ID: 635088
Sample Name: 4R66Cv0FvN
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:02:54
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

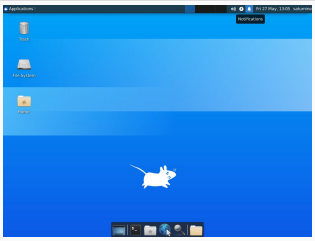
Linux Analysis Report

4R66Cv0FvN

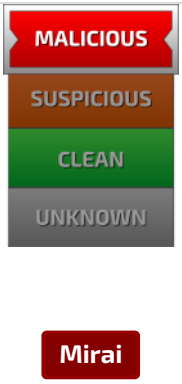
Overview

General Information

Sample Name:	4R66Cv0FvN
Analysis ID:	635088
MD5:	1a7dc7e371dd56..
SHA1:	96f35b9dee1d4a..
SHA256:	d3063711060e76.
Tags:	32 elf mirai motorola
Infos:	



Detection

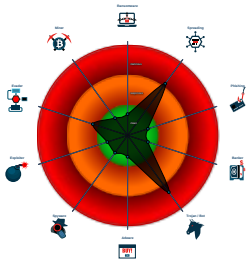


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

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

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.

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:	635088
Start date and time: 27/05/202213:02:54	2022-05-27 13:02:54 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4R66Cv0FvN
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:	mal72.spre.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/4R66Cv0FvN
PID:	6226
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected By Cult
Standard Error:	

Copyright Joe Security LLC 2022

Process Tree

- **system is lnxubuntu20**
- 4R66Cv0FvN (PID: 6226, Parent: 6121, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/4R66Cv0FvN
  - 4R66Cv0FvN New Fork (PID: 6228, Parent: 6226)
  - 4R66Cv0FvN New Fork (PID: 6229, Parent: 6226)
  - 4R66Cv0FvN New Fork (PID: 6230, Parent: 6226)
    - 4R66Cv0FvN New Fork (PID: 6234, Parent: 6230)
    - 4R66Cv0FvN New Fork (PID: 6235, Parent: 6230)
    - 4R66Cv0FvN New Fork (PID: 6238, Parent: 6230)
    - 4R66Cv0FvN New Fork (PID: 6239, Parent: 6230)
    - 4R66Cv0FvN New Fork (PID: 6242, Parent: 6230)
    - 4R66Cv0FvN New Fork (PID: 6244, Parent: 6230)
- **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: 112.78.149.155

Timestamp:	192.168.2.23112.78.149.15556872802839471 05/27/22-13:04:20.602390
SID:	2839471
Source Port:	56872
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.181.211.245

Timestamp:	192.168.2.2395.181.211.24543264802839471 05/27/22-13:05:39.450028
SID:	2839471
Source Port:	43264
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.239.33.52

Timestamp:	192.168.2.2395.239.33.5235314802839471 05/27/22-13:05:39.448496
SID:	2839471
Source Port:	35314
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.150.171.120

Timestamp:	192.168.2.2388.150.171.12034138802839471 05/27/22-13:04:25.483580
SID:	2839471
Source Port:	34138
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.147.150.44

Copyright Joe Security LLC 2022

Timestamp:	192.168.2.2388.147.150.4437374802839471 05/27/22-13:05:56.529243
SID:	2839471
Source Port:	37374
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.158.8.211

Timestamp:	192.168.2.2395.158.8.21139560802839471 05/27/22-13:05:14.237720
SID:	2839471
Source Port:	39560
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.158.141.220

Timestamp:	192.168.2.2395.158.141.22045834802839471 05/27/22-13:04:08.194012
SID:	2839471
Source Port:	45834
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.135.207.165

Timestamp:	192.168.2.23112.135.207.16556904802839471 05/27/22-13:06:05.012803
SID:	2839471
Source Port:	56904
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.116.44

Timestamp:	192.168.2.2395.100.116.4450488802839471 05/27/22-13:05:21.570636
SID:	2839471
Source Port:	50488
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.184.216

Timestamp:	192.168.2.2388.198.184.21648512802839471 05/27/22-13:04:25.431447
SID:	2839471
Source Port:	48512
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.78.9.203

Timestamp:	192.168.2.23112.78.9.20333502802839471 05/27/22-13:04:30.438295
SID:	2839471
Source Port:	33502
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.123.225

Timestamp:	192.168.2.2395.100.123.22559388802839471 05/27/22-13:03:53.103631
SID:	2839471
Source Port:	59388
Destination Port:	80

Copyright Joe Security LLC 2022

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.28.209.194

Timestamp:	192.168.2.23112.28.209.19459186802839471 05/27/22-13:05:31.839035
SID:	2839471
Source Port:	59186
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.85.99

Timestamp:	192.168.2.2395.101.85.9953610802839471 05/27/22-13:04:15.943706
SID:	2839471
Source Port:	53610
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.13.87.237

Timestamp:	192.168.2.23112.13.87.23736212802839471 05/27/22-13:04:37.094351
SID:	2839471
Source Port:	36212
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.44.74

Timestamp:	192.168.2.2388.221.44.7438338802839471 05/27/22-13:05:56.289401
SID:	2839471
Source Port:	38338
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.91.4.16

Timestamp:	192.168.2.2395.91.4.1657994802839471 05/27/22-13:04:33.477633
SID:	2839471
Source Port:	57994
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.30.198.60

Timestamp:	192.168.2.23112.30.198.6034490802839471 05/27/22-13:04:15.929622
SID:	2839471
Source Port:	34490
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.252.166.0

Timestamp:	192.168.2.2388.252.166.043712802839471 05/27/22-13:04:53.868578
SID:	2839471
Source Port:	43712
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.60.236.169

Timestamp:	192.168.2.2395.60.236.16945234802839471 05/27/22-13:04:10.614944
SID:	2839471
Source Port:	45234
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.84.90.99

Timestamp:	192.168.2.2388.84.90.9954854802839471 05/27/22-13:05:56.378913
SID:	2839471
Source Port:	54854
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.134.81

Timestamp:	192.168.2.2388.221.134.8156846802839471 05/27/22-13:04:53.823235
SID:	2839471
Source Port:	56846
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.149.59.230

Timestamp:	192.168.2.2388.149.59.23052470802839471 05/27/22-13:05:01.570447
SID:	2839471
Source Port:	52470
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.78.182.1

Timestamp:	192.168.2.23112.78.182.141584802839471 05/27/22-13:06:28.770098
SID:	2839471
Source Port:	41584
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.65.43

Timestamp:	192.168.2.2395.216.65.4345668802839471 05/27/22-13:04:18.497471
SID:	2839471
Source Port:	45668
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.187.41

Timestamp:	192.168.2.2395.100.187.4139724802839471 05/27/22-13:05:51.446986
SID:	2839471
Source Port:	39724
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.43.85.130

Timestamp:	192.168.2.2388.43.85.13037716802839471 05/27/22-13:06:09.159255
SID:	2839471
Source Port:	37716
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.139.168

Timestamp:	192.168.2.2388.221.139.16840636802839471 05/27/22-13:05:01.505866
SID:	2839471
Source Port:	40636
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.211.168.38

Timestamp:	192.168.2.2395.211.168.3848482802839471 05/27/22-13:04:08.445501
SID:	2839471
Source Port:	48482
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.210.164.219

Timestamp:	192.168.2.2388.210.164.21956930802839471 05/27/22-13:05:58.694600
SID:	2839471
Source Port:	56930
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.183.14.128

Timestamp:	192.168.2.2395.183.14.12849716802839471 05/27/22-13:04:24.407215
SID:	2839471
Source Port:	49716
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.4.190.117

Timestamp:	192.168.2.23112.4.190.11748158802839471 05/27/22-13:04:27.910495
SID:	2839471
Source Port:	48158
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.103.34.62

Timestamp:	192.168.2.2395.103.34.6233328802839471 05/27/22-13:04:33.152495
SID:	2839471
Source Port:	33328
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.165.151.208

Timestamp:	192.168.2.2395.165.151.20836920802839471 05/27/22-13:05:39.404260
SID:	2839471
Source Port:	36920
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.166.143.139

Timestamp:	192.168.2.23112.166.143.13935382802839471 05/27/22-13:05:31.862266
SID:	2839471
Source Port:	35382
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.187.193

Timestamp:	192.168.2.2395.101.187.19353624802839471 05/27/22-13:05:21.554013
SID:	2839471
Source Port:	53624
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.232.101.41

Timestamp:	192.168.2.2395.232.101.4135770802839471 05/27/22-13:05:51.492756
SID:	2839471
Source Port:	35770
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.15.20

Timestamp:	192.168.2.2395.100.15.2039684802839471 05/27/22-13:04:00.816075
SID:	2839471
Source Port:	39684
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.161.210.58

Timestamp:	192.168.2.23112.161.210.5858248802839471 05/27/22-13:04:12.947117
SID:	2839471
Source Port:	58248
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.39.162

Timestamp:	192.168.2.23112.72.39.16239026802839471 05/27/22-13:04:51.443600
SID:	2839471
Source Port:	39026
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.60.122

Timestamp:	192.168.2.2395.217.60.12256784802839471 05/27/22-13:04:57.072524
SID:	2839471
Source Port:	56784
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.165.151.52

Timestamp:	192.168.2.2395.165.151.5248400802839471 05/27/22-13:05:39.349485
SID:	2839471
Source Port:	48400
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.165.100.160

Timestamp:	192.168.2.2395.165.100.16038276802839471 05/27/22-13:04:33.147747
SID:	2839471
Source Port:	38276
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.211.216.32

Timestamp:	192.168.2.23112.211.216.3246524802839471 05/27/22-13:06:00.339210
SID:	2839471
Source Port:	46524
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.53.1.228

Timestamp:	192.168.2.23112.53.1.22840004802839471 05/27/22-13:06:05.767863
SID:	2839471
Source Port:	40004
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.90.211

Timestamp:	192.168.2.2395.101.90.21141812802839471 05/27/22-13:05:16.765662
SID:	2839471
Source Port:	41812
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.17.55.30

Timestamp:	192.168.2.23112.17.55.3033310802839471 05/27/22-13:04:01.321811
SID:	2839471
Source Port:	33310
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.65.37.15

Timestamp:	192.168.2.2395.65.37.1535686802839471 05/27/22-13:03:55.225527
SID:	2839471
Source Port:	35686
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.177.214

Timestamp:	192.168.2.2395.101.177.21440228802839471 05/27/22-13:06:20.561235
SID:	2839471
Source Port:	40228
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.199.166

Timestamp:	192.168.2.2395.216.199.16637990802839471 05/27/22-13:03:58.624651
SID:	2839471
Source Port:	37990
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.65.94

Timestamp:	192.168.2.2388.221.65.9454630802839471 05/27/22-13:03:47.643922
SID:	2839471
Source Port:	54630
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.111.116

Timestamp:	192.168.2.2395.100.111.11655968802839471 05/27/22-13:05:24.104016
SID:	2839471
Source Port:	55968
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.183.138.193

Timestamp:	192.168.2.2395.183.138.19359198802839471 05/27/22-13:04:42.817722
SID:	2839471
Source Port:	59198
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.216.100.117

Timestamp:	192.168.2.2388.216.100.11734840802839471 05/27/22-13:04:42.744445
SID:	2839471
Source Port:	34840
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.110.255.4

Timestamp:	192.168.2.2395.110.255.445770802839471 05/27/22-13:04:00.817953
SID:	2839471
Source Port:	45770
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.131.24

Timestamp:	192.168.2.2395.57.131.2450926802839471 05/27/22-13:05:24.268394
SID:	2839471
Source Port:	50926
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.87.245

Timestamp:	192.168.2.2395.101.87.24555976802839471 05/27/22-13:04:08.169650
SID:	2839471
Source Port:	55976
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.166.48.172

Timestamp:	192.168.2.23112.166.48.17256982802839471 05/27/22-13:04:20.654338
SID:	2839471
Source Port:	56982
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: 197.244.76.209

Timestamp:	192.168.2.23197.244.76.20952242372152835222 05/27/22-13:06:21.614936
SID:	2835222
Source Port:	52242
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: 95.220.189.196

Timestamp:	192.168.2.2395.220.189.19652720802839471 05/27/22-13:04:22.985272
SID:	2839471
Source Port:	52720
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.247.216.209

Timestamp:	192.168.2.2388.247.216.20936598802839471 05/27/22-13:05:14.180236
SID:	2839471
Source Port:	36598
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.250.103.77

Timestamp:	192.168.2.2388.250.103.7754546802839471 05/27/22-13:06:16.633551
SID:	2839471
Source Port:	54546
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.199.88.157

Timestamp:	192.168.2.2388.199.88.15749546802839471 05/27/22-13:06:09.126372
SID:	2839471
Source Port:	49546
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.15.39.41

Timestamp:	192.168.2.23112.15.39.4148806802839471 05/27/22-13:06:05.103489
SID:	2839471
Source Port:	48806
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.24.53

Timestamp:	192.168.2.2388.198.24.5341050802839471 05/27/22-13:04:08.193131
SID:	2839471
Source Port:	41050
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.248.56.159

Timestamp:	192.168.2.2388.248.56.15960604802839471 05/27/22-13:06:12.489676
SID:	2839471
Source Port:	60604
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.140.126.156

Timestamp:	192.168.2.2395.140.126.15656566802839471 05/27/22-13:04:08.457813
SID:	2839471
Source Port:	56566
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.87.193

Timestamp:	192.168.2.2395.101.87.19347086802839471 05/27/22-13:04:15.943798
SID:	2839471
Source Port:	47086
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.251.99.133

Timestamp:	192.168.2.2395.251.99.13355052802839471 05/27/22-13:06:20.657664
SID:	2839471
Source Port:	55052
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.120.129

Timestamp:	192.168.2.2388.198.120.12939978802839471 05/27/22-13:04:08.192593
SID:	2839471
Source Port:	39978
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.85.153.50

Timestamp:	192.168.2.2395.85.153.5042044802839471 05/27/22-13:04:31.837502
SID:	2839471
Source Port:	42044
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.126.220.226

Timestamp:	192.168.2.2395.126.220.22634098802839471 05/27/22-13:05:14.382886
SID:	2839471
Source Port:	34098
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.12.252.155

Timestamp:	192.168.2.2388.12.252.15544658802839471 05/27/22-13:06:26.051259
SID:	2839471
Source Port:	44658
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.120.7.48

Timestamp:	192.168.2.23112.120.7.4853822802839471 05/27/22-13:04:47.832854
SID:	2839471
Source Port:	53822
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.106.186.200

Timestamp:	192.168.2.23112.106.186.20053920802839471 05/27/22-13:04:33.254754
SID:	2839471
Source Port:	53920
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.48.166.34

Timestamp:	192.168.2.23112.48.166.3440202802839471 05/27/22-13:04:15.928246
SID:	2839471
Source Port:	40202
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.229.188.189

Timestamp:	192.168.2.2395.229.188.18954868802839471 05/27/22-13:04:23.007965
SID:	2839471
Source Port:	54868
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.173.186.156

Timestamp:	192.168.2.2395.173.186.15652650802839471 05/27/22-13:05:06.457295
SID:	2839471
Source Port:	52650
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.141.44.97

Timestamp:	192.168.2.2395.141.44.9738202802839471 05/27/22-13:03:53.071361
SID:	2839471
Source Port:	38202
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.91.98.61

Timestamp:	192.168.2.2395.91.98.6152152802839471 05/27/22-13:04:24.387154
SID:	2839471
Source Port:	52152
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.233.162

Timestamp:	192.168.2.2388.221.233.16236386802839471 05/27/22-13:04:20.617710
SID:	2839471
Source Port:	36386
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.59.109.253

Timestamp:	192.168.2.2395.59.109.25339602802839471 05/27/22-13:04:51.586146
SID:	2839471
Source Port:	39602
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.85.153.50

Timestamp:	192.168.2.2395.85.153.5041582802839471 05/27/22-13:04:15.963835
SID:	2839471
Source Port:	41582
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.42.216

Timestamp:	192.168.2.2388.221.42.21635522802839471 05/27/22-13:04:17.306842
SID:	2839471
Source Port:	35522
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.38.31

Timestamp:	192.168.2.23112.72.38.3158548802839471 05/27/22-13:05:49.895360
SID:	2839471
Source Port:	58548
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.224.150.76

Timestamp:	192.168.2.2395.224.150.7652178802839471 05/27/22-13:04:33.530691
SID:	2839471
Source Port:	52178
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.140.154.145

Timestamp:	192.168.2.2395.140.154.14559624802839471 05/27/22-13:05:16.851663
SID:	2839471
Source Port:	59624
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.164.198.91

Timestamp:	192.168.2.2388.164.198.9141656802839471 05/27/22-13:05:46.203775
SID:	2839471
Source Port:	41656
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.211.74.174

Timestamp:	192.168.2.23112.211.74.17435084802839471 05/27/22-13:05:16.764194
SID:	2839471
Source Port:	35084
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.125.179.75

Timestamp:	192.168.2.2395.125.179.7550044802839471 05/27/22-13:04:18.468033
SID:	2839471
Source Port:	50044
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.125.129.71

Timestamp:	192.168.2.2388.125.129.7142440802839471 05/27/22-13:06:02.686031
SID:	2839471
Source Port:	42440
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.157.202.215

Timestamp:	192.168.2.2395.157.202.21553570802839471 05/27/22-13:06:20.635499
SID:	2839471
Source Port:	53570
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.0.97.92

Timestamp:	192.168.2.2395.0.97.9252438802839471 05/27/22-13:04:08.208082
SID:	2839471
Source Port:	52438
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.47.7.36

Timestamp:	192.168.2.23112.47.7.3634256802839471 05/27/22-13:04:30.506288
SID:	2839471
Source Port:	34256
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.179.133.108

Timestamp:	192.168.2.2395.179.133.10846104802839471 05/27/22-13:04:24.372073
SID:	2839471
Source Port:	46104
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.150.101.86

Timestamp:	192.168.2.2395.150.101.8651304802839471 05/27/22-13:04:35.693151
SID:	2839471
Source Port:	51304
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.86.28.6

Timestamp:	192.168.2.2395.86.28.650582802839471 05/27/22-13:05:54.012173
SID:	2839471
Source Port:	50582
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.159.13.120

Timestamp:	192.168.2.2395.159.13.12043332802839471 05/27/22-13:05:54.097878
SID:	2839471
Source Port:	43332
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.69.89.228

Timestamp:	192.168.2.23112.69.89.22854452802839471 05/27/22-13:04:30.503603
SID:	2839471
Source Port:	54452
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.206.104

Timestamp:	192.168.2.2395.100.206.10460500802839471 05/27/22-13:04:18.524512
SID:	2839471
Source Port:	60500
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.115.92

Timestamp:	192.168.2.2395.100.115.9246792802839471 05/27/22-13:04:08.191909
SID:	2839471
Source Port:	46792
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.76.178.116

Timestamp:	192.168.2.2395.76.178.11651694802839471 05/27/22-13:06:20.681799
SID:	2839471
Source Port:	51694
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.168.107.15

Timestamp:	192.168.2.23112.168.107.1555932802839471 05/27/22-13:04:30.473653
SID:	2839471
Source Port:	55932
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.201.186.40

Timestamp:	192.168.2.23112.201.186.4049254802839471 05/27/22-13:06:28.379840
SID:	2839471
Source Port:	49254
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.190.201.217

Timestamp:	192.168.2.2395.190.201.21742914802839471 05/27/22-13:04:16.014619
SID:	2839471
Source Port:	42914
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.17.55.30

Timestamp:	192.168.2.23112.17.55.3033316802839471 05/27/22-13:04:01.597485
SID:	2839471
Source Port:	33316
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.67.8.52

Timestamp:	192.168.2.2395.67.8.5240610802839471 05/27/22-13:04:45.433835
SID:	2839471
Source Port:	40610
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.37.166

Timestamp:	192.168.2.2395.100.37.16645848802839471 05/27/22-13:03:47.375814
SID:	2839471
Source Port:	45848
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.106.149

Timestamp:	192.168.2.2395.101.106.14936712802839471 05/27/22-13:05:21.550644
SID:	2839471
Source Port:	36712
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.43.61

Timestamp:	192.168.2.2388.221.43.6156010802839471 05/27/22-13:04:08.228955
SID:	2839471
Source Port:	56010
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.78.174

Timestamp:	192.168.2.2395.100.78.17457174802839471 05/27/22-13:04:05.038544
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: 95.100.37.166

Timestamp:	192.168.2.2395.100.37.16645854802839471 05/27/22-13:03:47.790830
SID:	2839471
Source Port:	45854
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.159.17

Timestamp:	192.168.2.2395.100.159.1758962802839471 05/27/22-13:03:58.597943
SID:	2839471
Source Port:	58962
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.242.143

Timestamp:	192.168.2.2395.58.242.14355586802839471 05/27/22-13:04:00.918386
SID:	2839471
Source Port:	55586
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.112.16

Timestamp:	192.168.2.2395.216.112.1644556802839471 05/27/22-13:04:35.693366
SID:	2839471
Source Port:	44556
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.53.171.10

Timestamp:	192.168.2.2388.53.171.1045406802839471 05/27/22-13:05:56.346950
SID:	2839471
Source Port:	45406
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.118.152.22

Timestamp:	192.168.2.23112.118.152.2234928802839471 05/27/22-13:06:13.764321
SID:	2839471
Source Port:	34928
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.190.102

Timestamp:	192.168.2.2388.221.190.10251664802839471 05/27/22-13:04:20.624505
SID:	2839471
Source Port:	51664
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.70.198.244

Timestamp:	192.168.2.2388.70.198.24459710802839471 05/27/22-13:04:23.891813
SID:	2839471
Source Port:	59710
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.80.195

Timestamp:	192.168.2.2395.100.80.19544332802839471 05/27/22-13:04:33.112317
SID:	2839471
Source Port:	44332
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.56.150.106

Timestamp:	192.168.2.2395.56.150.10659840802839471 05/27/22-13:04:37.109752
SID:	2839471
Source Port:	59840
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.97.118

Timestamp:	192.168.2.2388.99.97.11844144802839471 05/27/22-13:04:47.856240
SID:	2839471
Source Port:	44144
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.210.206

Timestamp:	192.168.2.2395.100.210.20643696802839471 05/27/22-13:04:59.250583
SID:	2839471
Source Port:	43696
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.74.196

Timestamp:	192.168.2.2395.58.74.19638308802839471 05/27/22-13:04:08.278874
SID:	2839471
Source Port:	38308
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.239.224.2

Timestamp:	192.168.2.2395.239.224.256866802839471 05/27/22-13:06:31.391618
SID:	2839471
Source Port:	56866
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.239.79.43

Timestamp:	192.168.2.2395.239.79.4355498802839471 05/27/22-13:05:36.374792
SID:	2839471
Source Port:	55498
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.39.29

Timestamp:	192.168.2.23112.72.39.2951822802839471 05/27/22-13:06:05.131433
SID:	2839471
Source Port:	51822
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.253.57

Timestamp:	192.168.2.2395.101.253.5736330802839471 05/27/22-13:04:18.484250
SID:	2839471
Source Port:	36330
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.203.60.231

Timestamp:	192.168.2.2388.203.60.23138502802839471 05/27/22-13:05:05.149616
SID:	2839471
Source Port:	38502
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.249.121.16

Timestamp:	192.168.2.2388.249.121.1640596802839471 05/27/22-13:06:12.476180
SID:	2839471
Source Port:	40596
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.185.189

Timestamp:	192.168.2.2395.100.185.18943458802839471 05/27/22-13:04:45.390768
SID:	2839471
Source Port:	43458
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.121.176.19

Timestamp:	192.168.2.2395.121.176.1933106802839471 05/27/22-13:05:06.602903
SID:	2839471
Source Port:	33106
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.53.164

Timestamp:	192.168.2.23112.72.53.16445676802839471 05/27/22-13:06:11.062571
SID:	2839471
Source Port:	45676
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.70.156.137

Timestamp:	192.168.2.2395.70.156.13749788802839471 05/27/22-13:05:21.575721
SID:	2839471
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.238.169

Timestamp:	192.168.2.2388.221.238.16943664802839471 05/27/22-13:04:20.645815
SID:	2839471
Source Port:	43664
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.130.157.77

Timestamp:	192.168.2.2395.130.157.7733788802839471 05/27/22-13:03:46.108586
SID:	2839471
Source Port:	33788
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.58.35

Timestamp:	192.168.2.2395.100.58.3560888802839471 05/27/22-13:03:53.067017
SID:	2839471
Source Port:	60888
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.2.132.120

Timestamp:	192.168.2.2388.2.132.12058834802839471 05/27/22-13:04:25.561928
SID:	2839471
Source Port:	58834
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.206.22.115

Timestamp:	192.168.2.23112.206.22.11538904802839471 05/27/22-13:04:27.907853
SID:	2839471
Source Port:	38904
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.65.111.136

Timestamp:	192.168.2.2395.65.111.13633458802839471 05/27/22-13:04:10.628999
SID:	2839471
Source Port:	33458
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.83.183

Timestamp:	192.168.2.2388.221.83.18340668802839471 05/27/22-13:04:40.388106
SID:	2839471
Source Port:	40668
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.48.176.115

Timestamp:	192.168.2.23112.48.176.11546760802839471 05/27/22-13:04:33.159308
SID:	2839471
Source Port:	46760
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.70.222.210

Timestamp:	192.168.2.2395.70.222.21041464802839471 05/27/22-13:04:08.192156
SID:	2839471
Source Port:	41464
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.141.110.118

Timestamp:	192.168.2.2395.141.110.11849180802839471 05/27/22-13:04:05.065436
SID:	2839471
Source Port:	49180
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.17.100

Timestamp:	192.168.2.2395.216.17.10044418802839471 05/27/22-13:05:21.561769
SID:	2839471
Source Port:	44418
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.101.132

Timestamp:	192.168.2.2388.221.101.13243424802839471 05/27/22-13:04:25.558514
SID:	2839471
Source Port:	43424
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.133.72.135

Timestamp:	192.168.2.2388.133.72.13560994802839471 05/27/22-13:05:43.394130
SID:	2839471
Source Port:	60994
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.33.99

Timestamp:	192.168.2.23112.72.33.9953148802839471 05/27/22-13:06:00.069187
SID:	2839471
Source Port:	53148
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.120.127.94

Timestamp:	192.168.2.23112.120.127.9447642802839471 05/27/22-13:04:27.849512
SID:	2839471
Source Port:	47642
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.117.6.82

Timestamp:	192.168.2.2395.117.6.8243852802839471 05/27/22-13:04:37.013306
SID:	2839471
Source Port:	43852
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.76.127.13

Timestamp:	192.168.2.2395.76.127.1347666802839471 05/27/22-13:04:18.517977
SID:	2839471
Source Port:	47666
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.26.244.98

Timestamp:	192.168.2.2388.26.244.9843668802839471 05/27/22-13:04:59.368308
SID:	2839471
Source Port:	43668
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.114.235.230

Timestamp:	192.168.2.2388.114.235.23047494802839471 05/27/22-13:04:40.400051
SID:	2839471
Source Port:	47494
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.215.157.76

Timestamp:	192.168.2.2395.215.157.7648526802839471 05/27/22-13:04:24.407396
SID:	2839471
Source Port:	48526
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.191.126

Timestamp:	192.168.2.2395.101.191.12650204802839471 05/27/22-13:03:58.582602
SID:	2839471
Source Port:	50204
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.17.36.46

Timestamp:	192.168.2.23112.17.36.4641138802839471 05/27/22-13:04:30.476428
SID:	2839471
Source Port:	41138
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.209.140.254

Timestamp:	192.168.2.2395.209.140.25453542802839471 05/27/22-13:04:35.709277
SID:	2839471
Source Port:	53542
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.163.185.9

Timestamp:	192.168.2.23112.163.185.933146802839471 05/27/22-13:04:24.349016
SID:	2839471
Source Port:	33146
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.161.184.117

Timestamp:	192.168.2.2395.161.184.11737976802839471 05/27/22-13:05:21.869058
SID:	2839471
Source Port:	37976
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.9.7.242

Timestamp:	192.168.2.2395.9.7.24244100802839471 05/27/22-13:06:16.741731
SID:	2839471
Source Port:	44100
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.110.185.50

Timestamp:	192.168.2.2395.110.185.5049274802839471 05/27/22-13:04:10.609867
SID:	2839471
Source Port:	49274
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.104.126.240

Timestamp:	192.168.2.2395.104.126.24038646802839471 05/27/22-13:04:45.494826
SID:	2839471
Source Port:	38646
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.53.238

Timestamp:	192.168.2.23112.72.53.23844226802839471 05/27/22-13:06:28.902634
SID:	2839471
Source Port:	44226
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.240.10

Timestamp:	192.168.2.2395.101.240.1035640802839471 05/27/22-13:06:26.079919
SID:	2839471
Source Port:	35640
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.9.7.126

Timestamp:	192.168.2.2395.9.7.12638206802839471 05/27/22-13:04:18.891800
SID:	2839471
Source Port:	38206
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.6.247

Timestamp:	192.168.2.2388.198.6.24736942802839471 05/27/22-13:03:47.608525
SID:	2839471
Source Port:	36942
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.164.223.177

Timestamp:	192.168.2.2395.164.223.17753586802839471 05/27/22-13:04:18.455458
SID:	2839471
Source Port:	53586
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.30.129

Timestamp:	192.168.2.2395.57.30.12959278802839471 05/27/22-13:05:21.624854
SID:	2839471
Source Port:	59278
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.90.103.64

Timestamp:	192.168.2.2395.90.103.6438860802839471 05/27/22-13:04:24.387885
SID:	2839471
Source Port:	38860
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.187.219.207

Timestamp:	192.168.2.23112.187.219.20733170802839471 05/27/22-13:04:15.916796
SID:	2839471
Source Port:	33170
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.228.77

Timestamp:	192.168.2.2388.221.228.7748986802839471 05/27/22-13:05:24.064397
SID:	2839471
Source Port:	48986
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.85.153.50

Timestamp:	192.168.2.2395.85.153.5041626802839471 05/27/22-13:04:17.269588
SID:	2839471
Source Port:	41626
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.110.131.62

Timestamp:	192.168.2.2395.110.131.6235766802839471 05/27/22-13:06:20.608382
SID:	2839471
Source Port:	35766
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.127.233

Timestamp:	192.168.2.2395.100.127.23346024802839471 05/27/22-13:05:39.345363
SID:	2839471
Source Port:	46024
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.111.216.201

Timestamp:	192.168.2.2395.111.216.20135796802839471 05/27/22-13:05:51.680328
SID:	2839471
Source Port:	35796
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.13.37

Timestamp:	192.168.2.2395.100.13.3744810802839471 05/27/22-13:04:33.128359
SID:	2839471
Source Port:	44810
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.167.198.20

Timestamp:	192.168.2.2395.167.198.2040752802839471 05/27/22-13:05:39.500438
SID:	2839471
Source Port:	40752
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.202.112.145

Timestamp:	192.168.2.2388.202.112.14543448802839471 05/27/22-13:04:57.119516
SID:	2839471
Source Port:	43448
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.160.123

Timestamp:	192.168.2.2395.101.160.12346350802839471 05/27/22-13:05:24.185440
SID:	2839471
Source Port:	46350
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.187.117.178

Timestamp:	192.168.2.23112.187.117.17858906802839471 05/27/22-13:05:43.877335
SID:	2839471
Source Port:	58906
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.129.107.6

Timestamp:	192.168.2.2395.129.107.636136802839471 05/27/22-13:04:35.691708
SID:	2839471
Source Port:	36136
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.111.47

Timestamp:	192.168.2.2395.57.111.4757226802839471 05/27/22-13:05:14.344178
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: 112.133.211.235

Timestamp:	192.168.2.23112.133.211.23553356802839471 05/27/22-13:04:36.986734
SID:	2839471
Source Port:	53356
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.132.243.63

Timestamp:	192.168.2.2388.132.243.6334818802839471 05/27/22-13:04:59.316938
SID:	2839471
Source Port:	34818
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.247.219.25

Timestamp:	192.168.2.2388.247.219.2550356802839471 05/27/22-13:06:26.066590
SID:	2839471
Source Port:	50356
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.33.235

Timestamp:	192.168.2.2388.99.33.23547888802839471 05/27/22-13:04:25.478285
SID:	2839471
Source Port:	47888
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.213.103.214

Timestamp:	192.168.2.23112.213.103.21444710802839471 05/27/22-13:04:20.597108
SID:	2839471
Source Port:	44710
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.218.239.143

Timestamp:	192.168.2.2388.218.239.14343084802839471 05/27/22-13:04:30.578027
SID:	2839471
Source Port:	43084
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.106.30

Timestamp:	192.168.2.2395.57.106.3049270802839471 05/27/22-13:03:58.644273
SID:	2839471
Source Port:	49270
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.155.10

Timestamp:	192.168.2.2388.221.155.1059756802839471 05/27/22-13:04:53.876216
SID:	2839471
Source Port:	59756
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.85.153.50

Timestamp:	192.168.2.2395.85.153.5041814802839471 05/27/22-13:04:22.959914
SID:	2839471
Source Port:	41814
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.182.144.153

Timestamp:	192.168.2.2395.182.144.15357434802839471 05/27/22-13:05:01.492383
SID:	2839471
Source Port:	57434
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.41.62

Timestamp:	192.168.2.2395.101.41.6242692802839471 05/27/22-13:05:25.683735
SID:	2839471
Source Port:	42692
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.171.7.245

Timestamp:	192.168.2.23112.171.7.24542792802839471 05/27/22-13:04:40.046300
SID:	2839471
Source Port:	42792
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.98.126.27

Timestamp:	192.168.2.2388.98.126.2759894802839471 05/27/22-13:04:40.409092
SID:	2839471
Source Port:	59894
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.244.35.60

Timestamp:	192.168.2.2395.244.35.6059610802839471 05/27/22-13:03:56.357379
SID:	2839471
Source Port:	59610
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.133.26

Timestamp:	192.168.2.2395.217.133.2639062802839471 05/27/22-13:06:26.092536
SID:	2839471
Source Port:	39062
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.77.227

Timestamp:	192.168.2.2388.221.77.22755310802839471 05/27/22-13:03:46.017622
SID:	2839471
Source Port:	55310
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.236.244.179

Timestamp:	192.168.2.2395.236.244.17949700802839471 05/27/22-13:04:45.431867
SID:	2839471
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.197.81.172

Timestamp:	192.168.2.23112.197.81.17234328802839471 05/27/22-13:04:20.650769
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: 95.77.180.151

Timestamp:	192.168.2.2395.77.180.15157626802839471 05/27/22-13:06:20.606470
SID:	2839471
Source Port:	57626
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.24.241.244

Timestamp:	192.168.2.2395.24.241.24439838802839471 05/27/22-13:04:59.314949
SID:	2839471
Source Port:	39838
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.163.41.65

Timestamp:	192.168.2.23112.163.41.6556006802839471 05/27/22-13:04:45.121235
SID:	2839471
Source Port:	56006
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.226.39

Timestamp:	192.168.2.2395.101.226.3947394802839471 05/27/22-13:04:33.122056
SID:	2839471
Source Port:	47394
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.95.139.93

Timestamp:	192.168.2.23112.95.139.9355414802839471 05/27/22-13:05:28.027023
SID:	2839471
Source Port:	55414
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.208.230.158

Timestamp:	192.168.2.2388.208.230.15860616802839471 05/27/22-13:04:20.629683
SID:	2839471
Source Port:	60616
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.111.240.249

Timestamp:	192.168.2.2395.111.240.24942288802839471 05/27/22-13:04:00.801797
SID:	2839471
Source Port:	42288
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.167.22.69

Timestamp:	192.168.2.2395.167.22.6935238802839471 05/27/22-13:04:33.517108
SID:	2839471
Source Port:	35238
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.83.249

Timestamp:	192.168.2.2388.221.83.24947230802839471 05/27/22-13:06:16.607344
SID:	2839471
Source Port:	47230
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.197.2.179

Timestamp:	192.168.2.23112.197.2.17952772802839471 05/27/22-13:04:33.093620
SID:	2839471
Source Port:	52772
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.85.153.50

Timestamp:	192.168.2.2395.85.153.5041692802839471 05/27/22-13:04:18.938202
SID:	2839471
Source Port:	41692
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.96.216

Timestamp:	192.168.2.2395.58.96.21648320802839471 05/27/22-13:03:56.405942
SID:	2839471
Source Port:	48320
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.109.82.106

Timestamp:	192.168.2.23112.109.82.10644688802839471 05/27/22-13:04:13.395359
SID:	2839471
Source Port:	44688
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.28.220.157

Timestamp:	192.168.2.2388.28.220.15735520802839471 05/27/22-13:04:05.021777
SID:	2839471
Source Port:	35520
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.14.26

Timestamp:	192.168.2.2388.221.14.2653848802839471 05/27/22-13:04:42.740244
SID:	2839471
Source Port:	53848
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.44.115

Timestamp:	192.168.2.2388.99.44.11543442802839471 05/27/22-13:04:47.856306
SID:	2839471
Source Port:	43442
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.178.165

Timestamp:	192.168.2.2395.217.178.16557240802839471 05/27/22-13:04:33.477846
SID:	2839471
Source Port:	57240
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.216.137.138

Timestamp:	192.168.2.23112.216.137.13846146802839471 05/27/22-13:05:36.375674
SID:	2839471
Source Port:	46146
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.217.72.206

Timestamp:	192.168.2.2388.217.72.20637644802839471 05/27/22-13:05:46.160365
SID:	2839471
Source Port:	37644
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.56.15

Timestamp:	192.168.2.23112.72.56.1536638802839471 05/27/22-13:04:51.447592
SID:	2839471
Source Port:	36638
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.122.71

Timestamp:	192.168.2.2395.100.122.7139298802839471 05/27/22-13:05:01.498732
SID:	2839471
Source Port:	39298
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.220.3.69

Timestamp:	192.168.2.23112.220.3.6959622802839471 05/27/22-13:04:40.361113
SID:	2839471
Source Port:	59622
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.162.22.242

Timestamp:	192.168.2.23112.162.22.24240730802839471 05/27/22-13:04:39.797776
SID:	2839471
Source Port:	40730
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.14.54.37

Timestamp:	192.168.2.2395.14.54.3732802802839471 05/27/22-13:04:35.727463
SID:	2839471
Source Port:	32802
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.123.124.212

Timestamp:	192.168.2.2395.123.124.21254822802839471 05/27/22-13:03:58.640860
SID:	2839471
Source Port:	54822
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.231.115.208

Timestamp:	192.168.2.2388.231.115.20853620802839471 05/27/22-13:06:02.705987
SID:	2839471
Source Port:	53620
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.244.61.56

Timestamp:	192.168.2.2388.244.61.5658106802839471 05/27/22-13:04:38.462881
SID:	2839471
Source Port:	58106
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.176.145.208

Timestamp:	192.168.2.23112.176.145.20848072802839471 05/27/22-13:05:26.171581
SID:	2839471
Source Port:	48072
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.30.198.60

Timestamp:	192.168.2.23112.30.198.6034494802839471 05/27/22-13:04:15.931762
SID:	2839471
Source Port:	34494
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.131.215.160

Timestamp:	192.168.2.2395.131.215.16040860802839471 05/27/22-13:05:48.370540
SID:	2839471
Source Port:	40860
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.40.119

Timestamp:	192.168.2.23112.72.40.11951192802839471 05/27/22-13:05:32.127889
SID:	2839471
Source Port:	51192
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.250.196.18

Timestamp:	192.168.2.2388.250.196.1844578802839471 05/27/22-13:05:14.410722
SID:	2839471
Source Port:	44578
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.58.103.131

Timestamp:	192.168.2.2395.58.103.13149386802839471 05/27/22-13:05:48.425818
SID:	2839471
Source Port:	49386
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.227.126

Timestamp:	192.168.2.2395.216.227.12653172802839471 05/27/22-13:04:22.951901
SID:	2839471
Source Port:	53172
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.57.93

Timestamp:	192.168.2.23112.72.57.9350388802839471 05/27/22-13:06:13.894712
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: 95.217.234.193

Timestamp:	192.168.2.2395.217.234.19336676802839471 05/27/22-13:03:53.097144
SID:	2839471
Source Port:	36676
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.69.89.228

Timestamp:	192.168.2.23112.69.89.22854400802839471 05/27/22-13:04:27.917428
SID:	2839471
Source Port:	54400
Destination Port:	80

Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.99.109.100

Timestamp:	192.168.2.2388.99.109.10044130802839471 05/27/22-13:04:17.292638
SID:	2839471
Source Port:	44130
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.215.139

Timestamp:	192.168.2.2395.101.215.13935234802839471 05/27/22-13:04:05.065712
SID:	2839471
Source Port:	35234
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

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

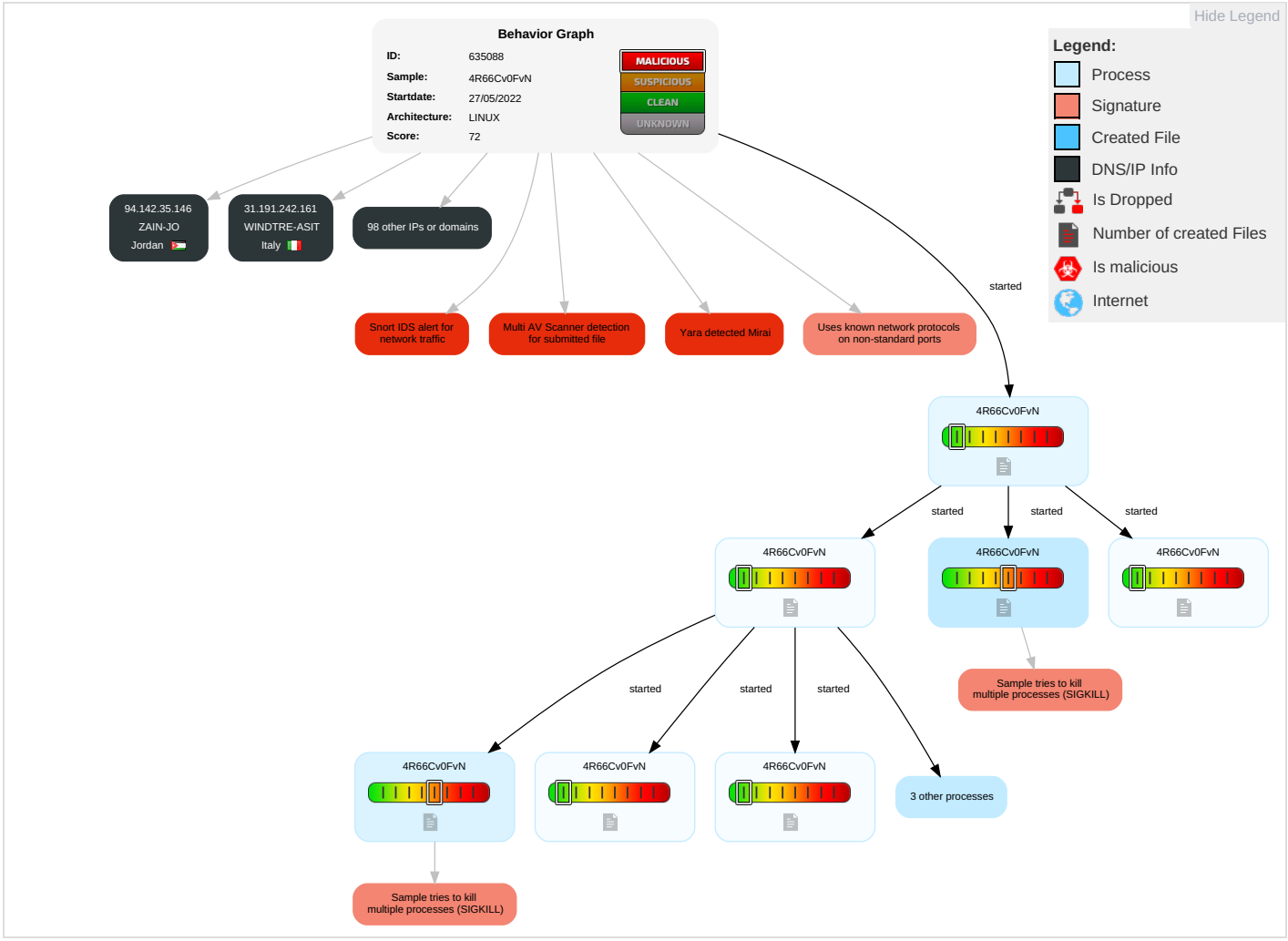
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

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	1 1 Security Software 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

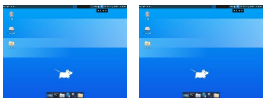
Behavior Graph

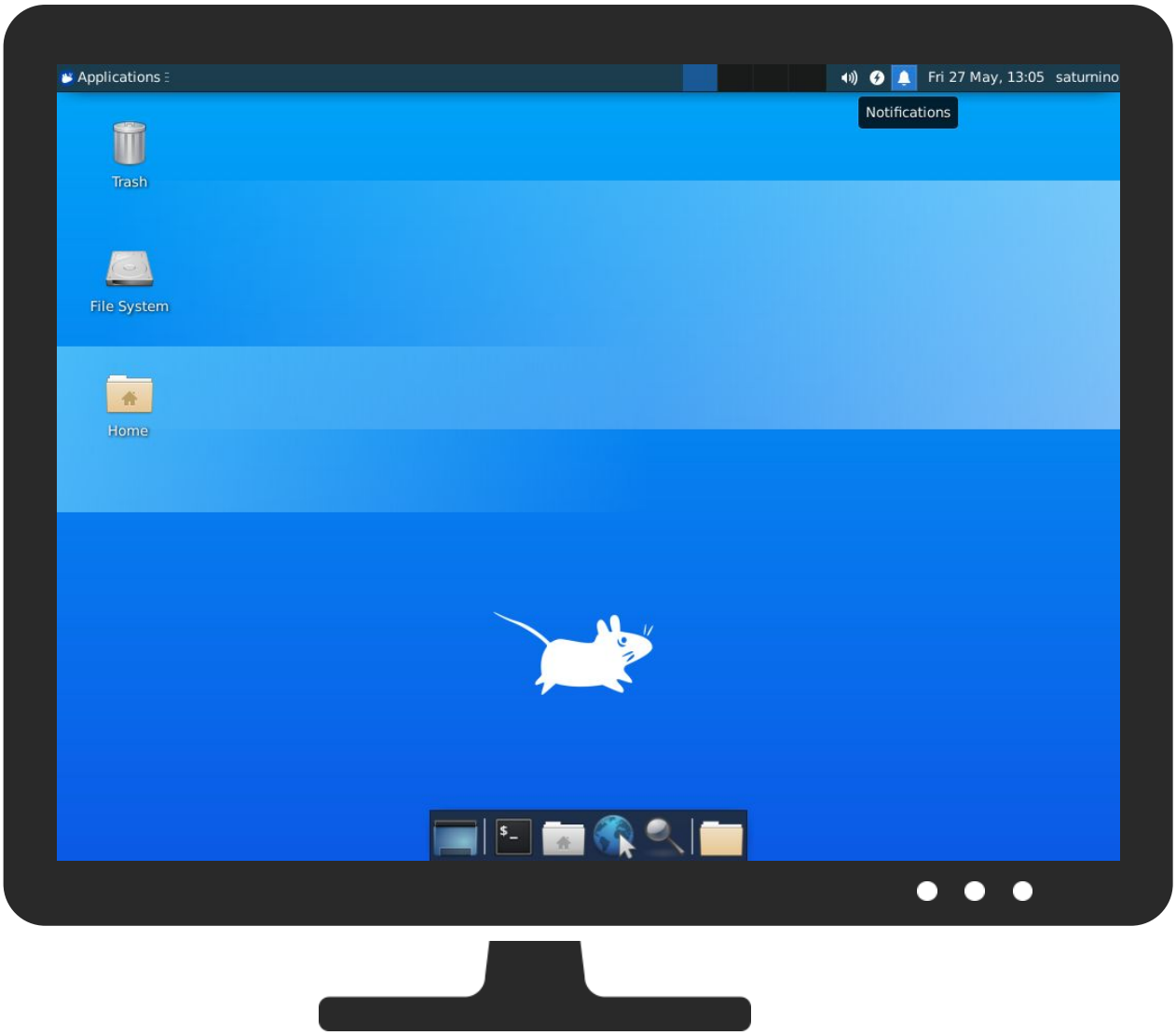


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
4R66Cv0FvN	55%	Virustotal		Browse
4R66Cv0FvN	57%	ReversingLabs	Linux.Trojan.Mirai	

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://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Virustotal		Browse
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

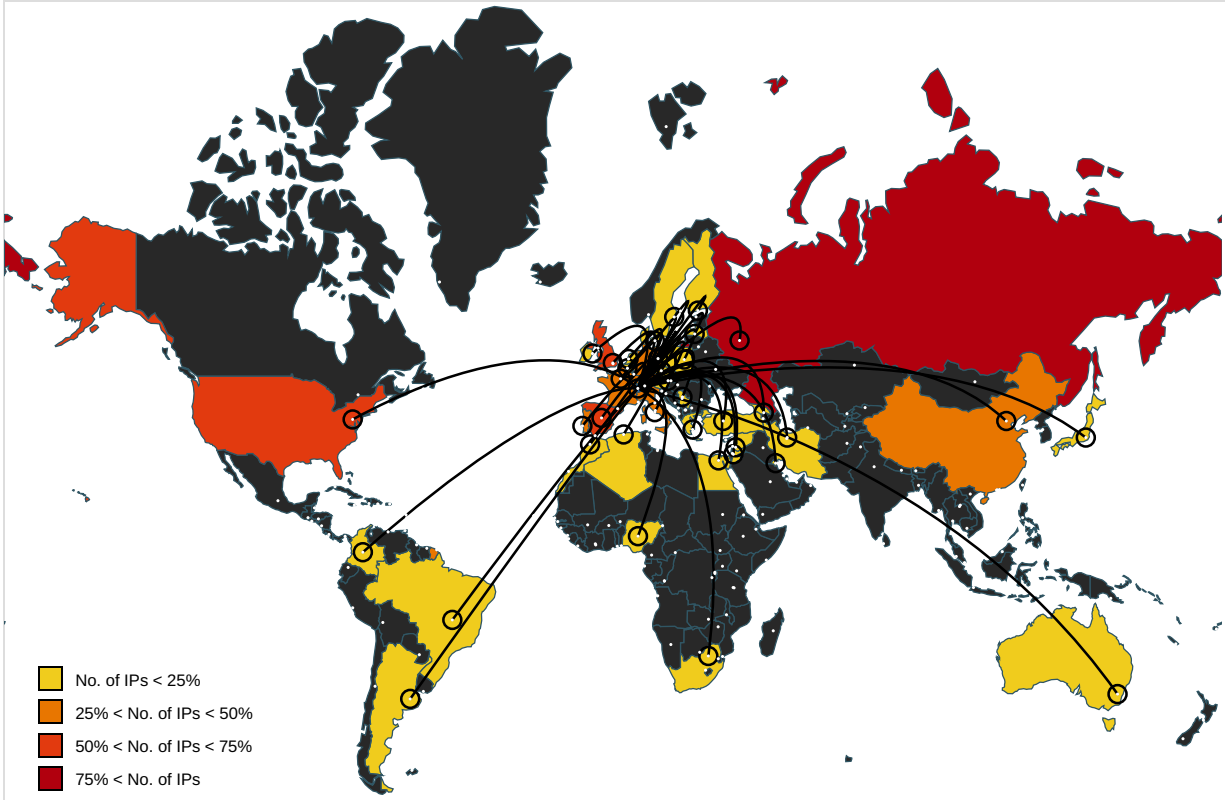
No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false	• 0%, Virustotal, Browse • 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
85.170.165.146	unknown	France		21502	ASN-NUMERICABLEFR	false
62.131.13.103	unknown	Netherlands		1136	KPNKPNNationalEU	false
48.168.241.203	unknown	United States		2686	ATGS-MMD-ASUS	false
62.153.147.137	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
85.25.248.127	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
94.194.186.8	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
62.213.233.249	unknown	Belgium		28707	STUART-ASStuartNetworksBrusselsdatacenterBelgiumBE	false
31.191.242.161	unknown	Italy		24608	WINDTRE-ASIT	false
31.38.6.157	unknown	France		5410	BOUYGTEL-ISPFR	false
197.59.229.28	unknown	Egypt		8452	TE-ASTE-ASEG	false
88.81.208.172	unknown	Russian Federation		28947	INTURAL-ASZAOInTRU	false
31.162.19.210	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
85.33.66.106	unknown	Italy		3269	ASN-IBSNAZIT	false
41.108.83.72	unknown	Algeria		36947	ALGTEL-ASDZ	false
95.160.85.251	unknown	Poland		29314	VECTRANET-ASAlZwyciestwa25381-525GdyniaPolandPL	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.85.184.211	unknown	Serbia		41897	SAT-TRAKT-ASSerbiaRS	false
196.27.215.250	unknown	Nigeria		37297	OAU-IfeNG	false
31.136.125.61	unknown	Netherlands		15480	VFNL-ASVodafoneNLAutonomousSystemNL	false
52.182.162.51	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
31.118.153.248	unknown	United Kingdom		12576	EELtdGB	false
62.242.237.57	unknown	Denmark		3292	TDCTDCASDK	false
61.89.99.228	unknown	Japan		18081	KCNKintetsuCableNetworkCoLtdJP	false
41.117.228.147	unknown	South Africa		16637	MTNNS-ASZA	false
31.181.44.200	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
94.76.139.179	unknown	Spain		29119	SERVIHOSTING-ASAireNetworksES	false
185.129.148.232	unknown	Latvia		15615	IT_SERVICESLV	false
62.141.74.244	unknown	Russian Federation		3216	SOVAM-ASRU	false
85.38.44.219	unknown	Italy		3269	ASN-IBSNAZIT	false
95.205.130.62	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
102.22.193.81	unknown	unknown		328317	Aerocom-ASZA	false
85.101.15.4	unknown	Turkey		9121	TTNETTR	false
31.34.216.38	unknown	France		5410	BOUYGTEL-ISPFR	false
62.76.192.78	unknown	Russian Federation		200135	FLEXSOFT-ASRU	false
185.11.191.240	unknown	France		203304	NETXPFR	false
85.202.224.229	unknown	Russian Federation		44622	MTK-MOSINTER-ASRU	false
62.105.89.78	unknown	United Kingdom		5413	AS5413GB	false
85.33.215.200	unknown	Italy		3269	ASN-IBSNAZIT	false
62.222.185.10	unknown	Ireland		8918	CARRIER1-ASIE	false
85.97.99.137	unknown	Turkey		9121	TTNETTR	false
31.163.215.132	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
94.142.35.146	unknown	Jordan		48832	ZAIN-JO	false
121.44.77.232	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	false
31.13.174.176	unknown	Germany		196819	TWK-KL-ASDE	false
31.58.18.181	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
85.127.123.137	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
156.15.146.173	unknown	United States		137	ASGARRConsortiumGARREU	false
31.162.185.151	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
85.245.242.187	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
31.193.7.87	unknown	United Kingdom		61323	UKFASTGB	false
94.9.108.42	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
112.23.65.230	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
95.94.164.68	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
85.57.45.36	unknown	Spain		12479	UNI2-ASES	false
95.54.216.109	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
130.70.248.45	unknown	United States		22985	UL-LAFAYETTE-1US	false
157.14.224.91	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	false
190.255.76.175	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
94.132.45.241	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
41.117.228.168	unknown	South Africa		16637	MTNNS-ASZA	false
62.215.147.67	unknown	Kuwait		21050	FAST-TELCOKW	false
95.39.201.164	unknown	Spain		12357	COMUNITELSPAINES	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
121.23.4.212	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
84.218.165.85	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
85.108.147.83	unknown	Turkey		9121	TTNETTR	false
94.132.45.249	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
181.12.226.251	unknown	Argentina		7303	TelecomArgentinaSAAR	false
179.235.141.123	unknown	Brazil		28573	CLAROSABR	false
85.40.82.3	unknown	Italy		3269	ASN-IBSNAZIT	false
62.242.237.82	unknown	Denmark		3292	TDCTDCASDK	false
31.73.32.227	unknown	United Kingdom		12576	EELtdGB	false
31.28.153.219	unknown	Czech Republic		15425	COMACZ	false
85.218.82.249	unknown	Switzerland		34781	SIL-CITYCABLE-ASCH	false
95.137.228.55	unknown	Georgia		34797	SYSTEM-NETGE	false
41.140.123.192	unknown	Morocco		36903	MT-MPLSMA	false
94.159.123.213	unknown	Russian Federation		49531	NETCOM-R-ASRU	false
31.245.105.244	unknown	Germany		3320	DTAGInternetserviceproviderationsDE	false
96.117.226.99	unknown	United States		7922	COMCAST-7922US	false
164.196.236.23	unknown	United States		2621	DNIC-AS-02621US	false
62.169.199.194	unknown	Greece		25472	WIND-ASGR	false
218.98.34.145	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
105.47.83.122	unknown	Egypt		37069	MOBINILEG	false
62.175.199.14	unknown	Spain		12357	COMUNITELSPAINES	false
85.4.56.16	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
112.130.194.173	unknown	China		7641	CHINABTNChinaBroadcastingTVNetCN	false
95.239.40.54	unknown	Italy		3269	ASN-IBSNAZIT	false
62.54.189.134	unknown	Germany		6805	TDDE-ASN1DE	false
95.212.143.87	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
197.40.144.162	unknown	Egypt		8452	TE-ASTE-ASEG	false
95.92.102.57	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
31.192.179.223	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
50.78.241.165	unknown	United States		7922	COMCAST-7922US	false
95.79.225.189	unknown	Russian Federation		42682	ERTH-NNOV-ASRU	false
88.2.210.131	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
85.155.150.191	unknown	Spain		12357	COMUNITELSPAINES	false
62.31.100.44	unknown	United Kingdom		5089	NTLGB	false
85.23.155.84	unknown	Finland		16086	DNAFI	false
85.155.51.111	unknown	Spain		6739	ONO-ASCableuropa-ONOES	false
50.20.233.28	unknown	United States		17184	ATL-CBEYONDUS	false
152.142.62.156	unknown	United States		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
41.242.158.98	unknown	unknown		328594	SUDATCHAD-ASTD	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 MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.298988373083089
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	4R66Cv0FvN
File size:	69576
MD5:	1a7dc7e371dd56f9c4d817599a534050
SHA1:	96f35b9dee1d4a27912c5589da6aa595be15c82e
SHA256:	d3063711060e7645b34e5daf91137d8e4f8bac8bd91e3087678383d3e0ff17b3
SHA512:	1ad3fcd2268007103e784e2c755de13e0b24656b5ff63c21c886c3d2cebcea18a9921a01b3ef74c49db7f433a9330e4d0809f872e3326b32bc041dbe4fefdca2
SSDEEP:	1536:+HwL/13tMFu+sQdXvQS6Nx8HZa2g8o08hbw:fL/rocCIZ74gDo
TLSH:	6F635CC5E801DE3CF95BD67E90130A08B921635456A30F2BE6AAFCD77CB305C9E56D81
File Content Preview:	.ELF.....D...4...8.....4. ...(..... .....+...+....$..... .dt.Q.....NV..a....da....8N^NuNV..J9..-.f>"y..+. QJ.g.X.#...+.N."y..+. QJ.f.A.....J.g.Hy....N.X.....-.N^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	69176
Section Header Size:	40
Number of Section Headers:	10

ELF header	
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	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0x10062	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8001010a	0x1010a	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x80010118	0x10118	0xab6	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x80012bd4	0x10bd4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80012bdc	0x10bdc	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80012be8	0x10be8	0x210	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80012df8	0x10df8	0x2d8	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x10df8	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	0x80000000	0x80000000	0x10bce	0x10bce	4.4278	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x10bd4	0x80012bd4	0x80012bd4	0x224	0x4fc	1.6584	0x6	RW	0x2000		.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
192.168.2.23112.78.149.155556872802839471 05/27/22-13:04:20.602390	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56872	80	192.168.2.23	112.78.149.155
192.168.2.2395.181.211.24543264802839471 05/27/22-13:05:39.450028	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43264	80	192.168.2.23	95.181.211.245
192.168.2.2395.239.33.5235314802839471 05/27/22-13:05:39.448496	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35314	80	192.168.2.23	95.239.33.52
192.168.2.2388.150.171.12034138802839471 05/27/22-13:04:25.483580	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34138	80	192.168.2.23	88.150.171.120
192.168.2.2388.147.150.4437374802839471 05/27/22-13:05:56.529243	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37374	80	192.168.2.23	88.147.150.44
192.168.2.2395.158.8.21139560802839471 05/27/22-13:05:14.237720	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39560	80	192.168.2.23	95.158.8.211
192.168.2.2395.158.141.22045834802839471 05/27/22-13:04:08.194012	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45834	80	192.168.2.23	95.158.141.220
192.168.2.23112.135.207.16556904802839471 05/27/22-13:06:05.012803	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56904	80	192.168.2.23	112.135.207.165
192.168.2.2395.100.116.44450488802839471 05/27/22-13:05:21.570636	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50488	80	192.168.2.23	95.100.116.44

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.198.184.21648512802839471 05/27/22-13:04:25.431447	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48512	80	192.168.2.23	88.198.184.216
192.168.2.23112.78.9.20333502802839471 05/27/22-13:04:30.438295	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33502	80	192.168.2.23	112.78.9.203
192.168.2.2395.100.123.22559388802839471 05/27/22-13:03:53.103631	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59388	80	192.168.2.23	95.100.123.225
192.168.2.23112.28.209.19459186802839471 05/27/22-13:05:31.839035	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59186	80	192.168.2.23	112.28.209.194
192.168.2.2395.101.85.9953610802839471 05/27/22-13:04:15.943706	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53610	80	192.168.2.23	95.101.85.99
192.168.2.23112.13.87.23736212802839471 05/27/22-13:04:37.094351	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36212	80	192.168.2.23	112.13.87.237
192.168.2.2388.221.44.7438338802839471 05/27/22-13:05:56.289401	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38338	80	192.168.2.23	88.221.44.74
192.168.2.2395.91.4.1657994802839471 05/27/22-13:04:33.477633	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57994	80	192.168.2.23	95.91.4.16
192.168.2.23112.30.198.6034490802839471 05/27/22-13:04:15.929622	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34490	80	192.168.2.23	112.30.198.60
192.168.2.2388.252.166.043712802839471 05/27/22-13:04:53.868578	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43712	80	192.168.2.23	88.252.166.0
192.168.2.2395.60.236.16945234802839471 05/27/22-13:04:10.614944	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45234	80	192.168.2.23	95.60.236.169
192.168.2.2388.84.90.9954854802839471 05/27/22-13:05:56.378913	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54854	80	192.168.2.23	88.84.90.99
192.168.2.2388.221.134.8156846802839471 05/27/22-13:04:53.823235	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56846	80	192.168.2.23	88.221.134.81
192.168.2.2388.149.59.23052470802839471 05/27/22-13:05:01.570447	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52470	80	192.168.2.23	88.149.59.230
192.168.2.23112.78.182.141584802839471 05/27/22-13:06:28.770098	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41584	80	192.168.2.23	112.78.182.1
192.168.2.2395.216.65.4345668802839471 05/27/22-13:04:18.497471	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45668	80	192.168.2.23	95.216.65.43
192.168.2.2395.100.187.4139724802839471 05/27/22-13:05:51.446986	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39724	80	192.168.2.23	95.100.187.41
192.168.2.2388.43.85.13037716802839471 05/27/22-13:06:09.159255	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37716	80	192.168.2.23	88.43.85.130
192.168.2.2388.221.139.16840636802839471 05/27/22-13:05:01.505866	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40636	80	192.168.2.23	88.221.139.168

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.211.168.3848482802839471 05/27/22-13:04:08.445501	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48482	80	192.168.2.23	95.211.168.38
192.168.2.2388.210.164.21956930802839471 05/27/22-13:05:58.694600	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56930	80	192.168.2.23	88.210.164.219
192.168.2.2395.183.14.12849716802839471 05/27/22-13:04:24.407215	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49716	80	192.168.2.23	95.183.14.128
192.168.2.23112.4.190.11748158802839471 05/27/22-13:04:27.910495	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48158	80	192.168.2.23	112.4.190.117
192.168.2.2395.103.34.6233328802839471 05/27/22-13:04:33.152495	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33328	80	192.168.2.23	95.103.34.62
192.168.2.2395.165.151.20836920802839471 05/27/22-13:05:39.404260	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36920	80	192.168.2.23	95.165.151.208
192.168.2.23112.166.143.13935382802839471 05/27/22-13:05:31.862266	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35382	80	192.168.2.23	112.166.143.139
192.168.2.2395.101.187.19353624802839471 05/27/22-13:05:21.554013	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53624	80	192.168.2.23	95.101.187.193
192.168.2.2395.232.101.4135770802839471 05/27/22-13:05:51.492756	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35770	80	192.168.2.23	95.232.101.41
192.168.2.2395.100.15.2039684802839471 05/27/22-13:04:00.816075	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39684	80	192.168.2.23	95.100.15.20
192.168.2.23112.161.210.5858248802839471 05/27/22-13:04:12.947117	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58248	80	192.168.2.23	112.161.210.58
192.168.2.23112.72.39.16239026802839471 05/27/22-13:04:51.443600	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39026	80	192.168.2.23	112.72.39.162
192.168.2.2395.217.60.12256784802839471 05/27/22-13:04:57.072524	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56784	80	192.168.2.23	95.217.60.122
192.168.2.2395.165.151.5248400802839471 05/27/22-13:05:39.349485	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48400	80	192.168.2.23	95.165.151.52
192.168.2.2395.165.100.16038276802839471 05/27/22-13:04:33.147747	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38276	80	192.168.2.23	95.165.100.160
192.168.2.23112.211.216.3246524802839471 05/27/22-13:06:00.339210	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46524	80	192.168.2.23	112.211.216.32
192.168.2.23112.53.1.22840004802839471 05/27/22-13:06:05.767863	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40004	80	192.168.2.23	112.53.1.228
192.168.2.2395.101.90.21141812802839471 05/27/22-13:05:16.765662	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41812	80	192.168.2.23	95.101.90.211
192.168.2.23112.17.55.3033310802839471 05/27/22-13:04:01.321811	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33310	80	192.168.2.23	112.17.55.30

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.65.37.153 5686802839471 05/27/22-13:03:55.225527	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35686	80	192.168.2.23	95.65.37.15
192.168.2.2395.101.177.2 1440228802839471 05/27/22-13:06:20.561235	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40228	80	192.168.2.23	95.101.177.214
192.168.2.2395.216.199.1 6637990802839471 05/27/22-13:03:58.624651	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37990	80	192.168.2.23	95.216.199.166
192.168.2.2388.221.65.94 54630802839471 05/27/22-13:03:47.643922	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54630	80	192.168.2.23	88.221.65.94
192.168.2.2395.100.111.1 1655968802839471 05/27/22-13:05:24.104016	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55968	80	192.168.2.23	95.100.111.116
192.168.2.2395.183.138.1 9359198802839471 05/27/22-13:04:42.817722	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59198	80	192.168.2.23	95.183.138.193
192.168.2.2388.216.100.1 1734840802839471 05/27/22-13:04:42.744445	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34840	80	192.168.2.23	88.216.100.117
192.168.2.2395.110.255.4 45770802839471 05/27/22-13:04:00.817953	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45770	80	192.168.2.23	95.110.255.4
192.168.2.2395.57.131.24 50926802839471 05/27/22-13:05:24.268394	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50926	80	192.168.2.23	95.57.131.24
192.168.2.2395.101.87.24 555976802839471 05/27/22-13:04:08.169650	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55976	80	192.168.2.23	95.101.87.245
192.168.2.23112.166.48.1 7256982802839471 05/27/22-13:04:20.654338	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56982	80	192.168.2.23	112.166.48.172
192.168.2.23197.244.76.2 0952242372152835222 05/27/22-13:06:21.614936	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52242	37215	192.168.2.23	197.244.76.209
192.168.2.2395.220.189.1 9652720802839471 05/27/22-13:04:22.985272	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52720	80	192.168.2.23	95.220.189.196
192.168.2.2388.247.216.2 0936598802839471 05/27/22-13:05:14.180236	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36598	80	192.168.2.23	88.247.216.209
192.168.2.2388.250.103.7 754546802839471 05/27/22-13:06:16.633551	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54546	80	192.168.2.23	88.250.103.77
192.168.2.2388.199.88.15 749546802839471 05/27/22-13:06:09.126372	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49546	80	192.168.2.23	88.199.88.157
192.168.2.23112.15.39.41 48806802839471 05/27/22-13:06:05.103489	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48806	80	192.168.2.23	112.15.39.41
192.168.2.2388.198.24.53 41050802839471 05/27/22-13:04:08.193131	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41050	80	192.168.2.23	88.198.24.53
192.168.2.2388.248.56.15 960604802839471 05/27/22-13:06:12.489676	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60604	80	192.168.2.23	88.248.56.159

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.140.126.15656566802839471 05/27/22-13:04:08.457813	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56566	80	192.168.2.23	95.140.126.156
192.168.2.2395.101.87.19347086802839471 05/27/22-13:04:15.943798	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47086	80	192.168.2.23	95.101.87.193
192.168.2.2395.251.99.13355052802839471 05/27/22-13:06:20.657664	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55052	80	192.168.2.23	95.251.99.133
192.168.2.2388.198.120.12939978802839471 05/27/22-13:04:08.192593	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39978	80	192.168.2.23	88.198.120.129
192.168.2.2395.85.153.5042044802839471 05/27/22-13:04:31.837502	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42044	80	192.168.2.23	95.85.153.50
192.168.2.2395.126.220.22634098802839471 05/27/22-13:05:14.382886	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34098	80	192.168.2.23	95.126.220.226
192.168.2.2388.12.252.15544658802839471 05/27/22-13:06:26.051259	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44658	80	192.168.2.23	88.12.252.155
192.168.2.23112.120.7.4853822802839471 05/27/22-13:04:47.832854	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53822	80	192.168.2.23	112.120.7.48
192.168.2.23112.106.186.20053920802839471 05/27/22-13:04:33.254754	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53920	80	192.168.2.23	112.106.186.200
192.168.2.23112.48.166.3440202802839471 05/27/22-13:04:15.928246	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40202	80	192.168.2.23	112.48.166.34
192.168.2.2395.229.188.18954868802839471 05/27/22-13:04:23.007965	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54868	80	192.168.2.23	95.229.188.189
192.168.2.2395.173.186.15652650802839471 05/27/22-13:05:06.457295	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52650	80	192.168.2.23	95.173.186.156
192.168.2.2395.141.44.9738202802839471 05/27/22-13:03:53.071361	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38202	80	192.168.2.23	95.141.44.97
192.168.2.2395.91.98.6152152802839471 05/27/22-13:04:24.387154	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52152	80	192.168.2.23	95.91.98.61
192.168.2.2388.221.233.16236386802839471 05/27/22-13:04:20.617710	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36386	80	192.168.2.23	88.221.233.162
192.168.2.2395.59.109.25339602802839471 05/27/22-13:04:51.586146	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39602	80	192.168.2.23	95.59.109.253
192.168.2.2395.85.153.5041582802839471 05/27/22-13:04:15.963835	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41582	80	192.168.2.23	95.85.153.50
192.168.2.2388.221.42.21635522802839471 05/27/22-13:04:17.306842	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35522	80	192.168.2.23	88.221.42.216
192.168.2.23112.72.38.3158548802839471 05/27/22-13:05:49.895360	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58548	80	192.168.2.23	112.72.38.31

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.224.150.76521788028394710 5/27/22-13:04:33.530691	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52178	80	192.168.2.23	95.224.150.76
192.168.2.2395.140.154.14559624802839471 05/27/22-13:05:16.851663	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59624	80	192.168.2.23	95.140.154.145
192.168.2.2388.164.198.9141656802839471 05/27/22-13:05:46.203775	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41656	80	192.168.2.23	88.164.198.91
192.168.2.23112.211.74.17435084802839471 05/27/22-13:05:16.764194	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35084	80	192.168.2.23	112.211.74.174
192.168.2.2395.125.179.75550044802839471 05/27/22-13:04:18.468033	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50044	80	192.168.2.23	95.125.179.75
192.168.2.2388.125.129.7142440802839471 05/27/22-13:06:02.686031	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42440	80	192.168.2.23	88.125.129.71
192.168.2.2395.157.202.21553570802839471 05/27/22-13:06:20.635499	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53570	80	192.168.2.23	95.157.202.215
192.168.2.2395.0.97.925243880283947 1 05/27/22-13:04:08.208082	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52438	80	192.168.2.23	95.0.97.92
192.168.2.23112.47.7.3634256802839471 05/27/22-13:04:30.506288	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34256	80	192.168.2.23	112.47.7.36
192.168.2.2395.179.133.10846104802839471 05/27/22-13:04:24.372073	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46104	80	192.168.2.23	95.179.133.108
192.168.2.2395.150.101.86513048028394710 5/27/22-13:04:35.693151	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51304	80	192.168.2.23	95.150.101.86
192.168.2.2395.86.28.650582802839471 05/27/22-13:05:54.012173	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50582	80	192.168.2.23	95.86.28.6
192.168.2.2395.159.13.120433328028394710 5/27/22-13:05:54.097878	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43332	80	192.168.2.23	95.159.13.120
192.168.2.23112.69.89.228544528028394710 5/27/22-13:04:30.503603	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54452	80	192.168.2.23	112.69.89.228
192.168.2.2395.100.206.10460500802839471 05/27/22-13:04:18.524512	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60500	80	192.168.2.23	95.100.206.104
192.168.2.2395.100.115.9246792802839471 05/27/22-13:04:08.191909	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46792	80	192.168.2.23	95.100.115.92
192.168.2.2395.76.178.11651694802839471 05/27/22-13:06:20.681799	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51694	80	192.168.2.23	95.76.178.116
192.168.2.23112.168.107.1555932802839471 05/27/22-13:04:30.473653	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55932	80	192.168.2.23	112.168.107.15
192.168.2.23112.201.186.4049254802839471 05/27/22-13:06:28.379840	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49254	80	192.168.2.23	112.201.186.40
192.168.2.2395.190.201.21742914802839471 05/27/22-13:04:16.014619	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42914	80	192.168.2.23	95.190.201.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23112.17.55.3033316802839471 05/27/22-13:04:01.597485	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33316	80	192.168.2.23	112.17.55.30
192.168.2.2395.67.8.5240610802839471 05/27/22-13:04:45.433835	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40610	80	192.168.2.23	95.67.8.52
192.168.2.2395.100.37.16645848802839471 05/27/22-13:03:47.375814	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45848	80	192.168.2.23	95.100.37.166
192.168.2.2395.101.106.14936712802839471 05/27/22-13:05:21.550644	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36712	80	192.168.2.23	95.101.106.149
192.168.2.2388.221.43.6156010802839471 05/27/22-13:04:08.228955	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56010	80	192.168.2.23	88.221.43.61
192.168.2.2395.100.78.17457174802839471 05/27/22-13:04:05.038544	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57174	80	192.168.2.23	95.100.78.174
192.168.2.2395.100.37.16645854802839471 05/27/22-13:03:47.790830	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45854	80	192.168.2.23	95.100.37.166
192.168.2.2395.100.159.175896280283947 1 05/27/22-13:03:58.597943	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58962	80	192.168.2.23	95.100.159.17
192.168.2.2395.58.242.14355586802839471 05/27/22-13:04:00.918386	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55586	80	192.168.2.23	95.58.242.143
192.168.2.2395.216.112.1644556802839471 05/27/22-13:04:35.693366	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44556	80	192.168.2.23	95.216.112.16
192.168.2.2388.53.171.1045406802839471 05/27/22-13:05:56.346950	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45406	80	192.168.2.23	88.53.171.10
192.168.2.23112.118.152.2234928802839471 05/27/22-13:06:13.764321	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34928	80	192.168.2.23	112.118.152.22
192.168.2.2388.221.190.10251664802839471 05/27/22-13:04:20.624505	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51664	80	192.168.2.23	88.221.190.102
192.168.2.2388.70.198.24459710802839471 05/27/22-13:04:23.891813	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59710	80	192.168.2.23	88.70.198.244
192.168.2.2395.100.80.19544332802839471 05/27/22-13:04:33.112317	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44332	80	192.168.2.23	95.100.80.195
192.168.2.2395.56.150.1065984080283947 1 05/27/22-13:04:37.109752	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59840	80	192.168.2.23	95.56.150.106
192.168.2.2388.99.97.11844144802839471 05/27/22-13:04:47.856240	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44144	80	192.168.2.23	88.99.97.118
192.168.2.2395.100.210.20643696802839471 05/27/22-13:04:59.250583	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43696	80	192.168.2.23	95.100.210.206
192.168.2.2395.58.74.19638308802839471 05/27/22-13:04:08.278874	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38308	80	192.168.2.23	95.58.74.196

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.239.224.256866802839471 05/27/22-13:06:31.391618	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56866	80	192.168.2.23	95.239.224.2
192.168.2.2395.239.79.4355498802839471 05/27/22-13:05:36.374792	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55498	80	192.168.2.23	95.239.79.43
192.168.2.23112.72.39.2951822802839471 05/27/22-13:06:05.131433	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51822	80	192.168.2.23	112.72.39.29
192.168.2.2395.101.253.5736330802839471 05/27/22-13:04:18.484250	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36330	80	192.168.2.23	95.101.253.57
192.168.2.2388.203.60.23138502802839471 05/27/22-13:05:05.149616	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38502	80	192.168.2.23	88.203.60.231
192.168.2.2388.249.121.1640596802839471 05/27/22-13:06:12.476180	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40596	80	192.168.2.23	88.249.121.16
192.168.2.2395.100.185.18943458802839471 05/27/22-13:04:45.390768	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43458	80	192.168.2.23	95.100.185.189
192.168.2.2395.121.176.1933106802839471 05/27/22-13:05:06.602903	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33106	80	192.168.2.23	95.121.176.19
192.168.2.23112.72.53.16445676802839471 05/27/22-13:06:11.062571	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45676	80	192.168.2.23	112.72.53.164
192.168.2.2395.70.156.13749788802839471 05/27/22-13:05:21.575721	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49788	80	192.168.2.23	95.70.156.137
192.168.2.2388.221.238.16943664802839471 05/27/22-13:04:20.645815	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43664	80	192.168.2.23	88.221.238.169
192.168.2.2395.130.157.773378802839471 05/27/22-13:03:46.108586	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33788	80	192.168.2.23	95.130.157.77
192.168.2.2395.100.58.3560888802839471 05/27/22-13:03:53.067017	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60888	80	192.168.2.23	95.100.58.35
192.168.2.2388.2.132.12058834802839471 05/27/22-13:04:25.561928	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58834	80	192.168.2.23	88.2.132.120
192.168.2.23112.206.22.11538904802839471 05/27/22-13:04:27.907853	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38904	80	192.168.2.23	112.206.22.115
192.168.2.2395.65.111.13633458802839471 05/27/22-13:04:10.628999	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33458	80	192.168.2.23	95.65.111.136
192.168.2.2388.221.83.18340668802839471 05/27/22-13:04:40.388106	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40668	80	192.168.2.23	88.221.83.183
192.168.2.23112.48.176.11546760802839471 05/27/22-13:04:33.159308	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46760	80	192.168.2.23	112.48.176.115
192.168.2.2395.70.222.21041464802839471 05/27/22-13:04:08.192156	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41464	80	192.168.2.23	95.70.222.210

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.141.110.1184918080283947105/27/22-13:04:05.065436	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49180	80	192.168.2.23	95.141.110.118
192.168.2.2395.216.17.100444188028394710 5/27/22-13:05:21.561769	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44418	80	192.168.2.23	95.216.17.100
192.168.2.2388.221.101.132434248028394710 5/27/22-13:04:25.558514	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43424	80	192.168.2.23	88.221.101.132
192.168.2.2388.133.72.135609948028394710 5/27/22-13:05:43.394130	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60994	80	192.168.2.23	88.133.72.135
192.168.2.23112.72.33.995314880283947105/27/22-13:06:00.069187	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53148	80	192.168.2.23	112.72.33.99
192.168.2.23112.120.127.94476428028394710 5/27/22-13:04:27.849512	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47642	80	192.168.2.23	112.120.127.94
192.168.2.2395.117.6.8243852802839471 05/27/22-13:04:37.013306	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43852	80	192.168.2.23	95.117.6.82
192.168.2.2395.76.127.1347666802839471 05/27/22-13:04:18.517977	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47666	80	192.168.2.23	95.76.127.13
192.168.2.2388.26.244.9843668802839471 05/27/22-13:04:59.368308	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43668	80	192.168.2.23	88.26.244.98
192.168.2.2388.114.235.23047494802839471 05/27/22-13:04:40.400051	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47494	80	192.168.2.23	88.114.235.230
192.168.2.2395.215.157.7648526802839471 05/27/22-13:04:24.407396	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48526	80	192.168.2.23	95.215.157.76
192.168.2.2395.101.191.12650204802839471 05/27/22-13:03:58.582602	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50204	80	192.168.2.23	95.101.191.126
192.168.2.23112.17.36.4641138802839471 05/27/22-13:04:30.476428	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41138	80	192.168.2.23	112.17.36.46
192.168.2.2395.209.140.25453542802839471 05/27/22-13:04:35.709277	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53542	80	192.168.2.23	95.209.140.254
192.168.2.23112.163.185.933146802839471 05/27/22-13:04:24.349016	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33146	80	192.168.2.23	112.163.185.9
192.168.2.2395.161.184.11737976802839471 05/27/22-13:05:21.869058	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37976	80	192.168.2.23	95.161.184.117
192.168.2.2395.9.7.24244100802839471 05/27/22-13:06:16.741731	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44100	80	192.168.2.23	95.9.7.242
192.168.2.2395.110.185.5049274802839471 05/27/22-13:04:10.609867	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49274	80	192.168.2.23	95.110.185.50
192.168.2.2395.104.126.24038646802839471 05/27/22-13:04:45.494826	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38646	80	192.168.2.23	95.104.126.240

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23112.72.53.23 844226802839471 05/27/22-13:06:28.902634	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44226	80	192.168.2.23	112.72.53.238
192.168.2.2395.101.240.1 035640802839471 05/27/22-13:06:26.079919	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35640	80	192.168.2.23	95.101.240.10
192.168.2.2395.9.7.12638 206802839471 05/27/22-13:04:18.891800	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38206	80	192.168.2.23	95.9.7.126
192.168.2.2388.198.6.247 36942802839471 05/27/22-13:03:47.608525	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36942	80	192.168.2.23	88.198.6.247
192.168.2.2395.164.223.1 7753586802839471 05/27/22-13:04:18.455458	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53586	80	192.168.2.23	95.164.223.177
192.168.2.2395.57.30.129 59278802839471 05/27/22-13:05:21.624854	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59278	80	192.168.2.23	95.57.30.129
192.168.2.2395.90.103.64 38860802839471 05/27/22-13:04:24.387885	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38860	80	192.168.2.23	95.90.103.64
192.168.2.23112.187.219. 20733170802839471 05/27/22-13:04:15.916796	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33170	80	192.168.2.23	112.187.219.207
192.168.2.2388.221.228.7 748986802839471 05/27/22-13:05:24.064397	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48986	80	192.168.2.23	88.221.228.77
192.168.2.2395.85.153.50 41626802839471 05/27/22-13:04:17.269588	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41626	80	192.168.2.23	95.85.153.50
192.168.2.2395.110.131.6 235766802839471 05/27/22-13:06:20.608382	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35766	80	192.168.2.23	95.110.131.62
192.168.2.2395.100.127.2 3346024802839471 05/27/22-13:05:39.345363	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46024	80	192.168.2.23	95.100.127.233
192.168.2.2395.111.216.2 0135796802839471 05/27/22-13:05:51.680328	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35796	80	192.168.2.23	95.111.216.201
192.168.2.2395.100.13.37 44810802839471 05/27/22-13:04:33.128359	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44810	80	192.168.2.23	95.100.13.37
192.168.2.2395.167.198.2 040752802839471 05/27/22-13:05:39.500438	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40752	80	192.168.2.23	95.167.198.20
192.168.2.2388.202.112.1 4543448802839471 05/27/22-13:04:57.119516	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43448	80	192.168.2.23	88.202.112.145
192.168.2.2395.101.160.1 2346350802839471 05/27/22-13:05:24.185440	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46350	80	192.168.2.23	95.101.160.123
192.168.2.23112.187.117. 17858906802839471 05/27/22-13:05:43.877335	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58906	80	192.168.2.23	112.187.117.178
192.168.2.2395.129.107.6 36136802839471 05/27/22-13:04:35.691708	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36136	80	192.168.2.23	95.129.107.6

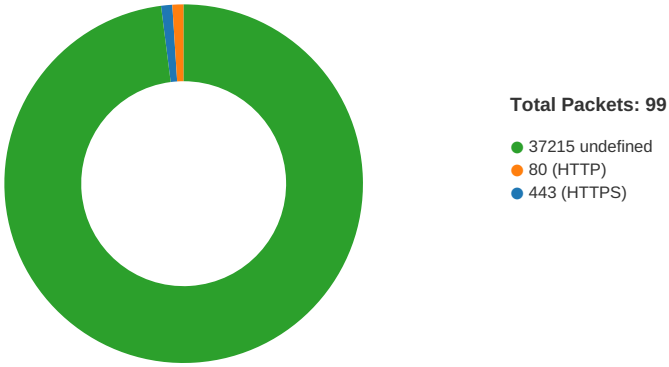
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.57.111.47 57226802839471 05/27/22-13:05:14.344178	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57226	80	192.168.2.23	95.57.111.47
192.168.2.23112.133.211. 23553356802839471 05/27/22-13:04:36.986734	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53356	80	192.168.2.23	112.133.211.235
192.168.2.2388.132.243.6 334818802839471 05/27/22-13:04:59.316938	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34818	80	192.168.2.23	88.132.243.63
192.168.2.2388.247.219.2 550356802839471 05/27/22-13:06:26.066590	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50356	80	192.168.2.23	88.247.219.25
192.168.2.2388.99.33.235 47888802839471 05/27/22-13:04:25.478285	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47888	80	192.168.2.23	88.99.33.235
192.168.2.23112.213.103. 21444710802839471 05/27/22-13:04:20.597108	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44710	80	192.168.2.23	112.213.103.214
192.168.2.2388.218.239.1 4343084802839471 05/27/22-13:04:30.578027	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43084	80	192.168.2.23	88.218.239.143
192.168.2.2395.57.106.30 49270802839471 05/27/22-13:03:58.644273	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49270	80	192.168.2.23	95.57.106.30
192.168.2.2388.221.155.1 059756802839471 05/27/22-13:04:53.876216	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59756	80	192.168.2.23	88.221.155.10
192.168.2.2395.85.153.50 41814802839471 05/27/22-13:04:22.959914	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41814	80	192.168.2.23	95.85.153.50
192.168.2.2395.182.144.1 5357434802839471 05/27/22-13:05:01.492383	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57434	80	192.168.2.23	95.182.144.153
192.168.2.2395.101.41.62 42692802839471 05/27/22-13:05:25.683735	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42692	80	192.168.2.23	95.101.41.62
192.168.2.23112.171.7.24 542792802839471 05/27/22-13:04:40.046300	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42792	80	192.168.2.23	112.171.7.245
192.168.2.2388.98.126.27 59894802839471 05/27/22-13:04:40.409092	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59894	80	192.168.2.23	88.98.126.27
192.168.2.2395.244.35.60 59610802839471 05/27/22-13:03:56.357379	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59610	80	192.168.2.23	95.244.35.60
192.168.2.2395.217.133.2 639062802839471 05/27/22-13:06:26.092536	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39062	80	192.168.2.23	95.217.133.26
192.168.2.2388.221.77.22 755310802839471 05/27/22-13:03:46.017622	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55310	80	192.168.2.23	88.221.77.227
192.168.2.2395.236.244.1 7949700802839471 05/27/22-13:04:45.431867	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49700	80	192.168.2.23	95.236.244.179
192.168.2.23112.197.81.1 7234328802839471 05/27/22-13:04:20.650769	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34328	80	192.168.2.23	112.197.81.172

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.77.180.15 157626802839471 05/27/22-13:06:20.606470	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57626	80	192.168.2.23	95.77.180.151
192.168.2.2395.24.241.24 439838802839471 05/27/22-13:04:59.314949	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39838	80	192.168.2.23	95.24.241.244
192.168.2.23112.163.41.6 556006802839471 05/27/22-13:04:45.121235	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56006	80	192.168.2.23	112.163.41.65
192.168.2.2395.101.226.3 947394802839471 05/27/22-13:04:33.122056	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47394	80	192.168.2.23	95.101.226.39
192.168.2.23112.95.139.9 355414802839471 05/27/22-13:05:28.027023	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55414	80	192.168.2.23	112.95.139.93
192.168.2.2388.208.230.1 5860616802839471 05/27/22-13:04:20.629683	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60616	80	192.168.2.23	88.208.230.158
192.168.2.2395.111.240.2 4942288802839471 05/27/22-13:04:00.801797	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42288	80	192.168.2.23	95.111.240.249
192.168.2.2395.167.22.69 35238802839471 05/27/22-13:04:33.517108	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35238	80	192.168.2.23	95.167.22.69
192.168.2.2388.221.83.24 947230802839471 05/27/22-13:06:16.607344	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47230	80	192.168.2.23	88.221.83.249
192.168.2.23112.197.2.17 952772802839471 05/27/22-13:04:33.093620	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52772	80	192.168.2.23	112.197.2.179
192.168.2.2395.85.153.50 41692802839471 05/27/22-13:04:18.938202	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41692	80	192.168.2.23	95.85.153.50
192.168.2.2395.58.96.216 48320802839471 05/27/22-13:03:56.405942	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48320	80	192.168.2.23	95.58.96.216
192.168.2.23112.109.82.1 0644688802839471 05/27/22-13:04:13.395359	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44688	80	192.168.2.23	112.109.82.106
192.168.2.2388.28.220.15 735520802839471 05/27/22-13:04:05.021777	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35520	80	192.168.2.23	88.28.220.157
192.168.2.2388.221.14.26 53848802839471 05/27/22-13:04:42.740244	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53848	80	192.168.2.23	88.221.14.26
192.168.2.2388.99.44.115 43442802839471 05/27/22-13:04:47.856306	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43442	80	192.168.2.23	88.99.44.115
192.168.2.2395.217.178.1 6557240802839471 05/27/22-13:04:33.477846	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	57240	80	192.168.2.23	95.217.178.165
192.168.2.23112.216.137. 13846146802839471 05/27/22-13:05:36.375674	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46146	80	192.168.2.23	112.216.137.138
192.168.2.2388.217.72.20 637644802839471 05/27/22-13:05:46.160365	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37644	80	192.168.2.23	88.217.72.206

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23112.72.56.15 36638802839471 05/27/22-13:04:51.447592	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36638	80	192.168.2.23	112.72.56.15
192.168.2.2395.100.122.7 139298802839471 05/27/22-13:05:01.498732	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39298	80	192.168.2.23	95.100.122.71
192.168.2.23112.220.3.69 59622802839471 05/27/22-13:04:40.361113	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59622	80	192.168.2.23	112.220.3.69
192.168.2.23112.162.22.2 4240730802839471 05/27/22-13:04:39.797776	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40730	80	192.168.2.23	112.162.22.242
192.168.2.2395.14.54.373 2802802839471 05/27/22-13:04:35.727463	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	32802	80	192.168.2.23	95.14.54.37
192.168.2.2395.123.124.2 1254822802839471 05/27/22-13:03:58.640860	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54822	80	192.168.2.23	95.123.124.212
192.168.2.2388.231.115.2 0853620802839471 05/27/22-13:06:02.705987	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53620	80	192.168.2.23	88.231.115.208
192.168.2.2388.244.61.56 58106802839471 05/27/22-13:04:38.462881	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58106	80	192.168.2.23	88.244.61.56
192.168.2.23112.176.145. 20848072802839471 05/27/22-13:05:26.171581	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48072	80	192.168.2.23	112.176.145.208
192.168.2.23112.30.198.6 034494802839471 05/27/22-13:04:15.931762	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34494	80	192.168.2.23	112.30.198.60
192.168.2.2395.131.215.1 6040860802839471 05/27/22-13:05:48.370540	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40860	80	192.168.2.23	95.131.215.160
192.168.2.23112.72.40.11 951192802839471 05/27/22-13:05:32.127889	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51192	80	192.168.2.23	112.72.40.119
192.168.2.2388.250.196.1 844578802839471 05/27/22-13:05:14.410722	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44578	80	192.168.2.23	88.250.196.18
192.168.2.2395.58.103.13 149386802839471 05/27/22-13:05:48.425818	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49386	80	192.168.2.23	95.58.103.131
192.168.2.2395.216.227.1 2653172802839471 05/27/22-13:04:22.951901	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53172	80	192.168.2.23	95.216.227.126
192.168.2.23112.72.57.93 50388802839471 05/27/22-13:06:13.894712	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50388	80	192.168.2.23	112.72.57.93
192.168.2.2395.217.234.1 9336676802839471 05/27/22-13:03:53.097144	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36676	80	192.168.2.23	95.217.234.193
192.168.2.23112.69.89.22 854400802839471 05/27/22-13:04:27.917428	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54400	80	192.168.2.23	112.69.89.228
192.168.2.2388.99.109.10 044130802839471 05/27/22-13:04:17.292638	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44130	80	192.168.2.23	88.99.109.100

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.101.215.13935234802839471 05/27/22-13:04:05.065712	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35234	80	192.168.2.23	95.101.215.139

Network Port Distribution



TCP Packets

HTTP Request Dependency Graph

- 192.168.0.14:80

System Behavior

Analysis Process: 4R66Cv0FvN PID: 6226, Parent PID: 6121

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	/tmp/4R66Cv0FvN
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: 4R66Cv0FvN PID: 6228, Parent PID: 6226

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

Copyright Joe Security LLC 2022

File Read

Directory Enumerated

Analysis Process: 4R66Cv0FvN PID: **6229**, Parent PID: **6226**

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 4R66Cv0FvN PID: **6230**, Parent PID: **6226**

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 4R66Cv0FvN PID: **6234**, Parent PID: **6230**

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 4R66Cv0FvN PID: **6235**, Parent PID: **6230**

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 4R66Cv0FvN PID: **6238**, Parent PID: **6230**

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 4R66Cv0FvN PID: **6239**, Parent PID: **6230**

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a

Copyright Joe Security LLC 2022

File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: 4R66Cv0FvN PID: **6242**, Parent PID: **6230**

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 4R66Cv0FvN PID: **6244**, Parent PID: **6230**

General

Start time:	13:03:42
Start date:	27/05/2022
Path:	/tmp/4R66Cv0FvN
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Copyright Joe Security LLC 2022