
SID:	2839471
Source Port:	36802
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.244.64

Timestamp:	192.168.2.2395.58.244.6440006802839471 05/27/22-12:32:30.316788
SID:	2839471
Source Port:	40006
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.151.105

Timestamp:	192.168.2.2388.198.151.10550458802839471 05/27/22-12:31:23.849032
SID:	2839471
Source Port:	50458
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.65.82.201

Timestamp:	192.168.2.2395.65.82.20149266802839471 05/27/22-12:34:15.312931
SID:	2839471
Source Port:	49266
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.87.122.44

Timestamp:	192.168.2.2388.87.122.4440572802839471 05/27/22-12:31:54.832677
SID:	2839471
Source Port:	40572
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.20.119.93

Timestamp:	192.168.2.2395.20.119.9339774802839471 05/27/22-12:33:53.002379
SID:	2839471
Source Port:	39774
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.214.91.9

Timestamp:	192.168.2.23112.214.91.943860802839471 05/27/22-12:34:06.593929
SID:	2839471
Source Port:	43860
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.124.202.59

Timestamp:	192.168.2.23112.124.202.5949088802839471 05/27/22-12:32:30.928386
SID:	2839471
Source Port:	49088
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.154.219.67

Timestamp:	192.168.2.2395.154.219.6738350802839471 05/27/22-12:32:36.726942
SID:	2839471
Source Port:	38350
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.84.182

Timestamp:	192.168.2.2395.100.84.18252118802839471 05/27/22-12:31:38.667115
SID:	2839471
Source Port:	52118
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.235.105.204

Timestamp:	192.168.2.2395.235.105.20446940802839471 05/27/22-12:33:12.901640
SID:	2839471
Source Port:	46940
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.178.147.97

Timestamp:	192.168.2.23112.178.147.9751130802839471 05/27/22-12:31:28.520517
SID:	2839471
Source Port:	51130
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.204.110

Timestamp:	192.168.2.2395.100.204.11037574802839471 05/27/22-12:31:00.396025
SID:	2839471
Source Port:	37574
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.137.152

Timestamp:	192.168.2.2388.198.137.15253476802839471 05/27/22-12:31:42.335689
SID:	2839471
Source Port:	53476
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.154.221.177

Timestamp:	192.168.2.2395.154.221.17751686802839471 05/27/22-12:32:22.567031
SID:	2839471
Source Port:	51686
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.84.42

Timestamp:	192.168.2.2388.99.84.4244326802839471 05/27/22-12:31:54.754494
SID:	2839471
Source Port:	44326
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.82.7

Timestamp:	192.168.2.2395.217.82.746910802839471 05/27/22-12:31:19.799558
SID:	2839471
Source Port:	46910
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.164.173.23

Timestamp:	192.168.2.23112.164.173.2357754802839471 05/27/22-12:32:02.457344
SID:	2839471
Source Port:	57754
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.169.182.145

Timestamp:	192.168.2.23112.169.182.14540522802839471 05/27/22-12:31:28.532451
SID:	2839471
Source Port:	40522
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.211.189.204

Timestamp:	192.168.2.2395.211.189.20459478802839471 05/27/22-12:33:00.977962
SID:	2839471
Source Port:	59478
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.171.40.223

Timestamp:	192.168.2.23112.171.40.22351266802839471 05/27/22-12:34:26.065722
SID:	2839471
Source Port:	51266
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.98.181.157

Timestamp:	192.168.2.2388.98.181.15749770802839471 05/27/22-12:33:01.043025
SID:	2839471
Source Port:	49770
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.161.28

Timestamp:	192.168.2.2395.101.161.2857428802839471 05/27/22-12:31:33.308821
SID:	2839471
Source Port:	57428
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.113.5

Timestamp:	192.168.2.2395.58.113.559516802839471 05/27/22-12:32:19.026650
SID:	2839471
Source Port:	59516
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.208.214.83

Timestamp:	192.168.2.2388.208.214.8354508802839471 05/27/22-12:33:14.819620
SID:	2839471
Source Port:	54508
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.59.245.20

Timestamp:	192.168.2.2395.59.245.2043218802839471 05/27/22-12:32:30.308154
SID:	2839471
Source Port:	43218
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.208.220.5

Timestamp:	192.168.2.2388.208.220.547198802839471 05/27/22-12:31:23.868712
SID:	2839471
Source Port:	47198
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.39.140.15

Timestamp:	192.168.2.2395.39.140.1534816802839471 05/27/22-12:31:38.557073
SID:	2839471
Source Port:	34816
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.22.247.175

Timestamp:	192.168.2.2388.22.247.17554798802839471 05/27/22-12:32:16.218137
SID:	2839471
Source Port:	54798
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.80.166

Timestamp:	192.168.2.2395.101.80.16635368802839471 05/27/22-12:31:19.815486
SID:	2839471
Source Port:	35368
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.165.255.5

Timestamp:	192.168.2.2395.165.255.538992802839471 05/27/22-12:34:00.476246
SID:	2839471
Source Port:	38992
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.179.72

Timestamp:	192.168.2.2395.101.179.7247718802839471 05/27/22-12:33:45.559487
SID:	2839471
Source Port:	47718
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.31.233.3

Timestamp:	192.168.2.2388.31.233.346718802839471 05/27/22-12:31:20.193652
SID:	2839471
Source Port:	46718
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.138.128.78

Timestamp:	192.168.2.2395.138.128.7836584802839471 05/27/22-12:31:54.758519
SID:	2839471
Source Port:	36584
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.59.33.161

Timestamp:	192.168.2.2395.59.33.16151250802839471 05/27/22-12:32:24.240623
SID:	2839471
Source Port:	51250
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.163.26.192

Timestamp:	192.168.2.2388.163.26.19238608802839471 05/27/22-12:32:18.792798
SID:	2839471
Source Port:	38608
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.46.138

Timestamp:	192.168.2.2388.221.46.13850426802839471 05/27/22-12:31:51.214773
SID:	2839471
Source Port:	50426
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.26.93

Timestamp:	192.168.2.2395.217.26.9340238802839471 05/27/22-12:32:22.579519
SID:	2839471
Source Port:	40238
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.117.85

Timestamp:	192.168.2.2395.57.117.8556186802839471 05/27/22-12:31:15.088619
SID:	2839471
Source Port:	56186
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.159.47.27

Timestamp:	192.168.2.2395.159.47.2739312802839471 05/27/22-12:31:19.910781
SID:	2839471
Source Port:	39312
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.12.46.218

Timestamp:	192.168.2.2388.12.46.21853806802839471 05/27/22-12:31:23.930863
SID:	2839471
Source Port:	53806
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.14.207

Timestamp:	192.168.2.2395.101.14.20760674802839471 05/27/22-12:33:11.611379
SID:	2839471
Source Port:	60674
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.80.20.160

Timestamp:	192.168.2.2388.80.20.16059264802839471 05/27/22-12:31:31.124184
SID:	2839471
Source Port:	59264
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.129.59.54

Timestamp:	192.168.2.2388.129.59.5441168802839471 05/27/22-12:31:54.808552
SID:	2839471
Source Port:	41168
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.179.162.82

Timestamp:	192.168.2.2395.179.162.8249118802839471 05/27/22-12:32:12.671842
SID:	2839471
Source Port:	49118
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.154.232.180

Timestamp:	192.168.2.2395.154.232.18054160802839471 05/27/22-12:31:19.786814
SID:	2839471
Source Port:	54160
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.210.113

Timestamp:	192.168.2.2395.100.210.11343142802839471 05/27/22-12:31:56.914233
SID:	2839471
Source Port:	43142
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.247.209.76

Timestamp:	192.168.2.2388.247.209.7656418802839471 05/27/22-12:32:44.011426
SID:	2839471
Source Port:	56418
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.78.215

Timestamp:	192.168.2.2395.101.78.21536224802839471 05/27/22-12:32:22.566529
SID:	2839471
Source Port:	36224
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.111.194.231

Timestamp:	192.168.2.2395.111.194.23152466802839471 05/27/22-12:31:33.671458
SID:	2839471
Source Port:	52466
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.242.252

Timestamp:	192.168.2.2388.99.242.25248898802839471 05/27/22-12:32:00.067857
SID:	2839471
Source Port:	48898
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.239.156

Timestamp:	192.168.2.2395.58.239.15650468802839471 05/27/22-12:32:19.018154
SID:	2839471
Source Port:	50468
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.174.10

Timestamp:	192.168.2.2395.101.174.1043504802839471 05/27/22-12:33:58.075621
SID:	2839471
Source Port:	43504
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.148.46

Timestamp:	192.168.2.2388.221.148.4654120802839471 05/27/22-12:31:23.853653
SID:	2839471
Source Port:	54120
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.38.192.99

Timestamp:	192.168.2.2395.38.192.9948692802839471 05/27/22-12:31:34.995858
SID:	2839471
Source Port:	48692
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.143.188.168

Timestamp:	192.168.2.2395.143.188.16843516802839471 05/27/22-12:31:45.547396
SID:	2839471
Source Port:	43516
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.77.15

Timestamp:	192.168.2.2388.221.77.1557238802839471 05/27/22-12:33:39.992640
SID:	2839471
Source Port:	57238
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.222.195

Timestamp:	192.168.2.2388.99.222.19559234802839471 05/27/22-12:31:17.577531
SID:	2839471
Source Port:	59234
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.157.177

Timestamp:	192.168.2.2395.58.157.17757174802839471 05/27/22-12:31:38.540240
SID:	2839471
Source Port:	57174
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.74.142.34

Timestamp:	192.168.2.23112.74.142.3459320802839471 05/27/22-12:31:23.802886
SID:	2839471
Source Port:	59320
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.186.177

Timestamp:	192.168.2.2395.100.186.17755934802839471 05/27/22-12:31:19.783764
SID:	2839471
Source Port:	55934
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.197.186.69

Timestamp:	192.168.2.23112.197.186.6934232802839471 05/27/22-12:34:15.264649
SID:	2839471
Source Port:	34232
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.225.193

Timestamp:	192.168.2.2388.99.225.19342160802839471 05/27/22-12:31:43.544055
SID:	2839471
Source Port:	42160
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.213.207.4

Timestamp:	192.168.2.2388.213.207.446980802839471 05/27/22-12:31:48.561691
SID:	2839471
Source Port:	46980
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.167.13

Timestamp:	192.168.2.2395.58.167.1339100802839471 05/27/22-12:31:17.554715
SID:	2839471
Source Port:	39100
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.169.212.140

Timestamp:	192.168.2.2395.169.212.14050382802839471 05/27/22-12:33:09.361075
SID:	2839471
Source Port:	50382
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.122.156.191

Timestamp:	192.168.2.23112.122.156.19160710802839471 05/27/22-12:32:09.446158
SID:	2839471
Source Port:	60710
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.181.216.134

Timestamp:	192.168.2.2395.181.216.13439360802839471 05/27/22-12:33:56.676376
SID:	2839471
Source Port:	39360
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.39.110

Timestamp:	192.168.2.2395.217.39.11039044802839471 05/27/22-12:31:34.961644
SID:	2839471
Source Port:	39044
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.165.103.75

Timestamp:	192.168.2.23112.165.103.7553042802839471 05/27/22-12:32:06.956682
SID:	2839471
Source Port:	53042
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.210.20

Timestamp:	192.168.2.2388.198.210.2041554802839471 05/27/22-12:33:48.061475
SID:	2839471
Source Port:	41554
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.111.247.191

Timestamp:	192.168.2.2395.111.247.19134022802839471 05/27/22-12:31:33.249723
SID:	2839471
Source Port:	34022
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.56.134.41

Timestamp:	192.168.2.2395.56.134.4155198802839471 05/27/22-12:33:43.132577
SID:	2839471
Source Port:	55198
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.143.218.151

Timestamp:	192.168.2.2395.143.218.15158842802839471 05/27/22-12:31:34.920579
SID:	2839471
Source Port:	58842
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.56.25.177

Timestamp:	192.168.2.2395.56.25.17758708802839471 05/27/22-12:33:11.671020
SID:	2839471
Source Port:	58708
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.45.117.152

Timestamp:	192.168.2.23112.45.117.15235872802839471 05/27/22-12:32:22.616897
SID:	2839471
Source Port:	35872
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.225.240.206

Timestamp:	192.168.2.2388.225.240.20647174802839471 05/27/22-12:32:00.123619
SID:	2839471
Source Port:	47174
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.139.131.71

Timestamp:	192.168.2.2395.139.131.7156624802839471 05/27/22-12:31:19.900307
SID:	2839471
Source Port:	56624
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.70.237.15

Timestamp:	192.168.2.23112.70.237.1542186802839471 05/27/22-12:32:16.418537
SID:	2839471
Source Port:	42186
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.48.238

Timestamp:	192.168.2.2395.100.48.23837696802839471 05/27/22-12:33:40.977680
SID:	2839471
Source Port:	37696
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.173.178.4

Timestamp:	192.168.2.2395.173.178.449408802839471 05/27/22-12:32:07.017851
SID:	2839471
Source Port:	49408
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.152.159.96

Timestamp:	192.168.2.2388.152.159.9645460802839471 05/27/22-12:32:18.787691
SID:	2839471
Source Port:	45460
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.143.50

Timestamp:	192.168.2.2395.217.143.5041066802839471 05/27/22-12:31:38.463113
SID:	2839471
Source Port:	41066
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.206.140.206

Timestamp:	192.168.2.23112.206.140.20648232802839471 05/27/22-12:33:29.276621
SID:	2839471
Source Port:	48232
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.48.170.103

Timestamp:	192.168.2.23112.48.170.10346806802839471 05/27/22-12:31:51.437308
SID:	2839471
Source Port:	46806
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.111.251.31

Timestamp:	192.168.2.2395.111.251.3158270802839471 05/27/22-12:34:13.924270
SID:	2839471
Source Port:	58270
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.138.204

Timestamp:	192.168.2.2395.216.138.20456560802839471 05/27/22-12:32:06.997755
SID:	2839471
Source Port:	56560
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.64.216

Timestamp:	192.168.2.2395.217.64.21642418802839471 05/27/22-12:31:38.463136
SID:	2839471
Source Port:	42418
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.164.219.100

Timestamp:	192.168.2.2395.164.219.10052268802839471 05/27/22-12:32:07.060866
SID:	2839471
Source Port:	52268
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.139.173

Timestamp:	192.168.2.2388.221.139.17341446802839471 05/27/22-12:31:15.018641
SID:	2839471
Source Port:	41446
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.111.27

Timestamp:	192.168.2.2388.221.111.2735636802839471 05/27/22-12:31:25.170536
SID:	2839471
Source Port:	35636
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.196.100

Timestamp:	192.168.2.2388.221.196.10042160802839471 05/27/22-12:31:29.023462
SID:	2839471
Source Port:	42160
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.103.173.67

Timestamp:	192.168.2.2388.103.173.6754636802839471 05/27/22-12:34:17.807413
SID:	2839471
Source Port:	54636
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.47.1.173

Timestamp:	192.168.2.23112.47.1.17334512802839471 05/27/22-12:32:15.868522
SID:	2839471
Source Port:	34512
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.200.243.93

Timestamp:	192.168.2.23112.200.243.9341862802839471 05/27/22-12:33:05.511661
SID:	2839471
Source Port:	41862
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.203.6.129

Timestamp:	192.168.2.2388.203.6.12952030802839471 05/27/22-12:31:45.486116
SID:	2839471
Source Port:	52030
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.197.186.69

Timestamp:	192.168.2.23112.197.186.6934662802839471 05/27/22-12:34:29.593435
SID:	2839471
Source Port:	34662
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.181.161.188

Timestamp:	192.168.2.2395.181.161.18833806802839471 05/27/22-12:32:12.680954
SID:	2839471
Source Port:	33806
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.211.83.72

Timestamp:	192.168.2.2388.211.83.7245092802839471 05/27/22-12:31:54.800343
SID:	2839471
Source Port:	45092
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.87.4.51

Timestamp:	192.168.2.2388.87.4.5151120802839471 05/27/22-12:31:15.092894
SID:	2839471
Source Port:	51120
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.179.180.152

Timestamp:	192.168.2.2395.179.180.15238212802839471 05/27/22-12:33:30.964976
SID:	2839471
Source Port:	38212
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.87.26.25

Timestamp:	192.168.2.2388.87.26.2551386802839471 05/27/22-12:31:15.092875
SID:	2839471
Source Port:	51386
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.34.44.172

Timestamp:	192.168.2.2388.34.44.17258598802839471 05/27/22-12:32:45.075473
SID:	2839471
Source Port:	58598
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.111.27

Timestamp:	192.168.2.2388.221.111.2735596802839471 05/27/22-12:31:23.848429
SID:	2839471
Source Port:	35596
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.163.5.179

Timestamp:	192.168.2.23112.163.5.17945500802839471 05/27/22-12:31:23.584004
SID:	2839471
Source Port:	45500
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.86.215.220

Timestamp:	192.168.2.2388.86.215.22060880802839471 05/27/22-12:31:43.521931
SID:	2839471
Source Port:	60880
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.121.174.27

Timestamp:	192.168.2.23112.121.174.2733836802839471 05/27/22-12:32:12.885897
SID:	2839471
Source Port:	33836
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.211.189.109

Timestamp:	192.168.2.23112.211.189.10935672802839471 05/27/22-12:33:05.551569
SID:	2839471
Source Port:	35672
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.139.246.106

Timestamp:	192.168.2.2395.139.246.10660628802839471 05/27/22-12:31:00.389921
SID:	2839471
Source Port:	60628
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.245.178.8

Timestamp:	192.168.2.2395.245.178.853938802839471 05/27/22-12:32:18.853740
SID:	2839471
Source Port:	53938
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.211.85.79

Timestamp:	192.168.2.23112.211.85.7945736802839471 05/27/22-12:32:52.261918
SID:	2839471
Source Port:	45736
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.226.61.130

Timestamp:	192.168.2.2395.226.61.13044442802839471 05/27/22-12:33:05.595447
SID:	2839471
Source Port:	44442
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.196.112.113

Timestamp:	192.168.2.23112.196.112.11338078802839471 05/27/22-12:34:26.100254
SID:	2839471
Source Port:	38078
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.47.233

Timestamp:	192.168.2.2395.216.47.23354886802839471 05/27/22-12:32:06.997849
SID:	2839471
Source Port:	54886
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.213.212.189

Timestamp:	192.168.2.2395.213.212.18938108802839471 05/27/22-12:31:06.389031
SID:	2839471
Source Port:	38108
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.213.45.92

Timestamp:	192.168.2.23112.213.45.9234744802839471 05/27/22-12:31:23.654056
SID:	2839471
Source Port:	34744
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.255.55.215

Timestamp:	192.168.2.2388.255.55.21546638802839471 05/27/22-12:31:48.630707
SID:	2839471
Source Port:	46638
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.0.91.127

Timestamp:	192.168.2.2341.0.91.12739528372152835222 05/27/22-12:34:12.220909
SID:	2835222
Source Port:	39528
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.216.103.158

Timestamp:	192.168.2.2388.216.103.15835942802839471 05/27/22-12:31:42.389093
SID:	2839471
Source Port:	35942
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.131.160.144

Timestamp:	192.168.2.2395.131.160.14457636802839471 05/27/22-12:32:36.982308
SID:	2839471
Source Port:	57636
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.35.79.54

Timestamp:	192.168.2.23112.35.79.5439488802839471 05/27/22-12:32:12.893316
SID:	2839471
Source Port:	39488
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.29.123

Timestamp:	192.168.2.2395.57.29.12344802802839471 05/27/22-12:33:01.063137
SID:	2839471
Source Port:	44802
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.250.68.225

Timestamp:	192.168.2.2388.250.68.22540434802839471 05/27/22-12:34:17.873487
SID:	2839471
Source Port:	40434
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.109.137.162

Timestamp:	192.168.2.2388.109.137.16250830802839471 05/27/22-12:32:53.097961
SID:	2839471
Source Port:	50830
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.205.11

Timestamp:	192.168.2.2388.221.205.1139676802839471 05/27/22-12:32:22.952163
SID:	2839471
Source Port:	39676
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.172.108.68

Timestamp:	192.168.2.23112.172.108.6844012802839471 05/27/22-12:31:26.456649
SID:	2839471
Source Port:	44012
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.65.181

Timestamp:	192.168.2.2395.101.65.18134938802839471 05/27/22-12:34:15.279681
SID:	2839471
Source Port:	34938
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.74.184.160

Timestamp:	192.168.2.23112.74.184.16060202802839471 05/27/22-12:31:46.274302
SID:	2839471
Source Port:	60202
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.24.129.161

Timestamp:	192.168.2.2388.24.129.16135668802839471 05/27/22-12:34:17.895514
SID:	2839471
Source Port:	35668
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.129.208.236

Timestamp:	192.168.2.2395.129.208.23659430802839471 05/27/22-12:32:22.558579
SID:	2839471
Source Port:	59430
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.14.5.224

Timestamp:	192.168.2.23112.14.5.22450654802839471 05/27/22-12:32:06.968249
SID:	2839471
Source Port:	50654
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.213.102.197

Timestamp:	192.168.2.23112.213.102.19753180802839471 05/27/22-12:31:40.096566
SID:	2839471
Source Port:	53180
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.197.186.69

Timestamp:	192.168.2.23112.197.186.6934428802839471 05/27/22-12:34:21.537072
SID:	2839471
Source Port:	34428
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.151.147.37

Timestamp:	192.168.2.2395.151.147.3752382802839471 05/27/22-12:31:33.320284
SID:	2839471
Source Port:	52382
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.225.231.241

Timestamp:	192.168.2.2388.225.231.24140972802839471 05/27/22-12:33:30.985507
SID:	2839471
Source Port:	40972
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.58.127

Timestamp:	192.168.2.23112.72.58.12757136802839471 05/27/22-12:31:00.709407
SID:	2839471
Source Port:	57136
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.203.6.129

Timestamp:	192.168.2.2388.203.6.12952022802839471 05/27/22-12:31:42.372374
SID:	2839471
Source Port:	52022
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.186.122

Timestamp:	192.168.2.2388.221.186.12234042802839471 05/27/22-12:31:43.549751
SID:	2839471
Source Port:	34042
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.77.153.13

Timestamp:	192.168.2.2395.77.153.1350944802839471 05/27/22-12:31:34.999503
SID:	2839471
Source Port:	50944
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.232.101

Timestamp:	192.168.2.2395.217.232.10152404802839471 05/27/22-12:33:43.043686
SID:	2839471
Source Port:	52404
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.249.6.182

Timestamp:	192.168.2.2395.249.6.18243248802839471 05/27/22-12:31:19.925251
SID:	2839471
Source Port:	43248
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.135.194.129

Timestamp:	192.168.2.23112.135.194.12947528802839471 05/27/22-12:32:27.557736
SID:	2839471
Source Port:	47528
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.140.155.240

Timestamp:	192.168.2.2395.140.155.24039534802839471 05/27/22-12:31:11.848254
SID:	2839471
Source Port:	39534
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.67.8.56

Timestamp:	192.168.2.2395.67.8.5649576802839471 05/27/22-12:31:54.770414
SID:	2839471
Source Port:	49576
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.163.251.196

Timestamp:	192.168.2.2395.163.251.19650388802839471 05/27/22-12:32:24.131657
SID:	2839471
Source Port:	50388
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.225.222.132

Timestamp:	192.168.2.2388.225.222.13260712802839471 05/27/22-12:32:44.015755
SID:	2839471
Source Port:	60712
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.205.207

Timestamp:	192.168.2.2388.99.205.20749030802839471 05/27/22-12:33:00.999487
SID:	2839471
Source Port:	49030
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.214.95.185

Timestamp:	192.168.2.2395.214.95.18560942802839471 05/27/22-12:31:45.629413
SID:	2839471
Source Port:	60942
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.203.102.187

Timestamp:	192.168.2.2388.203.102.18741940802839471 05/27/22-12:31:31.123524
SID:	2839471
Source Port:	41940
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.109.137.162

Timestamp:	192.168.2.2388.109.137.16250882802839471 05/27/22-12:32:56.716771
SID:	2839471
Source Port:	50882
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.9.242.104

Timestamp:	192.168.2.2395.9.242.10437384802839471 05/27/22-12:33:09.302194
SID:	2839471
Source Port:	37384
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.61.204.220

Timestamp:	192.168.2.2395.61.204.22037348802839471 05/27/22-12:32:36.837881
SID:	2839471
Source Port:	37348
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.71.129.220

Timestamp:	192.168.2.2395.71.129.22054036802839471 05/27/22-12:33:56.718060
SID:	2839471
Source Port:	54036
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.86.215.220

Timestamp:	192.168.2.2388.86.215.22060870802839471 05/27/22-12:31:45.496953
SID:	2839471
Source Port:	60870
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.209.132.118

Timestamp:	192.168.2.2395.209.132.11833830802839471 05/27/22-12:33:58.194099
SID:	2839471
Source Port:	33830
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.236.22

Timestamp:	192.168.2.2388.221.236.2257688802839471 05/27/22-12:32:16.195697
SID:	2839471
Source Port:	57688
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.229.33

Timestamp:	192.168.2.2395.101.229.3341400802839471 05/27/22-12:31:09.563382
SID:	2839471
Source Port:	41400
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.149.176.152

Timestamp:	192.168.2.2388.149.176.15243380802839471 05/27/22-12:32:16.195035
SID:	2839471
Source Port:	43380
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.208.139

Timestamp:	192.168.2.2395.101.208.13949116802839471 05/27/22-12:34:13.943690
SID:	2839471
Source Port:	49116
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.225.198

Timestamp:	192.168.2.2395.100.225.19844024802839471 05/27/22-12:31:06.356024
SID:	2839471
Source Port:	44024
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.159.43.113

Timestamp:	192.168.2.2395.159.43.11338992802839471 05/27/22-12:32:59.949064
SID:	2839471
Source Port:	38992
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.216.185.99

Timestamp:	192.168.2.2388.216.185.9945494802839471 05/27/22-12:31:24.036858
SID:	2839471
Source Port:	45494
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.227.36

Timestamp:	192.168.2.2395.101.227.3638306802839471 05/27/22-12:34:15.292281
SID:	2839471
Source Port:	38306
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.202.224.45

Timestamp:	192.168.2.2388.202.224.4533472802839471 05/27/22-12:34:17.743999
SID:	2839471
Source Port:	33472
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.179.232.73

Timestamp:	192.168.2.2395.179.232.7353852802839471 05/27/22-12:31:56.918991
SID:	2839471
Source Port:	53852
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.130.126.25

Timestamp:	192.168.2.2395.130.126.2559386802839471 05/27/22-12:31:15.003635
SID:	2839471
Source Port:	59386
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.124.20.130

Timestamp:	192.168.2.23112.124.20.13054500802839471 05/27/22-12:31:23.574128
SID:	2839471
Source Port:	54500
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.106.79

Timestamp:	192.168.2.2395.101.106.7939324802839471 05/27/22-12:31:34.935665
SID:	2839471
Source Port:	39324
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.48.238

Timestamp:	192.168.2.2395.100.48.23837708802839471 05/27/22-12:33:40.003945
SID:	2839471
Source Port:	37708
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.245.107.155

Timestamp:	192.168.2.2395.245.107.15543538802839471 05/27/22-12:31:56.958042
SID:	2839471
Source Port:	43538
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.149.24

Timestamp:	192.168.2.2395.100.149.2437798802839471 05/27/22-12:33:06.925655
SID:	2839471
Source Port:	37798
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.148.79.180

Timestamp:	192.168.2.2388.148.79.18059856802839471 05/27/22-12:32:49.499358
SID:	2839471
Source Port:	59856
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.187.174.204

Timestamp:	192.168.2.23112.187.174.20457618802839471 05/27/22-12:31:23.569091
SID:	2839471
Source Port:	57618
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.249.121.153

Timestamp:	192.168.2.2388.249.121.15335810802839471 05/27/22-12:33:32.552249
SID:	2839471
Source Port:	35810
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.18.254.57

Timestamp:	192.168.2.2395.18.254.5759420802839471 05/27/22-12:33:03.227728
SID:	2839471
Source Port:	59420
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.84.184.123

Timestamp:	192.168.2.23112.84.184.12345694802839471 05/27/22-12:33:25.000957
SID:	2839471
Source Port:	45694
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.201.52.51

Timestamp:	192.168.2.2388.201.52.5153612802839471 05/27/22-12:31:21.447416
SID:	2839471
Source Port:	53612
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.84.220.99

Timestamp:	192.168.2.23112.84.220.9939174802839471 05/27/22-12:32:02.417435
SID:	2839471
Source Port:	39174
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.197.186.69

Timestamp:	192.168.2.23112.197.186.6934310802839471 05/27/22-12:34:17.929289
SID:	2839471
Source Port:	34310
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.110.156.50

Timestamp:	192.168.2.2395.110.156.5059712802839471 05/27/22-12:31:56.929753
SID:	2839471
Source Port:	59712
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.65.15.147

Timestamp:	192.168.2.2395.65.15.14756142802839471 05/27/22-12:32:36.806859
SID:	2839471
Source Port:	56142
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.56.77.31

Timestamp:	192.168.2.2395.56.77.3144018802839471 05/27/22-12:31:01.178429
SID:	2839471
Source Port:	44018
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.173.11

Timestamp:	192.168.2.2388.99.173.1142122802839471 05/27/22-12:34:00.363964
SID:	2839471
Source Port:	42122
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.184.22.97

Timestamp:	192.168.2.23112.184.22.9750054802839471 05/27/22-12:34:15.300043
SID:	2839471
Source Port:	50054
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.17.60.219

Timestamp:	192.168.2.23112.17.60.21942544802839471 05/27/22-12:31:26.982240
SID:	2839471
Source Port:	42544
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.10.28

Timestamp:	192.168.2.2395.100.10.2841958802839471 05/27/22-12:34:29.402917
SID:	2839471
Source Port:	41958
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.136.69

Timestamp:	192.168.2.2388.198.136.6953612802839471 05/27/22-12:31:29.021624
SID:	2839471
Source Port:	53612
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.124.202.59

Timestamp:	192.168.2.23112.124.202.5949138802839471 05/27/22-12:32:33.941935
SID:	2839471
Source Port:	49138
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.177.75.25

Timestamp:	192.168.2.23112.177.75.2539808802839471 05/27/22-12:32:52.499221
SID:	2839471
Source Port:	39808
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.214.189.219

Timestamp:	192.168.2.2388.214.189.21950920802839471 05/27/22-12:31:09.651368
SID:	2839471
Source Port:	50920
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.38.125.78

Timestamp:	192.168.2.2395.38.125.7843592802839471 05/27/22-12:34:00.555290
SID:	2839471
Source Port:	43592
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.230.242

Timestamp:	192.168.2.2395.101.230.24241354802839471 05/27/22-12:32:56.792589
SID:	2839471
Source Port:	41354
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.81.113.147

Timestamp:	192.168.2.2395.81.113.14750458802839471 05/27/22-12:34:04.042063
SID:	2839471
Source Port:	50458
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.165.232.154

Timestamp:	192.168.2.23112.165.232.15442434802839471 05/27/22-12:31:00.635005
SID:	2839471
Source Port:	42434
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.80.109.205

Timestamp:	192.168.2.2395.80.109.20545616802839471 05/27/22-12:33:44.171390
SID:	2839471
Source Port:	45616
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.110.131.91

Timestamp:	192.168.2.2395.110.131.9152760802839471 05/27/22-12:33:06.964903
SID:	2839471
Source Port:	52760
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.209.121

Timestamp:	192.168.2.2395.217.209.12134086802839471 05/27/22-12:31:19.799060
SID:	2839471
Source Port:	34086
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.225.130

Timestamp:	192.168.2.2395.101.225.13057228802839471 05/27/22-12:31:19.784946
SID:	2839471
Source Port:	57228
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.93.106.224

Timestamp:	192.168.2.2395.93.106.22447370802839471 05/27/22-12:32:21.246012
SID:	2839471
Source Port:	47370
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Uses known network protocols on non-standard ports

System Summary

Sample tries to kill multiple processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

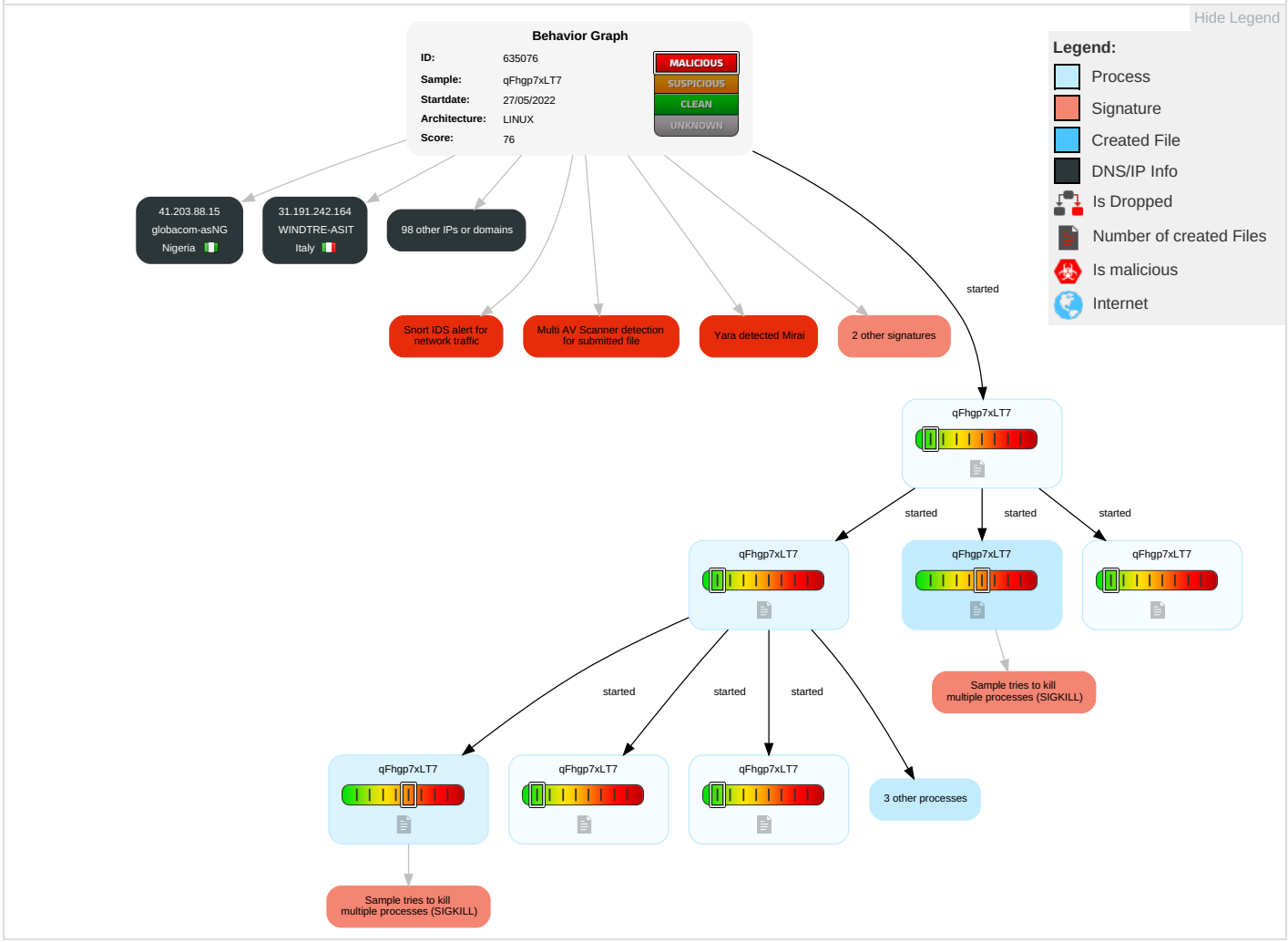
Mitre Att&ck Matrix

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	Path Interception	Direct Volume Access	1 OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Service Stop
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	4 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
qFhgp7xLT7	57%	Virustotal		Browse
qFhgp7xLT7	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.95.55.16/bins/x86	100%	Avira URL Cloud	malware	
http://45.95.55.16/8UsA.sh;	100%	Avira URL Cloud	malware	
http://102.129.143.42:45766/	0%	Avira URL Cloud	safe	
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

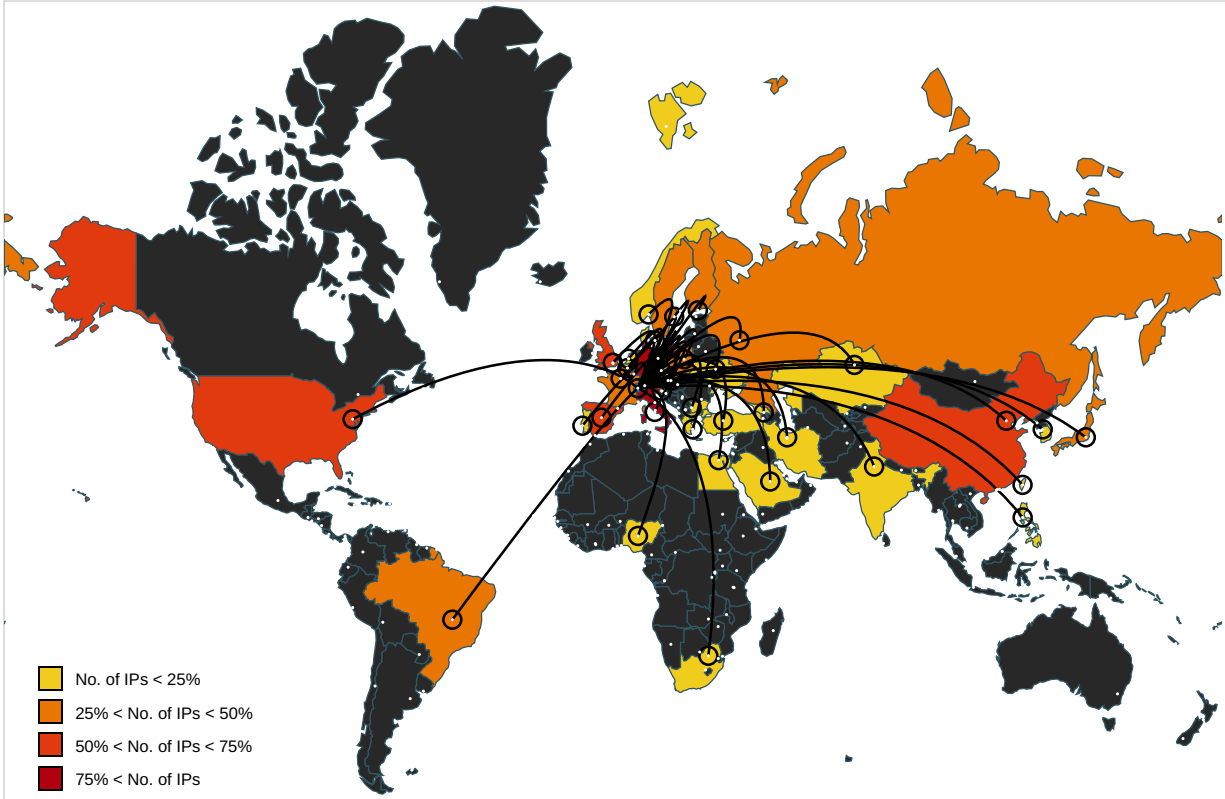
No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://102.129.143.42:45766/	false	• Avira URL Cloud: safe	unknown
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.253.206.97	unknown	Germany		3320	DTAGInternetserviceproviderOperationsDE	false
95.145.60.28	unknown	United Kingdom		12576	EELtdGB	false
94.159.123.250	unknown	Russian Federation		49531	NETCOM-R-ASRU	false
201.30.209.120	unknown	Brazil		4230	CLAROSABR	false
88.146.190.11	unknown	Czech Republic		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
31.220.220.235	unknown	United Kingdom		42689	GLIDEGB	false
94.99.181.106	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
95.195.139.134	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
85.84.200.25	unknown	Spain		12338	EUSKALTELES	false
94.94.61.52	unknown	Italy		3269	ASN-IBSNAZIT	false
95.109.203.228	unknown	Ukraine		34610	RIKSNETSE	false
94.42.250.14	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
94.55.185.148	unknown	Turkey		47524	TURKSAT-ASTR	false
169.26.51.250	unknown	United States		37611	AfrihostZA	false
62.141.160.9	unknown	Germany		20588	FVBDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.235.98.9	unknown	Italy		3269	ASN-IBSNAZIT	false
62.60.239.87	unknown	Iran (ISLAMIC Republic Of)		18013	ASLINE-AS-APASLINELIMITEDHK	false
85.4.81.27	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
62.35.119.106	unknown	France		5410	BOUYGTEL-ISPFR	false
95.115.114.37	unknown	Germany		6805	TDDE-ASN1DE	false
157.29.93.233	unknown	Italy		8968	BT-ITALIAIT	false
163.16.181.143	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
31.191.242.164	unknown	Italy		24608	WINDTRE-ASIT	false
95.117.176.89	unknown	Germany		6805	TDDE-ASN1DE	false
41.203.88.15	unknown	Nigeria		37148	globacom-asNG	false
62.129.56.59	unknown	Czech Republic		30764	PODA-ASCZ	false
157.114.204.191	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
94.72.179.67	unknown	Bulgaria		42735	MAXTELECOM-ASBG	false
96.173.246.144	unknown	United States		7922	COMCAST-7922US	false
95.221.2.232	unknown	Russian Federation		12714	TI-ASMoscowRussiaRU	false
85.18.200.222	unknown	Italy		12874	FASTWEBIT	false
94.8.166.131	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
31.85.14.80	unknown	United Kingdom		12576	EELtdGB	false
94.137.178.59	unknown	Georgia		16010	MAGTICOMASCaucasus-OnlineGE	false
62.181.174.193	unknown	Poland		12741	AS-NETIAWarszawa02-822PL	false
85.248.194.82	unknown	Slovakia (SLOVAK Republic)		5578	AS-BENESTRABratislavaSlovakRepublicSK	false
157.113.23.17	unknown	Japan		9993	CTC-ODCITOCHUTechno-SolutionsCorporationJP	false
138.99.154.13	unknown	Brazil		264205	ENInformaticaProvedordeInternetLTDA-MEBR	false
62.181.174.195	unknown	Poland		12741	AS-NETIAWarszawa02-822PL	false
17.137.34.147	unknown	United States		714	APPLE-ENGINEERINGUS	false
62.58.31.144	unknown	Belgium		13127	VERSATELASfortheTrans-EuropeanTele2IPTransportbackbo	false
94.226.96.232	unknown	Belgium		6848	TELENET-ASBE	false
85.23.76.207	unknown	Finland		16086	DNAFI	false
115.244.44.117	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
93.13.252.32	unknown	France		15557	LDCOMNETFR	false
62.198.53.98	unknown	Denmark		3308	TELIANET-DENMARKDK	false
95.87.151.78	unknown	Slovenia		2107	ARNES-NETAcademicandResearchNetworkofSloveniaSI	false
112.207.198.197	unknown	Philippines		9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	false
191.140.250.68	unknown	Brazil		26615	TIMSABR	false
31.210.249.105	unknown	Sweden		35706	NAOSE	false
62.130.69.46	unknown	United Kingdom		12337	NORIS-NETWORKITServiceProviderlocatedinNuernbergGerm	false
85.48.34.102	unknown	Spain		12479	UNI2-ASES	false
95.152.245.248	unknown	United Kingdom		8190	MDNXGB	false
85.203.114.30	unknown	France		30801	OZONE53avenuedelapierrevalleeFR	false
95.38.211.215	unknown	Iran (ISLAMIC Republic Of)		41881	FANAVA-ASFanavaGroupCommunicationCoIR	false
62.69.168.200	unknown	Finland		59766	ASWICITYIT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.194.33.151	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
31.249.160.244	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
41.145.255.155	unknown	South Africa		5713	SAIX-NETZA	false
134.233.80.36	unknown	United States		531	DNIC-AS-00531US	false
85.145.61.252	unknown	Netherlands		50266	TMOBILE-THUISNL	false
62.154.36.54	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
85.251.82.24	unknown	Spain		12357	COMUNITELSPAINES	false
95.255.148.99	unknown	Italy		3269	ASN-IBSNAZIT	false
85.4.81.41	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
85.246.119.70	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
112.168.206.75	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
34.96.170.37	unknown	United States		15169	GOOGLEUS	false
31.142.125.232	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
133.202.207.37	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
85.84.200.51	unknown	Spain		12338	EUSKALTELES	false
31.2.10.21	unknown	Poland		21243	PLUSNETPlusGSMtransitcorenetworkPL	false
31.138.187.95	unknown	Netherlands		15480	VFNL-ASVodafoneNLAutonomousSystemNL	false
95.17.57.3	unknown	Spain		12479	UNI2-ASES	false
120.204.61.130	unknown	China		24400	CMNET-V4SHANGHAI-AS-APShanghaiMobileCommunicationsCoLt	false
94.94.36.76	unknown	Italy		3269	ASN-IBSNAZIT	false
95.214.171.221	unknown	Germany		398083	TING-WIRELESSUS	false
197.132.199.82	unknown	Egypt		24835	RAYA-ASEG	false
94.193.8.111	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
182.142.116.186	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
85.86.237.89	unknown	Spain		12338	EUSKALTELES	false
112.229.41.35	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
64.250.214.67	unknown	United States		11650	PLDIUS	false
94.81.248.205	unknown	Italy		3269	ASN-IBSNAZIT	false
81.167.199.108	unknown	Norway		29695	ALTIBOX_ASNorwayNO	false
85.4.81.34	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
62.74.8.188	unknown	Greece		12361	PANAFONET-ASAthensGreeceGR	false
94.22.161.90	unknown	Finland		15527	ANVIASilmukkatie6VaasaFinlandFI	false
95.58.131.6	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
211.110.246.112	unknown	Korea Republic of		18302	SKG_NW-AS-KRSKTelecomKR	false
112.99.5.255	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
85.225.228.65	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
31.230.126.182	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
95.25.159.120	unknown	Russian Federation		3216	SOVAM-ASRU	false
170.179.27.54	unknown	China		11685	HNBCOL-ASUS	false
107.12.162.47	unknown	United States		11426	TWC-11426-CAROLINASUS	false
31.234.6.33	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
117.29.208.192	unknown	China		133776	CHINATELECOM-FUJIAN-QUANZHOU-IDC1QuanzhouCN	false
94.85.243.94	unknown	Italy		3269	ASN-IBSNAZIT	false
85.47.176.191	unknown	Italy		3269	ASN-IBSNAZIT	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.429540192344578
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	qFhgp7xLT7
File size:	62224
MD5:	60c16bbdea70d058618c85e3e7d5a7c5
SHA1:	333cc469a02c21fdde6206127bc0656919f7d05c
SHA256:	3d8b14056393a46c2f3b2c2db245f3d3bef205eae544ab7a01cb47d56cbb8e8c
SHA512:	0f06345bb69568cea61c1957c58a86ebf2226fa1121030fc7b53f35faf47ad7bf8a025fcfc2a570349224fd88d741a2545f850621ab0ac4a43b8c3ca37ffcd2a
SSDEEP:	1536:VMzVhePhrkmetvEucklzN/hkfgiu5BSSs84llZ6fUoBiA+pTLEx:VMzVhePlkmetvBcxJhyu5BNAlg9oAuf
TLSH:	AF5339C0A993DCF2DD1146B93177FF328636F436212AE9E7D7D9A923AC81E40910729D
File Content Preview:	.ELF.....d...4.....4. ...(.....p...p..@.....Q.td.....U..S.....w....h..... []...$.....U.....=@q...t..5....$p.....$p.....u.....t....h.o.....

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8048164
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	61824
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0xe116	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x80561c6	0xe1c6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x80561e0	0xe1e0	0xd20	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8057000	0xf000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8057008	0xf008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8057020	0xf020	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8057140	0xf140	0x6a0	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xf140	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0xef00	0xef00	3.9502	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0xf000	0x8057000	0x8057000	0x140	0x7e0	2.5837	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23112.72.202.70372348028394710 5/27/22-12:33:25.144916	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37234	80	192.168.2.23	112.72.202.70
192.168.2.2388.248.3.1233844802839471 05/27/22-12:32:09.515172	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33844	80	192.168.2.23	88.248.3.12
192.168.2.2388.221.67.12845550802839471 05/27/22-12:31:17.612604	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45550	80	192.168.2.23	88.221.67.128

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.198.95.58 34904802839471 05/27/22-12:33:19.894224	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34904	80	192.168.2.23	88.198.95.58
192.168.2.2395.216.157.1 3536388802839471 05/27/22-12:31:45.532082	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36388	80	192.168.2.23	95.216.157.135
192.168.2.2388.80.187.20 54684802839471 05/27/22-12:31:48.571853	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54684	80	192.168.2.23	88.80.187.20
192.168.2.23112.186.20.3 843052802839471 05/27/22-12:32:37.328412	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43052	80	192.168.2.23	112.186.20.38
192.168.2.2395.142.154.3 538450802839471 05/27/22-12:33:45.996466	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38450	80	192.168.2.23	95.142.154.35
192.168.2.2388.119.176.7 846082802839471 05/27/22-12:31:17.602521	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46082	80	192.168.2.23	88.119.176.78
192.168.2.2388.202.185.3 443256802839471 05/27/22-12:31:48.544252	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43256	80	192.168.2.23	88.202.185.34
192.168.2.2395.213.144.2 3458586802839471 05/27/22-12:31:56.949860	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58586	80	192.168.2.23	95.213.144.234
192.168.2.23112.72.55.52 40524802839471 05/27/22-12:33:51.607828	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40524	80	192.168.2.23	112.72.55.52
192.168.2.2388.221.182.1 0450788802839471 05/27/22-12:32:43.974254	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50788	80	192.168.2.23	88.221.182.104
192.168.2.2395.181.216.1 8845576802839471 05/27/22-12:31:45.532015	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45576	80	192.168.2.23	95.181.216.188
192.168.2.2395.216.46.56 38706802839471 05/27/22-12:30:59.349797	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38706	80	192.168.2.23	95.216.46.56
192.168.2.23112.197.186. 6934248802839471 05/27/22-12:34:15.486204	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34248	80	192.168.2.23	112.197.186.69
192.168.2.2395.85.49.125 57494802839471 05/27/22-12:31:01.042653	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57494	80	192.168.2.23	95.85.49.125
192.168.2.2395.101.51.17 833806802839471 05/27/22-12:34:11.712649	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33806	80	192.168.2.23	95.101.51.178
192.168.2.2388.248.97.42 51404802839471 05/27/22-12:31:19.756383	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51404	80	192.168.2.23	88.248.97.42
192.168.2.23112.211.86.2 2251576802839471 05/27/22-12:31:28.539011	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51576	80	192.168.2.23	112.211.86.222
192.168.2.23197.234.59.4 957624372152835222 05/27/22-12:33:52.815817	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57624	37215	192.168.2.23	197.234.59.49
192.168.2.2395.217.223.8 845340802839471 05/27/22-12:31:01.059678	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45340	80	192.168.2.23	95.217.223.88

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.80.109.205545624802839471 05/27/22-12:33:44.241244	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45624	80	192.168.2.23	95.80.109.205
192.168.2.2395.183.11.6060636802839471 05/27/22-12:31:33.291681	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60636	80	192.168.2.23	95.183.11.60
192.168.2.2388.153.193.1055722680283947 1 05/27/22-12:33:32.506696	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57226	80	192.168.2.23	88.153.193.105
192.168.2.23112.186.70.8049836802839471 05/27/22-12:31:46.023807	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49836	80	192.168.2.23	112.186.70.80
192.168.2.2395.110.179.2294744280283947 1 05/27/22-12:32:12.681029	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47442	80	192.168.2.23	95.110.179.229
192.168.2.23112.166.221.9432838802839471 05/27/22-12:32:39.180234	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	32838	80	192.168.2.23	112.166.221.94
192.168.2.2388.212.1.16633040802839471 05/27/22-12:32:16.185110	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33040	80	192.168.2.23	88.212.1.166
192.168.2.2395.14.86.19846290802839471 05/27/22-12:31:33.281866	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46290	80	192.168.2.23	95.14.86.198
192.168.2.23112.167.174.10546562802839471 05/27/22-12:31:50.944811	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46562	80	192.168.2.23	112.167.174.105
192.168.2.23112.186.20.3843220802839471 05/27/22-12:32:47.374861	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43220	80	192.168.2.23	112.186.20.38
192.168.2.2388.119.146.2644976802839471 05/27/22-12:33:27.528059	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44976	80	192.168.2.23	88.119.146.26
192.168.2.2388.225.227.2443382080283947 1 05/27/22-12:31:06.463207	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33820	80	192.168.2.23	88.225.227.244
192.168.2.23112.81.130.6753396802839471 05/27/22-12:31:51.424495	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53396	80	192.168.2.23	112.81.130.67
192.168.2.2395.56.61.339992802839471 05/27/22-12:31:33.483422	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39992	80	192.168.2.23	95.56.61.3
192.168.2.23112.175.41.18034328802839471 05/27/22-12:32:13.340256	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34328	80	192.168.2.23	112.175.41.180
192.168.2.23112.74.93.13439556802839471 05/27/22-12:32:02.442088	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39556	80	192.168.2.23	112.74.93.134
192.168.2.2388.221.40.18858726802839471 05/27/22-12:31:54.763991	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58726	80	192.168.2.23	88.221.40.188
192.168.2.2395.56.210.23144612802839471 05/27/22-12:31:00.444715	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44612	80	192.168.2.23	95.56.210.231
192.168.2.2395.211.24.21636048802839471 05/27/22-12:34:29.393344	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36048	80	192.168.2.23	95.211.24.216

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.163.202.3455820802839471 05/27/22-12:31:35.237352	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55820	80	192.168.2.23	95.163.202.34
192.168.2.2388.218.28.7358892802839471 05/27/22-12:32:18.783163	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58892	80	192.168.2.23	88.218.28.73
192.168.2.2395.100.7.13456148802839471 05/27/22-12:33:06.960464	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56148	80	192.168.2.23	95.100.7.134
192.168.2.2395.174.197.18435646802839471 05/27/22-12:31:11.849947	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35646	80	192.168.2.23	95.174.197.184
192.168.2.23112.74.79.4439520802839471 05/27/22-12:31:50.936841	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39520	80	192.168.2.23	112.74.79.44
192.168.2.23112.149.226.20155834802839471 05/27/22-12:32:37.572523	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55834	80	192.168.2.23	112.149.226.201
192.168.2.23112.186.20.384310480283947 1 05/27/22-12:32:41.687023	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43104	80	192.168.2.23	112.186.20.38
192.168.2.2395.168.210.3346156802839471 05/27/22-12:32:06.984091	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46156	80	192.168.2.23	95.168.210.33
192.168.2.2395.211.152.13753944802839471 05/27/22-12:32:18.728402	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53944	80	192.168.2.23	95.211.152.137
192.168.2.2395.142.205.21235762802839471 05/27/22-12:31:34.926249	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35762	80	192.168.2.23	95.142.205.212
192.168.2.2395.238.152.22358532802839471 05/27/22-12:32:22.621176	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58532	80	192.168.2.23	95.238.152.223
192.168.2.2395.100.70.247368028028394 71 05/27/22-12:32:30.210014	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36802	80	192.168.2.23	95.100.70.247
192.168.2.2395.58.244.6440006802839471 05/27/22-12:32:30.316788	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40006	80	192.168.2.23	95.58.244.64
192.168.2.2388.198.151.10550458802839471 05/27/22-12:31:23.849032	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50458	80	192.168.2.23	88.198.151.105
192.168.2.2395.65.82.20149266802839471 05/27/22-12:34:15.312931	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49266	80	192.168.2.23	95.65.82.201
192.168.2.2388.87.122.4440572802839471 05/27/22-12:31:54.832677	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40572	80	192.168.2.23	88.87.122.44
192.168.2.2395.20.119.9339774802839471 05/27/22-12:33:53.002379	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39774	80	192.168.2.23	95.20.119.93
192.168.2.23112.214.91.943860802839471 05/27/22-12:34:06.593929	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43860	80	192.168.2.23	112.214.91.9
192.168.2.23112.124.202.5949088802839471 05/27/22-12:32:30.928386	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49088	80	192.168.2.23	112.124.202.59

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.154.219.6 738350802839471 05/27/22- 12:32:36.726942	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38350	80	192.168.2.23	95.154.219.67
192.168.2.2395.100.84.18 252118802839471 05/27/22- 12:31:38.667115	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52118	80	192.168.2.23	95.100.84.182
192.168.2.2395.235.105.2 0446940802839471 05/27/22- 12:33:12.901640	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46940	80	192.168.2.23	95.235.105.204
192.168.2.23112.178.147. 9751130802839471 05/27/22- 12:31:28.520517	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51130	80	192.168.2.23	112.178.147.97
192.168.2.2395.100.204.1 1037574802839471 05/27/22- 12:31:00.396025	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37574	80	192.168.2.23	95.100.204.110
192.168.2.2388.198.137.1 5253476802839471 05/27/22- 12:31:42.335689	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53476	80	192.168.2.23	88.198.137.152
192.168.2.2395.154.221.1 7751686802839471 05/27/22- 12:32:22.567031	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51686	80	192.168.2.23	95.154.221.177
192.168.2.2388.99.84.424 4326802839471 05/27/22- 12:31:54.754494	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44326	80	192.168.2.23	88.99.84.42
192.168.2.2395.217.82.74 6910802839471 05/27/22- 12:31:19.799558	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46910	80	192.168.2.23	95.217.82.7
192.168.2.23112.164.173. 2357754802839471 05/27/22- 12:32:02.457344	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57754	80	192.168.2.23	112.164.173.23
192.168.2.23112.169.182. 14540522802839471 05/27/22- 12:31:28.532451	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40522	80	192.168.2.23	112.169.182.145
192.168.2.2395.211.189.2 0459478802839471 05/27/22- 12:33:00.977962	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59478	80	192.168.2.23	95.211.189.204
192.168.2.23112.171.40.2 2351266802839471 05/27/22- 12:34:26.065722	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51266	80	192.168.2.23	112.171.40.223
192.168.2.2388.98.181.15 749770802839471 05/27/22- 12:33:01.043025	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49770	80	192.168.2.23	88.98.181.157
192.168.2.2395.101.161.2 857428802839471 05/27/22- 12:31:33.308821	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57428	80	192.168.2.23	95.101.161.28
192.168.2.2395.58.113.55 9516802839471 05/27/22- 12:32:19.026650	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59516	80	192.168.2.23	95.58.113.5
192.168.2.2388.208.214.8 354508802839471 05/27/22- 12:33:14.819620	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54508	80	192.168.2.23	88.208.214.83
192.168.2.2395.59.245.20 43218802839471 05/27/22- 12:32:30.308154	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43218	80	192.168.2.23	95.59.245.20
192.168.2.2388.208.220.5 47198802839471 05/27/22- 12:31:23.868712	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47198	80	192.168.2.23	88.208.220.5

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.39.140.15 34816802839471 05/27/22-12:31:38.557073	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34816	80	192.168.2.23	95.39.140.15
192.168.2.2388.22.247.17 554798802839471 05/27/22-12:32:16.218137	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54798	80	192.168.2.23	88.22.247.175
192.168.2.2395.101.80.16 635368802839471 05/27/22-12:31:19.815486	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35368	80	192.168.2.23	95.101.80.166
192.168.2.2395.165.255.5 38992802839471 05/27/22-12:34:00.476246	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38992	80	192.168.2.23	95.165.255.5
192.168.2.2395.101.179.7 247718802839471 05/27/22-12:33:45.559487	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47718	80	192.168.2.23	95.101.179.72
192.168.2.2388.31.233.34 6718802839471 05/27/22-12:31:20.193652	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46718	80	192.168.2.23	88.31.233.3
192.168.2.2395.138.128.7 836584802839471 05/27/22-12:31:54.758519	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36584	80	192.168.2.23	95.138.128.78
192.168.2.2395.59.33.161 51250802839471 05/27/22-12:32:24.240623	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51250	80	192.168.2.23	95.59.33.161
192.168.2.2388.163.26.19 238608802839471 05/27/22-12:32:18.792798	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38608	80	192.168.2.23	88.163.26.192
192.168.2.2388.221.46.13 850426802839471 05/27/22-12:31:51.214773	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50426	80	192.168.2.23	88.221.46.138
192.168.2.2395.217.26.93 40238802839471 05/27/22-12:32:22.579519	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40238	80	192.168.2.23	95.217.26.93
192.168.2.2395.57.117.85 56186802839471 05/27/22-12:31:15.088619	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56186	80	192.168.2.23	95.57.117.85
192.168.2.2395.159.47.27 39312802839471 05/27/22-12:31:19.910781	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39312	80	192.168.2.23	95.159.47.27
192.168.2.2388.12.46.218 53806802839471 05/27/22-12:31:23.930863	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53806	80	192.168.2.23	88.12.46.218
192.168.2.2395.101.14.20 760674802839471 05/27/22-12:33:11.611379	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60674	80	192.168.2.23	95.101.14.207
192.168.2.2388.80.20.160 59264802839471 05/27/22-12:31:31.124184	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59264	80	192.168.2.23	88.80.20.160
192.168.2.2388.129.59.54 41168802839471 05/27/22-12:31:54.808552	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41168	80	192.168.2.23	88.129.59.54
192.168.2.2395.179.162.8 249118802839471 05/27/22-12:32:12.671842	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49118	80	192.168.2.23	95.179.162.82
192.168.2.2395.154.232.1 8054160802839471 05/27/22-12:31:19.786814	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54160	80	192.168.2.23	95.154.232.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.100.210.1 1343142802839471 05/27/22-12:31:56.914233	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43142	80	192.168.2.23	95.100.210.113
192.168.2.2388.247.209.7 656418802839471 05/27/22-12:32:44.011426	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56418	80	192.168.2.23	88.247.209.76
192.168.2.2395.101.78.21 536224802839471 05/27/22-12:32:22.566529	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36224	80	192.168.2.23	95.101.78.215
192.168.2.2395.111.194.2 3152466802839471 05/27/22-12:31:33.671458	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52466	80	192.168.2.23	95.111.194.231
192.168.2.2388.99.242.25 248898802839471 05/27/22-12:32:00.067857	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48898	80	192.168.2.23	88.99.242.252
192.168.2.2395.58.239.15 650468802839471 05/27/22-12:32:19.018154	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50468	80	192.168.2.23	95.58.239.156
192.168.2.2395.101.174.1 043504802839471 05/27/22-12:33:58.075621	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43504	80	192.168.2.23	95.101.174.10
192.168.2.2388.221.148.4 654120802839471 05/27/22-12:31:23.853653	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54120	80	192.168.2.23	88.221.148.46
192.168.2.2395.38.192.99 48692802839471 05/27/22-12:31:34.995858	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48692	80	192.168.2.23	95.38.192.99
192.168.2.2395.143.188.1 6843516802839471 05/27/22-12:31:45.547396	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43516	80	192.168.2.23	95.143.188.168
192.168.2.2388.221.77.15 57238802839471 05/27/22-12:33:39.992640	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57238	80	192.168.2.23	88.221.77.15
192.168.2.2388.99.222.19 559234802839471 05/27/22-12:31:17.577531	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59234	80	192.168.2.23	88.99.222.195
192.168.2.2395.58.157.17 757174802839471 05/27/22-12:31:38.540240	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57174	80	192.168.2.23	95.58.157.177
192.168.2.23112.74.142.3 459320802839471 05/27/22-12:31:23.802886	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59320	80	192.168.2.23	112.74.142.34
192.168.2.2395.100.186.1 7755934802839471 05/27/22-12:31:19.783764	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55934	80	192.168.2.23	95.100.186.177
192.168.2.23112.197.186. 6934232802839471 05/27/22-12:34:15.264649	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34232	80	192.168.2.23	112.197.186.69
192.168.2.2388.99.225.19 342160802839471 05/27/22-12:31:43.544055	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42160	80	192.168.2.23	88.99.225.193
192.168.2.2388.213.207.4 46980802839471 05/27/22-12:31:48.561691	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46980	80	192.168.2.23	88.213.207.4
192.168.2.2395.58.167.13 39100802839471 05/27/22-12:31:17.554715	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39100	80	192.168.2.23	95.58.167.13

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.169.212.14050382802839471 05/27/22-12:33:09.361075	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50382	80	192.168.2.23	95.169.212.140
192.168.2.23112.122.156.19160710802839471 05/27/22-12:32:09.446158	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60710	80	192.168.2.23	112.122.156.191
192.168.2.2395.181.216.13439360802839471 05/27/22-12:33:56.676376	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39360	80	192.168.2.23	95.181.216.134
192.168.2.2395.217.39.11039044802839471 05/27/22-12:31:34.961644	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39044	80	192.168.2.23	95.217.39.110
192.168.2.23112.165.103.7553042802839471 05/27/22-12:32:06.956682	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53042	80	192.168.2.23	112.165.103.75
192.168.2.2388.198.210.2041554802839471 05/27/22-12:33:48.061475	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41554	80	192.168.2.23	88.198.210.20
192.168.2.2395.111.247.19134022802839471 05/27/22-12:31:33.249723	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34022	80	192.168.2.23	95.111.247.191
192.168.2.2395.56.134.4155198802839471 05/27/22-12:33:43.132577	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55198	80	192.168.2.23	95.56.134.41
192.168.2.2395.143.218.15158842802839471 05/27/22-12:31:34.920579	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58842	80	192.168.2.23	95.143.218.151
192.168.2.2395.56.25.17758708802839471 05/27/22-12:33:11.671020	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58708	80	192.168.2.23	95.56.25.177
192.168.2.23112.45.117.15235872802839471 05/27/22-12:32:22.616897	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35872	80	192.168.2.23	112.45.117.152
192.168.2.2388.225.240.20647174802839471 05/27/22-12:32:00.123619	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47174	80	192.168.2.23	88.225.240.206
192.168.2.2395.139.131.7156624802839471 05/27/22-12:31:19.900307	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56624	80	192.168.2.23	95.139.131.71
192.168.2.23112.70.237.1542186802839471 05/27/22-12:32:16.418537	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42186	80	192.168.2.23	112.70.237.15
192.168.2.2395.100.48.23837696802839471 05/27/22-12:33:40.977680	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37696	80	192.168.2.23	95.100.48.238
192.168.2.2395.173.178.449408802839471 05/27/22-12:32:07.017851	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49408	80	192.168.2.23	95.173.178.4
192.168.2.2388.152.159.9645460802839471 05/27/22-12:32:18.787691	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45460	80	192.168.2.23	88.152.159.96
192.168.2.2395.217.143.5041066802839471 05/27/22-12:31:38.463113	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41066	80	192.168.2.23	95.217.143.50
192.168.2.23112.206.140.20648232802839471 05/27/22-12:33:29.276621	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48232	80	192.168.2.23	112.206.140.206

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23112.48.170.1034680680283947105/27/22-12:31:51.437308	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46806	80	192.168.2.23	112.48.170.103
192.168.2.2395.111.251.3158270802839471 05/27/22-12:34:13.924270	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58270	80	192.168.2.23	95.111.251.31
192.168.2.2395.216.138.20456560802839471 05/27/22-12:32:06.997755	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56560	80	192.168.2.23	95.216.138.204
192.168.2.2395.217.64.21642418802839471 05/27/22-12:31:38.463136	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42418	80	192.168.2.23	95.217.64.216
192.168.2.2395.164.219.10052268802839471 05/27/22-12:32:07.060866	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52268	80	192.168.2.23	95.164.219.100
192.168.2.2388.221.139.17341446802839471 05/27/22-12:31:15.018641	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41446	80	192.168.2.23	88.221.139.173
192.168.2.2388.221.111.2735636802839471 05/27/22-12:31:25.170536	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35636	80	192.168.2.23	88.221.111.27
192.168.2.2388.221.196.10042160802839471 05/27/22-12:31:29.023462	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42160	80	192.168.2.23	88.221.196.100
192.168.2.2388.103.173.6754636802839471 05/27/22-12:34:17.807413	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54636	80	192.168.2.23	88.103.173.67
192.168.2.23112.47.1.17334512802839471 05/27/22-12:32:15.868522	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34512	80	192.168.2.23	112.47.1.173
192.168.2.23112.200.243.9341862802839471 05/27/22-12:33:05.511661	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41862	80	192.168.2.23	112.200.243.93
192.168.2.2388.203.6.12952030802839471 05/27/22-12:31:45.486116	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52030	80	192.168.2.23	88.203.6.129
192.168.2.23112.197.186.6934662802839471 05/27/22-12:34:29.593435	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34662	80	192.168.2.23	112.197.186.69
192.168.2.2395.181.161.18833806802839471 05/27/22-12:32:12.680954	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33806	80	192.168.2.23	95.181.161.188
192.168.2.2388.211.83.7245092802839471 05/27/22-12:31:54.800343	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45092	80	192.168.2.23	88.211.83.72
192.168.2.2388.87.4.5151120802839471 05/27/22-12:31:15.092894	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51120	80	192.168.2.23	88.87.4.51
192.168.2.2395.179.180.15238212802839471 05/27/22-12:33:30.964976	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38212	80	192.168.2.23	95.179.180.152
192.168.2.2388.87.26.2551386802839471 05/27/22-12:31:15.092875	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51386	80	192.168.2.23	88.87.26.25
192.168.2.2388.34.44.17258598802839471 05/27/22-12:32:45.075473	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58598	80	192.168.2.23	88.34.44.172

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.221.111.2735596802839471 05/27/22-12:31:23.848429	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35596	80	192.168.2.23	88.221.111.27
192.168.2.23112.163.5.17945500802839471 05/27/22-12:31:23.584004	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45500	80	192.168.2.23	112.163.5.179
192.168.2.2388.86.215.22060880802839471 05/27/22-12:31:43.521931	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60880	80	192.168.2.23	88.86.215.220
192.168.2.23112.121.174.2733836802839471 05/27/22-12:32:12.885897	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33836	80	192.168.2.23	112.121.174.27
192.168.2.23112.211.189.10935672802839471 05/27/22-12:33:05.551569	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35672	80	192.168.2.23	112.211.189.109
192.168.2.2395.139.246.10660628802839471 05/27/22-12:31:00.389921	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60628	80	192.168.2.23	95.139.246.106
192.168.2.2395.245.178.853938802839471 05/27/22-12:32:18.853740	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53938	80	192.168.2.23	95.245.178.8
192.168.2.23112.211.85.7945736802839471 05/27/22-12:32:52.261918	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45736	80	192.168.2.23	112.211.85.79
192.168.2.2395.226.61.13044442802839471 05/27/22-12:33:05.595447	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44442	80	192.168.2.23	95.226.61.130
192.168.2.23112.196.112.11338078802839471 05/27/22-12:34:26.100254	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38078	80	192.168.2.23	112.196.112.113
192.168.2.2395.216.47.23354886802839471 05/27/22-12:32:06.997849	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54886	80	192.168.2.23	95.216.47.233
192.168.2.2395.213.212.18938108802839471 05/27/22-12:31:06.389031	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38108	80	192.168.2.23	95.213.212.189
192.168.2.23112.213.45.9234744802839471 05/27/22-12:31:23.654056	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34744	80	192.168.2.23	112.213.45.92
192.168.2.2388.255.55.21546638802839471 05/27/22-12:31:48.630707	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46638	80	192.168.2.23	88.255.55.215
192.168.2.2341.0.91.12739528372152835222 05/27/22-12:34:12.220909	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39528	37215	192.168.2.23	41.0.91.127
192.168.2.2388.216.103.15835942802839471 05/27/22-12:31:42.389093	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35942	80	192.168.2.23	88.216.103.158
192.168.2.2395.131.160.14457636802839471 05/27/22-12:32:36.982308	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57636	80	192.168.2.23	95.131.160.144
192.168.2.23112.35.79.5439488802839471 05/27/22-12:32:12.893316	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39488	80	192.168.2.23	112.35.79.54
192.168.2.2395.57.29.12344802802839471 05/27/22-12:33:01.063137	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44802	80	192.168.2.23	95.57.29.123

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.250.68.22 540434802839471 05/27/22-12:34:17.873487	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40434	80	192.168.2.23	88.250.68.225
192.168.2.2388.109.137.1 6250830802839471 05/27/22-12:32:53.097961	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50830	80	192.168.2.23	88.109.137.162
192.168.2.2388.221.205.1 139676802839471 05/27/22-12:32:22.952163	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39676	80	192.168.2.23	88.221.205.11
192.168.2.23112.172.108. 6844012802839471 05/27/22-12:31:26.456649	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44012	80	192.168.2.23	112.172.108.68
192.168.2.2395.101.65.18 134938802839471 05/27/22-12:34:15.279681	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34938	80	192.168.2.23	95.101.65.181
192.168.2.23112.74.184.1 6060202802839471 05/27/22-12:31:46.274302	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60202	80	192.168.2.23	112.74.184.160
192.168.2.2388.24.129.16 135668802839471 05/27/22-12:34:17.895514	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35668	80	192.168.2.23	88.24.129.161
192.168.2.2395.129.208.2 3659430802839471 05/27/22-12:32:22.558579	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59430	80	192.168.2.23	95.129.208.236
192.168.2.23112.14.5.224 50654802839471 05/27/22-12:32:06.968249	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50654	80	192.168.2.23	112.14.5.224
192.168.2.23112.213.102. 19753180802839471 05/27/22-12:31:40.096566	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53180	80	192.168.2.23	112.213.102.197
192.168.2.23112.197.186. 6934428802839471 05/27/22-12:34:21.537072	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34428	80	192.168.2.23	112.197.186.69
192.168.2.2395.151.147.3 752382802839471 05/27/22-12:31:33.320284	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52382	80	192.168.2.23	95.151.147.37
192.168.2.2388.225.231.2 4140972802839471 05/27/22-12:33:30.985507	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40972	80	192.168.2.23	88.225.231.241
192.168.2.23112.72.58.12 757136802839471 05/27/22-12:31:00.709407	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57136	80	192.168.2.23	112.72.58.127
192.168.2.2388.203.6.129 52022802839471 05/27/22-12:31:42.372374	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52022	80	192.168.2.23	88.203.6.129
192.168.2.2388.221.186.1 2234042802839471 05/27/22-12:31:43.549751	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34042	80	192.168.2.23	88.221.186.122
192.168.2.2395.77.153.13 50944802839471 05/27/22-12:31:34.999503	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50944	80	192.168.2.23	95.77.153.13
192.168.2.2395.217.232.1 0152404802839471 05/27/22-12:33:43.043686	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52404	80	192.168.2.23	95.217.232.101
192.168.2.2395.249.6.182 43248802839471 05/27/22-12:31:19.925251	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43248	80	192.168.2.23	95.249.6.182

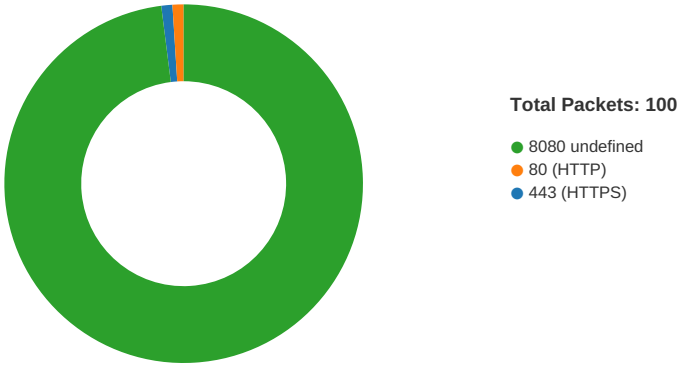
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23112.135.194.12947528802839471 05/27/22-12:32:27.557736	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47528	80	192.168.2.23	112.135.194.129
192.168.2.2395.140.155.24039534802839471 05/27/22-12:31:11.848254	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39534	80	192.168.2.23	95.140.155.240
192.168.2.2395.67.8.5649576802839471 05/27/22-12:31:54.770414	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49576	80	192.168.2.23	95.67.8.56
192.168.2.2395.163.251.19650388802839471 05/27/22-12:32:24.131657	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50388	80	192.168.2.23	95.163.251.196
192.168.2.2388.225.222.13260712802839471 05/27/22-12:32:44.015755	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60712	80	192.168.2.23	88.225.222.132
192.168.2.2388.99.205.207749030802839471 05/27/22-12:33:00.999487	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49030	80	192.168.2.23	88.99.205.207
192.168.2.2395.214.95.18560942802839471 05/27/22-12:31:45.629413	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60942	80	192.168.2.23	95.214.95.185
192.168.2.2388.203.102.18741940802839471 05/27/22-12:31:31.123524	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41940	80	192.168.2.23	88.203.102.187
192.168.2.2388.109.137.16250882802839471 05/27/22-12:32:56.716771	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50882	80	192.168.2.23	88.109.137.162
192.168.2.2395.9.242.10437384802839471 05/27/22-12:33:09.302194	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37384	80	192.168.2.23	95.9.242.104
192.168.2.2395.61.204.22037348802839471 05/27/22-12:32:36.837881	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37348	80	192.168.2.23	95.61.204.220
192.168.2.2395.71.129.22054036802839471 05/27/22-12:33:56.718060	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54036	80	192.168.2.23	95.71.129.220
192.168.2.2388.86.215.22060870802839471 05/27/22-12:31:45.496953	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60870	80	192.168.2.23	88.86.215.220
192.168.2.2395.209.132.11833830802839471 05/27/22-12:33:58.194099	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33830	80	192.168.2.23	95.209.132.118
192.168.2.2388.221.236.2257688802839471 05/27/22-12:32:16.195697	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57688	80	192.168.2.23	88.221.236.22
192.168.2.2395.101.229.3341400802839471 05/27/22-12:31:09.563382	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41400	80	192.168.2.23	95.101.229.33
192.168.2.2388.149.176.15243380802839471 05/27/22-12:32:16.195035	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43380	80	192.168.2.23	88.149.176.152
192.168.2.2395.101.208.13949116802839471 05/27/22-12:34:13.943690	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49116	80	192.168.2.23	95.101.208.139
192.168.2.2395.100.225.19844024802839471 05/27/22-12:31:06.356024	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44024	80	192.168.2.23	95.100.225.198

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.159.43.113 38992802839471 05/27/22-12:32:59.949064	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38992	80	192.168.2.23	95.159.43.113
192.168.2.2388.216.185.99 45494802839471 05/27/22-12:31:24.036858	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45494	80	192.168.2.23	88.216.185.99
192.168.2.2395.101.227.36 38306802839471 05/27/22-12:34:15.292281	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38306	80	192.168.2.23	95.101.227.36
192.168.2.2388.202.224.45 33472802839471 05/27/22-12:34:17.743999	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33472	80	192.168.2.23	88.202.224.45
192.168.2.2395.179.232.73 53852802839471 05/27/22-12:31:56.918991	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53852	80	192.168.2.23	95.179.232.73
192.168.2.2395.130.126.25 59386802839471 05/27/22-12:31:15.003635	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59386	80	192.168.2.23	95.130.126.25
192.168.2.23112.124.20.13 054500802839471 05/27/22-12:31:23.574128	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54500	80	192.168.2.23	112.124.20.130
192.168.2.2395.101.106.79 39324802839471 05/27/22-12:31:34.935665	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39324	80	192.168.2.23	95.101.106.79
192.168.2.2395.100.48.238 37708802839471 05/27/22-12:33:40.003945	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37708	80	192.168.2.23	95.100.48.238
192.168.2.2395.245.107.15 543538802839471 05/27/22-12:31:56.958042	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43538	80	192.168.2.23	95.245.107.155
192.168.2.2395.100.149.24 37798802839471 05/27/22-12:33:06.925655	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37798	80	192.168.2.23	95.100.149.24
192.168.2.2388.148.79.180 59856802839471 05/27/22-12:32:49.499358	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59856	80	192.168.2.23	88.148.79.180
192.168.2.23112.187.174.2 0457618802839471 05/27/22-12:31:23.569091	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57618	80	192.168.2.23	112.187.174.204
192.168.2.2388.249.121.15 335810802839471 05/27/22-12:33:32.552249	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35810	80	192.168.2.23	88.249.121.153
192.168.2.2395.18.254.57 59420802839471 05/27/22-12:33:03.227728	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59420	80	192.168.2.23	95.18.254.57
192.168.2.23112.84.184.12 345694802839471 05/27/22-12:33:25.000957	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45694	80	192.168.2.23	112.84.184.123
192.168.2.2388.201.52.51 53612802839471 05/27/22-12:31:21.447416	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53612	80	192.168.2.23	88.201.52.51
192.168.2.23112.84.220.99 39174802839471 05/27/22-12:32:02.417435	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39174	80	192.168.2.23	112.84.220.99
192.168.2.23112.197.186.6 934310802839471 05/27/22-12:34:17.929289	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34310	80	192.168.2.23	112.197.186.69

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.110.156.5059712802839471 05/27/22-12:31:56.929753	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59712	80	192.168.2.23	95.110.156.50
192.168.2.2395.65.15.14756142802839471 05/27/22-12:32:36.806859	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56142	80	192.168.2.23	95.65.15.147
192.168.2.2395.56.77.3144018802839471 05/27/22-12:31:01.178429	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44018	80	192.168.2.23	95.56.77.31
192.168.2.2388.99.173.1142122802839471 05/27/22-12:34:00.363964	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42122	80	192.168.2.23	88.99.173.11
192.168.2.23112.184.22.97750054802839471 05/27/22-12:34:15.300043	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50054	80	192.168.2.23	112.184.22.97
192.168.2.23112.17.60.21942544802839471 05/27/22-12:31:26.982240	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42544	80	192.168.2.23	112.17.60.219
192.168.2.2395.100.10.2841958802839471 05/27/22-12:34:29.402917	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41958	80	192.168.2.23	95.100.10.28
192.168.2.2388.198.136.6953612802839471 05/27/22-12:31:29.021624	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53612	80	192.168.2.23	88.198.136.69
192.168.2.23112.124.202.5949138802839471 05/27/22-12:32:33.941935	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49138	80	192.168.2.23	112.124.202.59
192.168.2.23112.177.75.2539808802839471 05/27/22-12:32:52.499221	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39808	80	192.168.2.23	112.177.75.25
192.168.2.2388.214.189.21950920802839471 05/27/22-12:31:09.651368	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50920	80	192.168.2.23	88.214.189.219
192.168.2.2395.38.125.7843592802839471 05/27/22-12:34:00.555290	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43592	80	192.168.2.23	95.38.125.78
192.168.2.2395.101.230.24241354802839471 05/27/22-12:32:56.792589	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41354	80	192.168.2.23	95.101.230.242
192.168.2.2395.81.113.14750458802839471 05/27/22-12:34:04.042063	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50458	80	192.168.2.23	95.81.113.147
192.168.2.23112.165.232.15442434802839471 05/27/22-12:31:00.635005	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42434	80	192.168.2.23	112.165.232.154
192.168.2.2395.80.109.20545616802839471 05/27/22-12:33:44.171390	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45616	80	192.168.2.23	95.80.109.205
192.168.2.2395.110.131.9152760802839471 05/27/22-12:33:06.964903	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52760	80	192.168.2.23	95.110.131.91
192.168.2.2395.217.209.12134086802839471 05/27/22-12:31:19.799060	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34086	80	192.168.2.23	95.217.209.121
192.168.2.2395.101.225.13057228802839471 05/27/22-12:31:19.784946	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57228	80	192.168.2.23	95.101.225.130

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.93.106.22 4473708028394710 5/27/22-12:32:21.246012	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47370	80	192.168.2.23	95.93.106.224

Network Port Distribution



TCP Packets

HTTP Request Dependency Graph

- 192.168.0.14:80
- 102.129.143.42:45766

System Behavior

Analysis Process: qFhgp7xLT7 PID: **6237**, Parent PID: **6125**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	/tmp/qFhgp7xLT7
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

Analysis Process: qFhgp7xLT7 PID: **6238**, Parent PID: **6237**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

File Activities

File Read

Directory Enumerated

Analysis Process: qFhgp7xLT7 PID: **6239**, Parent PID: **6237**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

Analysis Process: qFhgp7xLT7 PID: **6240**, Parent PID: **6237**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

Analysis Process: qFhgp7xLT7 PID: **6241**, Parent PID: **6240**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

Analysis Process: qFhgp7xLT7 PID: **6242**, Parent PID: **6240**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

Analysis Process: qFhgp7xLT7 PID: **6244**, Parent PID: **6240**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

Analysis Process: qFhgp7xLT7 PID: **6245**, Parent PID: **6240**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes

MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

File Activities

File Read

Directory Enumerated

Analysis Process: qFhgp7xLT7 PID: **6246**, Parent PID: **6240**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5

Analysis Process: qFhgp7xLT7 PID: **6247**, Parent PID: **6240**

General

Start time:	12:30:55
Start date:	27/05/2022
Path:	/tmp/qFhgp7xLT7
Arguments:	n/a
File size:	62224 bytes
MD5 hash:	60c16bbdea70d058618c85e3e7d5a7c5