ID: 635082
Sample Name: kuCwPmEwdM
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 12:46:06
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

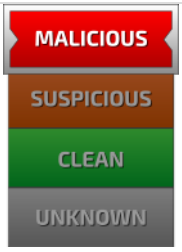
kuCwPmEwdM

Overview

General Information

Sample Name:	kuCwPmEwdM
Analysis ID:	635082
MD5:	5503ada6da9fa4..
SHA1:	2aee070f638cbf5..
SHA256:	a909a24a46ef62..
Tags:	32 elf mips mirai
Infos:	

Detection



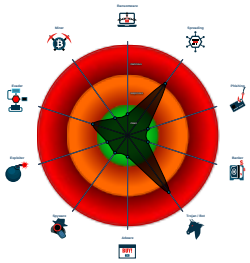
Mirai

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…
- 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…
- Detected non-DNS traffic on DNS po…
- Sample has stripped symbol table

Classification



Analysis Advice

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

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

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635082
Start date and time: 27/05/202212:46:06	2022-05-27 12:46:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kuCwPmEwdM
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/kuCwPmEwdM
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected By Cult

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- kuCwPmEwdM (PID: 6230, Parent: 6126, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/kuCwPmEwdM
  - kuCwPmEwdM New Fork (PID: 6233, Parent: 6230)
  - kuCwPmEwdM New Fork (PID: 6234, Parent: 6230)
  - kuCwPmEwdM New Fork (PID: 6236, Parent: 6230)
    - kuCwPmEwdM New Fork (PID: 6239, Parent: 6236)
    - kuCwPmEwdM New Fork (PID: 6240, Parent: 6236)
    - kuCwPmEwdM New Fork (PID: 6241, Parent: 6236)
    - kuCwPmEwdM New Fork (PID: 6242, Parent: 6236)
    - kuCwPmEwdM New Fork (PID: 6248, Parent: 6236)
    - kuCwPmEwdM New Fork (PID: 6249, Parent: 6236)
    - kuCwPmEwdM New Fork (PID: 6291, Parent: 6236)
      - kuCwPmEwdM New Fork (PID: 6293, Parent: 6291)
- **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: 88.147.25.230

Timestamp:	192.168.2.2388.147.25.23054608802839471 05/27/22-12:47:34.014385
SID:	2839471
Source Port:	54608
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.215.185.234

Timestamp:	192.168.2.2395.215.185.23438844802839471 05/27/22-12:47:51.607040
SID:	2839471
Source Port:	38844
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.67.237.66

Timestamp:	192.168.2.2395.67.237.6659082802839471 05/27/22-12:47:15.080363
SID:	2839471
Source Port:	59082
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.112.154.174

Timestamp:	192.168.2.2388.112.154.17441676802839471 05/27/22-12:47:15.090627
SID:	2839471
Source Port:	41676
Destination Port:	80
Protocol:	TCP

Classtype:	Web Application Attack

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.62.245.111

Timestamp:	192.168.2.2341.62.245.11149730372152835222 05/27/22-12:47:53.882683
SID:	2835222
Source Port:	49730
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: 95.179.137.174

Timestamp:	192.168.2.2395.179.137.17458194802839471 05/27/22-12:48:14.438208
SID:	2839471
Source Port:	58194
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.150.144.13

Timestamp:	192.168.2.2388.150.144.1353878802839471 05/27/22-12:47:10.978190
SID:	2839471
Source Port:	53878
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.130.6.151

Timestamp:	192.168.2.2395.130.6.15141382802839471 05/27/22-12:47:15.059849
SID:	2839471
Source Port:	41382
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.78.12

Timestamp:	192.168.2.2388.221.78.1259134802839471 05/27/22-12:47:49.018701
SID:	2839471
Source Port:	59134
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.214.234.136

Timestamp:	192.168.2.2395.214.234.13634152802839471 05/27/22-12:48:04.635268
SID:	2839471
Source Port:	34152
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.112.26.176

Timestamp:	192.168.2.2395.112.26.17644764802839471 05/27/22-12:47:49.003840
SID:	2839471
Source Port:	44764
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.241.100

Timestamp:	192.168.2.2395.100.241.10034392802839471 05/27/22-12:48:03.504850

SID:	2839471
Source Port:	34392
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.150.190

Timestamp:	192.168.2.2395.216.150.19036108802839471 05/27/22-12:47:15.053671
SID:	2839471
Source Port:	36108
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.159.21.173

Timestamp:	192.168.2.2395.159.21.17353860802839471 05/27/22-12:47:59.854206
SID:	2839471
Source Port:	53860
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.56.53.135

Timestamp:	192.168.2.2395.56.53.13533488802839471 05/27/22-12:47:49.073357
SID:	2839471
Source Port:	33488
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.255.41.28

Timestamp:	192.168.2.2388.255.41.2859640802839471 05/27/22-12:47:13.505289
SID:	2839471
Source Port:	59640
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.223.18.124

Timestamp:	192.168.2.23112.223.18.12440804802839471 05/27/22-12:47:13.498434
SID:	2839471
Source Port:	40804
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.247.238.126

Timestamp:	192.168.2.2388.247.238.12639848802839471 05/27/22-12:46:57.495420
SID:	2839471
Source Port:	39848
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.146.194.158

Timestamp:	192.168.2.2395.146.194.15851092802839471 05/27/22-12:47:33.709741
SID:	2839471
Source Port:	51092
Destination Port:	80
Protocol:	TCP

Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.230.20

Timestamp:	192.168.2.2395.100.230.2060114802839471 05/27/22-12:47:31.209429
SID:	2839471
Source Port:	60114
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.167.73.77

Timestamp:	192.168.2.2395.167.73.7760578802839471 05/27/22-12:47:07.038688
SID:	2839471
Source Port:	60578
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.122.162.81

Timestamp:	192.168.2.2395.122.162.8149276802839471 05/27/22-12:48:07.946255
SID:	2839471
Source Port:	49276
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.170.104

Timestamp:	192.168.2.2395.100.170.10448188802839471 05/27/22-12:47:07.172463
SID:	2839471
Source Port:	48188
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.208.231

Timestamp:	192.168.2.2395.100.208.23146568802839471 05/27/22-12:48:16.775027
SID:	2839471
Source Port:	46568
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.215.255.91

Timestamp:	192.168.2.2395.215.255.9151586802839471 05/27/22-12:47:42.722816
SID:	2839471
Source Port:	51586
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.110.234

Timestamp:	192.168.2.2388.198.110.23440074802839471 05/27/22-12:47:46.661375
SID:	2839471
Source Port:	40074
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.136.102.128

Timestamp:	192.168.2.2388.136.102.12851928802839471 05/27/22-12:47:38.633741

SID:	2839471
Source Port:	51928
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.136.54.28

Timestamp:	192.168.2.2388.136.54.2860044802839471 05/27/22-12:47:27.579938
SID:	2839471
Source Port:	60044
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.156.55.29

Timestamp:	192.168.2.2395.156.55.2955906802839471 05/27/22-12:47:36.188256
SID:	2839471
Source Port:	55906
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.188.43

Timestamp:	192.168.2.2388.221.188.4335412802839471 05/27/22-12:47:29.045100
SID:	2839471
Source Port:	35412
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.255.253.42

Timestamp:	192.168.2.2388.255.253.4234062802839471 05/27/22-12:48:16.968700
SID:	2839471
Source Port:	34062
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.214.45.1

Timestamp:	192.168.2.2388.214.45.152148802839471 05/27/22-12:47:24.075213
SID:	2839471
Source Port:	52148
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.211.165

Timestamp:	192.168.2.2395.101.211.16546204802839471 05/27/22-12:47:10.944613
SID:	2839471
Source Port:	46204
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.17.57.168

Timestamp:	192.168.2.23112.17.57.16850558802839471 05/27/22-12:47:20.105563
SID:	2839471
Source Port:	50558
Destination Port:	80
Protocol:	TCP

Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.182.207

Timestamp:	192.168.2.2395.216.182.20750770802839471 05/27/22-12:47:58.808550
SID:	2839471
Source Port:	50770
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.70.47

Timestamp:	192.168.2.2395.101.70.4758192802839471 05/27/22-12:47:15.046152
SID:	2839471
Source Port:	58192
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.168.220.97

Timestamp:	192.168.2.2395.168.220.9735532802839471 05/27/22-12:46:57.377011
SID:	2839471
Source Port:	35532
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.72.51.78

Timestamp:	192.168.2.23112.72.51.7837596802839471 05/27/22-12:48:11.670529
SID:	2839471
Source Port:	37596
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.242.231

Timestamp:	192.168.2.2395.101.242.23146042802839471 05/27/22-12:47:31.204962
SID:	2839471
Source Port:	46042
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.214.188.140

Timestamp:	192.168.2.2388.214.188.14054808802839471 05/27/22-12:47:49.127460
SID:	2839471
Source Port:	54808
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.23.239

Timestamp:	192.168.2.2395.101.23.23945600802839471 05/27/22-12:47:51.604867
SID:	2839471
Source Port:	45600
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.216.72.71

Timestamp:	192.168.2.2395.216.72.7139974802839471 05/27/22-12:48:12.019932

SID:	2839471
Source Port:	39974
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.159.11.30

Timestamp:	192.168.2.2395.159.11.3059024802839471 05/27/22-12:48:16.848947
SID:	2839471
Source Port:	59024
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.83.16

Timestamp:	192.168.2.2395.100.83.1649496802839471 05/27/22-12:47:28.999232
SID:	2839471
Source Port:	49496
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.65.56.138

Timestamp:	192.168.2.2395.65.56.13836468802839471 05/27/22-12:48:10.168925
SID:	2839471
Source Port:	36468
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.198.148.238

Timestamp:	192.168.2.2388.198.148.23836254802839471 05/27/22-12:47:38.619624
SID:	2839471
Source Port:	36254
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.128.147.220

Timestamp:	192.168.2.2395.128.147.22039230802839471 05/27/22-12:48:19.208516
SID:	2839471
Source Port:	39230
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.205.95.43

Timestamp:	192.168.2.23112.205.95.4333448802839471 05/27/22-12:48:11.887654
SID:	2839471
Source Port:	33448
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.87.64.255

Timestamp:	192.168.2.2395.87.64.25548256802839471 05/27/22-12:48:14.568167
SID:	2839471
Source Port:	48256
Destination Port:	80
Protocol:	TCP

Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.171.3.218

Timestamp:	192.168.2.23112.171.3.21846612802839471 05/27/22-12:47:13.447133
SID:	2839471
Source Port:	46612
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.210.22.221

Timestamp:	192.168.2.2388.210.22.22158942802839471 05/27/22-12:47:06.690087
SID:	2839471
Source Port:	58942
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.156.147

Timestamp:	192.168.2.2395.101.156.14756178802839471 05/27/22-12:47:36.242927
SID:	2839471
Source Port:	56178
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.249.107.254

Timestamp:	192.168.2.2388.249.107.25445124802839471 05/27/22-12:47:29.101579
SID:	2839471
Source Port:	45124
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.194.65.252

Timestamp:	192.168.2.23112.194.65.25249746802839471 05/27/22-12:47:23.716570
SID:	2839471
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.49.221.109

Timestamp:	192.168.2.2395.49.221.10932828802839471 05/27/22-12:47:42.672755
SID:	2839471
Source Port:	32828
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.171.3.218

Timestamp:	192.168.2.23112.171.3.21846688802839471 05/27/22-12:47:16.542926
SID:	2839471
Source Port:	46688
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.129.137.245

Timestamp:	192.168.2.2395.129.137.24538576802839471 05/27/22-12:47:36.183582

SID:	2839471
Source Port:	38576
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.28.199.253

Timestamp:	192.168.2.2388.28.199.25340702802839471 05/27/22-12:47:11.081110
SID:	2839471
Source Port:	40702
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.17.60.40

Timestamp:	192.168.2.23112.17.60.4039644802839471 05/27/22-12:47:53.228125
SID:	2839471
Source Port:	39644
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.231.53.220

Timestamp:	192.168.2.2395.231.53.22052380802839471 05/27/22-12:48:04.736705
SID:	2839471
Source Port:	52380
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.234.61.113

Timestamp:	192.168.2.23197.234.61.11341942372152835222 05/27/22-12:48:13.090975
SID:	2835222
Source Port:	41942
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: 95.68.75.97

Timestamp:	192.168.2.2395.68.75.9742456802839471 05/27/22-12:46:55.294531
SID:	2839471
Source Port:	42456
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: 197.214.98.132

Timestamp:	192.168.2.23197.214.98.13255698372152835222 05/27/22-12:47:20.408675
SID:	2835222
Source Port:	55698
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: 95.121.139.125

Timestamp:	192.168.2.2395.121.139.12559944802839471 05/27/22-12:47:20.135801
SID:	2839471
Source Port:	59944
Destination Port:	80
Protocol:	TCP

Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.156.51.102

Timestamp:	192.168.2.2395.156.51.10259576802839471 05/27/22-12:48:12.074131
SID:	2839471
Source Port:	59576
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.217.109.19

Timestamp:	192.168.2.2395.217.109.1953226802839471 05/27/22-12:46:57.392990
SID:	2839471
Source Port:	53226
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.68.127.121

Timestamp:	192.168.2.2395.68.127.12146654802839471 05/27/22-12:48:14.464045
SID:	2839471
Source Port:	46654
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.241.100

Timestamp:	192.168.2.2395.100.241.10034382802839471 05/27/22-12:48:02.219711
SID:	2839471
Source Port:	34382
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.120.6.61

Timestamp:	192.168.2.23112.120.6.6139842802839471 05/27/22-12:48:11.903918
SID:	2839471
Source Port:	39842
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.210.144.124

Timestamp:	192.168.2.2388.210.144.12460104802839471 05/27/22-12:47:27.576693
SID:	2839471
Source Port:	60104
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.98.202

Timestamp:	192.168.2.2395.57.98.20234828802839471 05/27/22-12:47:36.352619
SID:	2839471
Source Port:	34828
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.211.75.25

Timestamp:	192.168.2.2395.211.75.2541774802839471 05/27/22-12:48:19.124724

SID:	2839471
Source Port:	41774
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.203.252

Timestamp:	192.168.2.2395.57.203.25247000802839471 05/27/22-12:48:19.323847
SID:	2839471
Source Port:	47000
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.171.248.108

Timestamp:	192.168.2.23112.171.248.10837160802839471 05/27/22-12:47:27.589765
SID:	2839471
Source Port:	37160
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.149.185.118

Timestamp:	192.168.2.2388.149.185.11848152802839471 05/27/22-12:47:29.046007
SID:	2839471
Source Port:	48152
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.57.207.245

Timestamp:	192.168.2.2395.57.207.24558776802839471 05/27/22-12:47:31.306412
SID:	2839471
Source Port:	58776
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.222.56

Timestamp:	192.168.2.2395.101.222.5660330802839471 05/27/22-12:47:49.004541
SID:	2839471
Source Port:	60330
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.100.83.31

Timestamp:	192.168.2.2395.100.83.3160434802839471 05/27/22-12:47:51.581498
SID:	2839471
Source Port:	60434
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

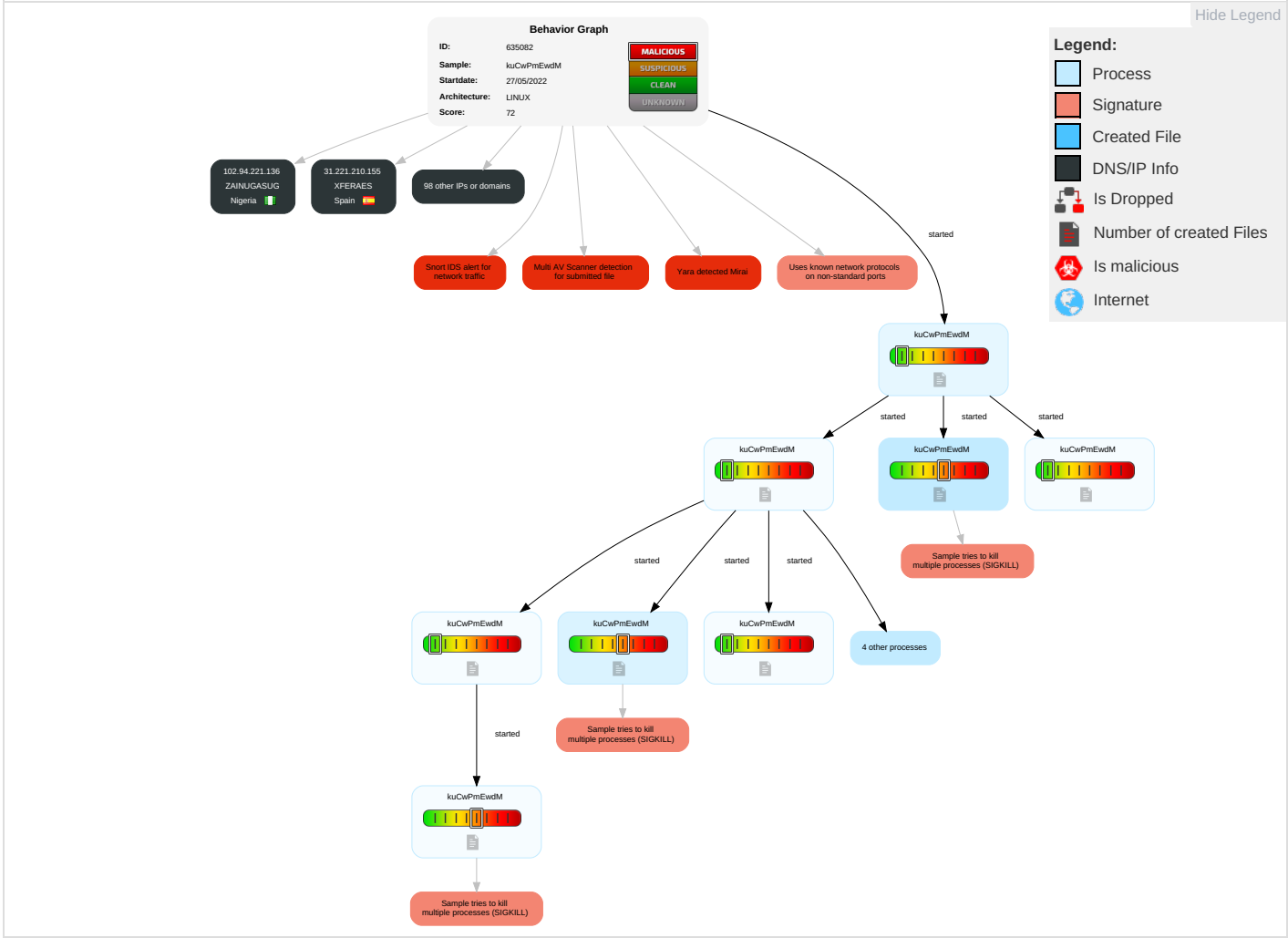
Mitre Att&ck Matrix

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
kuCwPmEwdM	53%	Virustotal		Browse

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	

Domains and IPs

Contacted Domains

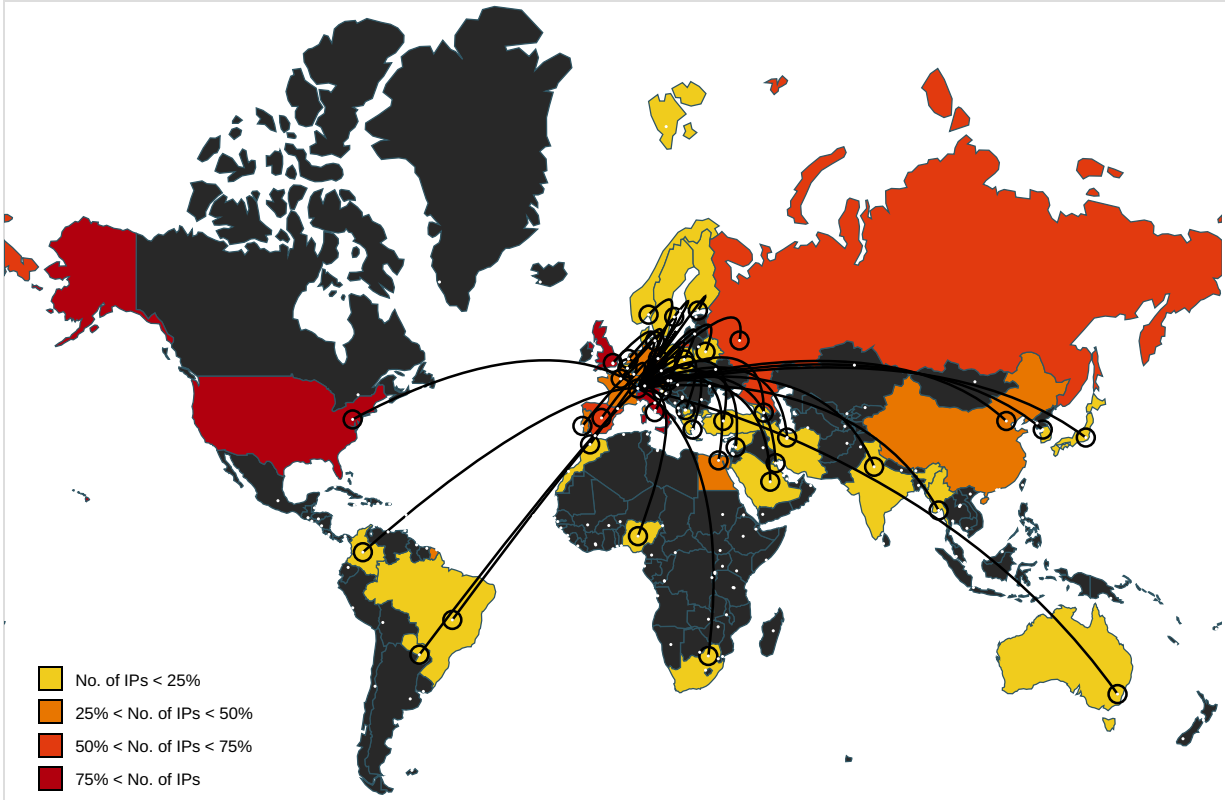
No contacted domains info

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
60.226.70.1	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
94.107.224.49	unknown	Belgium		47377	ORANGE_BELGIUM_SAKPNBelgiumBusinessNVhasbeenacquired	false
95.145.35.69	unknown	United Kingdom		12576	EELtdGB	false
62.76.90.1	unknown	Russian Federation		61400	NETRACK-ASRU	false
85.48.34.105	unknown	Spain		12479	UNI2-ASES	false
95.126.182.187	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
85.89.121.155	unknown	Russian Federation		5429	IIP-NET-AS5429RU	false
31.163.215.117	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
31.191.242.160	unknown	Italy		24608	WINDTRE-ASIT	false
95.226.168.243	unknown	Italy		3269	ASN-IBSNAZIT	false
87.186.120.233	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
94.132.45.232	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
178.120.4.157	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.30.239.199	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
95.141.197.180	unknown	Russian Federation		44158	ALTURA-ASRU	false
62.81.143.11	unknown	Spain		6739	ONO-ASCableuropa-ONOES	false
94.63.152.242	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	false
94.70.94.59	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
85.4.56.58	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
82.196.94.44	unknown	Russian Federation		20632	PETERSTAR-ASSaint-PetersburgRU	false
94.79.152.0	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
95.82.243.174	unknown	Russian Federation		12668	MIRALOGIC-ASRU	false
165.139.176.168	unknown	United States		11686	ENAUS	false
85.69.64.165	unknown	France		21502	ASN-NUMERICABLEFR	false
180.45.169.124	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
94.7.176.254	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
134.155.207.230	unknown	Germany		553	BELWUEBelWue-KoordinationEU	false
85.124.31.203	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
95.152.245.249	unknown	United Kingdom		8190	MDNXGB	false
85.126.133.224	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
150.215.62.16	unknown	United States		3680	NOVELLUS	false
95.94.164.54	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
94.177.219.212	unknown	Italy		31034	ARUBA-ASNIT	false
85.170.165.168	unknown	France		21502	ASN-NUMERICABLEFR	false
88.61.50.238	unknown	Italy		3269	ASN-IBSNAZIT	false
95.212.143.32	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
95.255.148.98	unknown	Italy		3269	ASN-IBSNAZIT	false
102.94.221.136	unknown	Nigeria		37075	ZAINUGASUG	false
44.135.35.240	unknown	United States		7377	UCSDUS	false
31.118.153.218	unknown	United Kingdom		12576	EELtdGB	false
31.38.6.179	unknown	France		5410	BOUYGTEL-ISPFR	false
88.241.107.77	unknown	Turkey		9121	TTNETTR	false
95.66.84.234	unknown	Kuwait		42961	GPRS-ASZAINKW	false
68.66.210.6	unknown	United States		55293	A2HOSTINGUS	false
72.147.224.57	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
95.193.27.123	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
62.23.59.149	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
94.236.86.104	unknown	United Kingdom		15395	RACKSPACE-LONGB	false
157.48.226.232	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
182.105.36.14	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
85.157.173.2	unknown	Finland		15527	ANVIASilmukkatie6VaasaFinlandFI	false
112.160.16.73	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
62.28.37.201	unknown	Portugal		15525	MEO-EMPRESASPT	false
94.208.51.101	unknown	Netherlands		33915	TNF-ASNL	false
132.197.249.125	unknown	United States		701	UUNETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.212.20.73	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
93.103.14.26	unknown	Slovenia		34779	T-2-ASASsetpropagatedbyT-2dooSI	false
181.71.150.158	unknown	Colombia		27831	ColombiaMovilCO	false
94.85.243.21	unknown	Italy		3269	ASN-IBSNAZIT	false
41.149.186.124	unknown	South Africa		5713	SAIX-NETZA	false
197.163.1.12	unknown	Egypt		24863	LINKdotNET-ASEG	false
62.83.246.144	unknown	Spain		12430	VODAFONE_ESES	false
162.50.37.237	unknown	United States		22958	FIDELITY-001US	false
95.48.117.196	unknown	Poland		5617	TPNETPL	false
62.235.224.99	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
31.221.210.155	unknown	Spain		16299	XFERAES	false
31.146.6.160	unknown	Georgia		35805	SILKNET-ASGE	false
112.86.152.55	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
62.120.3.102	unknown	Saudi Arabia		34400	ASN-ETTIHADETISALATSA	false
31.119.143.173	unknown	United Kingdom		12576	EELtdGB	false
31.100.145.50	unknown	United Kingdom		12576	EELtdGB	false
85.43.244.42	unknown	Italy		3269	ASN-IBSNAZIT	false
95.125.208.143	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
62.155.87.1	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
31.14.139.88	unknown	Italy		31034	ARUBA-ASNIT	false
95.7.215.147	unknown	Turkey		9121	TTNETTR	false
190.23.68.87	unknown	Paraguay		27866	COPACOPY	false
94.208.161.231	unknown	Netherlands		33915	TNF-ASNL	false
197.60.132.10	unknown	Egypt		8452	TE-ASTE-ASEG	false
135.66.52.3	unknown	United States		18676	AVAYAUS	false
95.33.71.119	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
41.248.235.194	unknown	Morocco		36903	MT-MPLSMA	false
62.114.184.238	unknown	Egypt		36992	ETISALAT-MISREG	false
103.99.28.153	unknown	Myanmar		136919	FACE24COLTD-AS-APFACE24CoLtdMM	false
31.179.155.83	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
173.140.23.196	unknown	United States		10507	SPCSUS	false
41.41.152.214	unknown	Egypt		8452	TE-ASTE-ASEG	false
85.252.191.146	unknown	Norway		2116	ASN-CATCHCOMNO	false
81.197.33.178	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
62.40.187.25	unknown	Austria		8339	KABSI-ASAT	false
62.147.6.228	unknown	France		12322	PROXADFR	false
50.190.219.211	unknown	United States		7922	COMCAST-7922US	false
179.135.242.184	unknown	Brazil		26599	TELEFONICABRASILSABR	false
37.10.4.102	unknown	Netherlands		43996	BOOKING-BVBookingcomNL	false
95.145.60.53	unknown	United Kingdom		12576	EELtdGB	false
62.145.208.62	unknown	Netherlands		33915	TNF-ASNL	false
182.133.200.184	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
101.246.44.255	unknown	China		17429	BGCTVNETBEIJINGGEHUACATVNETWORKCOLTDCN	false
94.144.144.173	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
95.156.28.214	unknown	Macedonia		6821	MT-AS-OWNbulOrceNikolovbbMK	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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.4519280276636035
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	kuCwPmEwdM
File size:	89612
MD5:	5503ada6da9fa406b1b76e372b1fcbb0
SHA1:	2aee070f638cbf5b49c5257c036118d9ca558f56
SHA256:	a909a24a46ef6270ac602102003e78a139e0750c3502a39f6c958896143d5bdb
SHA512:	eaf761947edb491f343d643af900032a73462e0a686b612e6900045598cf709a5bed7673858b78d03edef442503751e7e0bb862b468a6176d682652ba67e516c
SSDEEP:	1536:wa/QRnJeT0Q9aK88Q5Hi0eVTiZU3WSkHquiG7oBilom:FencTfedC0eVGZHSkHquiG7ac
TLSH:	4193A61E2E258FBCF79D863547B78E229648338A26E1C545E15CEA011EB034E741FBED
File Content Preview:	.ELF.....@.`...4..[.....4. ...(.....@...@....T...T.....T..ET..ET.....dt.Q.....<...'.....!'.....<...'.....!... ....'9... ..... <...'..h...!.....'9H

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V

ELF header	
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	89052
Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x147d0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x4148f0	0x148f0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x414950	0x14950	0xba0	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x4554f4	0x154f4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x4554fc	0x154fc	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x455508	0x15508	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x455510	0x15510	0x250	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x455760	0x15760	0x418	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x455b78	0x15b78	0x24	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x455ba0	0x15b78	0x340	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x71a	0x15b78	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x15b78	0x64	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	0x400000	0x400000	0x154f0	0x154f0	3.4219	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x154f4	0x4554f4	0x4554f4	0x684	0x9ec	2.7884	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.147.25.230546088028394710 5/27/22-12:47:34.014385	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54608	80	192.168.2.23	88.147.25.230
192.168.2.2395.215.185.234388448028394710 5/27/22-12:47:51.607040	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38844	80	192.168.2.23	95.215.185.234
192.168.2.2395.67.237.665908280283947105/27/22-12:47:15.080363	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59082	80	192.168.2.23	95.67.237.66

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.112.154.17441676802839471 05/27/22-12:47:15.090627	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41676	80	192.168.2.23	88.112.154.174
192.168.2.2341.62.245.11149730372152835222 05/27/22-12:47:53.882683	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49730	37215	192.168.2.23	41.62.245.111
192.168.2.2395.179.137.17458194802839471 05/27/22-12:48:14.438208	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58194	80	192.168.2.23	95.179.137.174
192.168.2.2388.150.144.1353878802839471 05/27/22-12:47:10.978190	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53878	80	192.168.2.23	88.150.144.13
192.168.2.2395.130.6.15141382802839471 05/27/22-12:47:15.059849	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41382	80	192.168.2.23	95.130.6.151
192.168.2.2388.221.78.1259134802839471 05/27/22-12:47:49.018701	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59134	80	192.168.2.23	88.221.78.12
192.168.2.2395.214.234.13634152802839471 05/27/22-12:48:04.635268	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34152	80	192.168.2.23	95.214.234.136
192.168.2.2395.112.26.17644764802839471 05/27/22-12:47:49.003840	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44764	80	192.168.2.23	95.112.26.176
192.168.2.2395.100.241.10034392802839471 05/27/22-12:48:03.504850	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34392	80	192.168.2.23	95.100.241.100
192.168.2.2395.216.150.19036108802839471 05/27/22-12:47:15.053671	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36108	80	192.168.2.23	95.216.150.190
192.168.2.2395.159.21.17353860802839471 05/27/22-12:47:59.854206	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53860	80	192.168.2.23	95.159.21.173
192.168.2.2395.56.53.13533488802839471 05/27/22-12:47:49.073357	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33488	80	192.168.2.23	95.56.53.135
192.168.2.2388.255.41.2859640802839471 05/27/22-12:47:13.505289	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59640	80	192.168.2.23	88.255.41.28
192.168.2.23112.223.18.12440804802839471 05/27/22-12:47:13.498434	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40804	80	192.168.2.23	112.223.18.124
192.168.2.2388.247.238.12639848802839471 05/27/22-12:46:57.495420	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39848	80	192.168.2.23	88.247.238.126
192.168.2.2395.146.194.15851092802839471 05/27/22-12:47:33.709741	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51092	80	192.168.2.23	95.146.194.158
192.168.2.2395.100.230.2060114802839471 05/27/22-12:47:31.209429	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60114	80	192.168.2.23	95.100.230.20
192.168.2.2395.167.73.7760578802839471 05/27/22-12:47:07.038688	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60578	80	192.168.2.23	95.167.73.77
192.168.2.2395.122.162.8149276802839471 05/27/22-12:48:07.946255	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49276	80	192.168.2.23	95.122.162.81

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.100.170.10448188802839471 05/27/22-12:47:07.172463	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48188	80	192.168.2.23	95.100.170.104
192.168.2.2395.100.208.23146568802839471 05/27/22-12:48:16.775027	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46568	80	192.168.2.23	95.100.208.231
192.168.2.2395.215.255.9151586802839471 05/27/22-12:47:42.722816	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51586	80	192.168.2.23	95.215.255.91
192.168.2.2388.198.110.23440074802839471 05/27/22-12:47:46.661375	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40074	80	192.168.2.23	88.198.110.234
192.168.2.2388.136.102.12851928802839471 05/27/22-12:47:38.633741	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51928	80	192.168.2.23	88.136.102.128
192.168.2.2388.136.54.2860044802839471 05/27/22-12:47:27.579938	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60044	80	192.168.2.23	88.136.54.28
192.168.2.2395.156.55.2955906802839471 05/27/22-12:47:36.188256	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	55906	80	192.168.2.23	95.156.55.29
192.168.2.2388.221.188.4335412802839471 05/27/22-12:47:29.045100	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35412	80	192.168.2.23	88.221.188.43
192.168.2.2388.255.253.4234062802839471 05/27/22-12:48:16.968700	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34062	80	192.168.2.23	88.255.253.42
192.168.2.2388.214.45.152148802839471 05/27/22-12:47:24.075213	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52148	80	192.168.2.23	88.214.45.1
192.168.2.2395.101.211.16546204802839471 05/27/22-12:47:10.944613	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46204	80	192.168.2.23	95.101.211.165
192.168.2.23112.17.57.16850558802839471 05/27/22-12:47:20.105563	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50558	80	192.168.2.23	112.17.57.168
192.168.2.2395.216.182.20750770802839471 05/27/22-12:47:58.808550	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	50770	80	192.168.2.23	95.216.182.207
192.168.2.2395.101.70.4758192802839471 05/27/22-12:47:15.046152	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58192	80	192.168.2.23	95.101.70.47
192.168.2.2395.168.220.9735532802839471 05/27/22-12:46:57.377011	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35532	80	192.168.2.23	95.168.220.97
192.168.2.23112.72.51.7837596802839471 05/27/22-12:48:11.670529	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37596	80	192.168.2.23	112.72.51.78
192.168.2.2395.101.242.23146042802839471 05/27/22-12:47:31.204962	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46042	80	192.168.2.23	95.101.242.231
192.168.2.2388.214.188.14054808802839471 05/27/22-12:47:49.127460	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54808	80	192.168.2.23	88.214.188.140
192.168.2.2395.101.23.23945600802839471 05/27/22-12:47:51.604867	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45600	80	192.168.2.23	95.101.23.239

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.216.72.71 39974802839471 05/27/22-12:48:12.019932	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39974	80	192.168.2.23	95.216.72.71
192.168.2.2395.159.11.30 59024802839471 05/27/22-12:48:16.848947	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59024	80	192.168.2.23	95.159.11.30
192.168.2.2395.100.83.16 49496802839471 05/27/22-12:47:28.999232	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49496	80	192.168.2.23	95.100.83.16
192.168.2.2395.65.56.138 36468802839471 05/27/22-12:48:10.168925	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36468	80	192.168.2.23	95.65.56.138
192.168.2.2388.198.148.2 3836254802839471 05/27/22-12:47:38.619624	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	36254	80	192.168.2.23	88.198.148.238
192.168.2.2395.128.147.2 2039230802839471 05/27/22-12:48:19.208516	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39230	80	192.168.2.23	95.128.147.220
192.168.2.23112.205.95.4 333448802839471 05/27/22-12:48:11.887654	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	33448	80	192.168.2.23	112.205.95.43
192.168.2.2395.87.64.255 48256802839471 05/27/22-12:48:14.568167	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48256	80	192.168.2.23	95.87.64.255
192.168.2.23112.171.3.21 846612802839471 05/27/22-12:47:13.447133	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46612	80	192.168.2.23	112.171.3.218
192.168.2.2388.210.22.22 158942802839471 05/27/22-12:47:06.690087	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58942	80	192.168.2.23	88.210.22.221
192.168.2.2395.101.156.1 4756178802839471 05/27/22-12:47:36.242927	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	56178	80	192.168.2.23	95.101.156.147
192.168.2.2388.249.107.2 5445124802839471 05/27/22-12:47:29.101579	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45124	80	192.168.2.23	88.249.107.254
192.168.2.23112.194.65.2 5249746802839471 05/27/22-12:47:23.716570	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49746	80	192.168.2.23	112.194.65.252
192.168.2.2395.49.221.10 932828802839471 05/27/22-12:47:42.672755	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	32828	80	192.168.2.23	95.49.221.109
192.168.2.23112.171.3.21 846688802839471 05/27/22-12:47:16.542926	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46688	80	192.168.2.23	112.171.3.218
192.168.2.2395.129.137.2 4538576802839471 05/27/22-12:47:36.183582	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38576	80	192.168.2.23	95.129.137.245
192.168.2.2388.28.199.25 340702802839471 05/27/22-12:47:11.081110	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	40702	80	192.168.2.23	88.28.199.253
192.168.2.23112.17.60.40 39644802839471 05/27/22-12:47:53.228125	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39644	80	192.168.2.23	112.17.60.40
192.168.2.2395.231.53.22 052380802839471 05/27/22-12:48:04.736705	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	52380	80	192.168.2.23	95.231.53.220

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23197.234.61.1134194237215283522205/27/22-12:48:13.090975	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41942	37215	192.168.2.23	197.234.61.113
192.168.2.2395.68.75.9742456802839471 05/27/22-12:46:55.294531	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	42456	80	192.168.2.23	95.68.75.97
192.168.2.23197.214.98.1325569837215283522205/27/22-12:47:20.408675	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55698	37215	192.168.2.23	197.214.98.132
192.168.2.2395.121.139.12559944802839471 05/27/22-12:47:20.135801	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59944	80	192.168.2.23	95.121.139.125
192.168.2.2395.156.51.102595768028394705/27/22-12:48:12.074131	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	59576	80	192.168.2.23	95.156.51.102
192.168.2.2395.217.109.1953226802839471 05/27/22-12:46:57.392990	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	53226	80	192.168.2.23	95.217.109.19
192.168.2.2395.68.127.121466548028394715/27/22-12:48:14.464045	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	46654	80	192.168.2.23	95.68.127.121
192.168.2.2395.100.241.100343828028394715/27/22-12:48:02.219711	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34382	80	192.168.2.23	95.100.241.100
192.168.2.23112.120.6.6139842802839471 05/27/22-12:48:11.903918	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	39842	80	192.168.2.23	112.120.6.61
192.168.2.2388.210.144.12460104802839471 05/27/22-12:47:27.576693	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60104	80	192.168.2.23	88.210.144.124
192.168.2.2395.57.98.20234828028394715/27/22-12:47:36.352619	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	34828	80	192.168.2.23	95.57.98.202
192.168.2.2395.211.75.2541774802839471 05/27/22-12:48:19.124724	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	41774	80	192.168.2.23	95.211.75.25
192.168.2.2395.57.203.25247000802839471 05/27/22-12:48:19.323847	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47000	80	192.168.2.23	95.57.203.252
192.168.2.23112.171.248.108371608028394715/27/22-12:47:27.589765	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37160	80	192.168.2.23	112.171.248.108
192.168.2.2388.149.185.11848152802839471 05/27/22-12:47:29.046007	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	48152	80	192.168.2.23	88.149.185.118
192.168.2.2395.57.207.24558776802839471 05/27/22-12:47:31.306412	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	58776	80	192.168.2.23	95.57.207.245
192.168.2.2395.101.222.5660330802839471 05/27/22-12:47:49.004541	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60330	80	192.168.2.23	95.101.222.56
192.168.2.2395.100.83.3160434802839471 05/27/22-12:47:51.581498	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	60434	80	192.168.2.23	95.100.83.31

TCP Packets

HTTP Request Dependency Graph

- 192.168.0.14:80

System Behavior

Analysis Process: kuCwPmEwdM PID: **6230**, Parent PID: **6126**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	/tmp/kuCwPmEwdM
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: kuCwPmEwdM PID: **6233**, Parent PID: **6230**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: kuCwPmEwdM PID: **6234**, Parent PID: **6230**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: kuCwPmEwdM PID: **6236**, Parent PID: **6230**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: kuCwPmEwdM PID: **6239**, Parent PID: **6236**

General

Start time:	12:46:52

Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: kuCwPmEwdM PID: **6240**, Parent PID: **6236**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: kuCwPmEwdM PID: **6241**, Parent PID: **6236**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: kuCwPmEwdM PID: **6242**, Parent PID: **6236**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: kuCwPmEwdM PID: **6248**, Parent PID: **6236**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: kuCwPmEwdM PID: **6249**, Parent PID: **6236**

General

Start time:	12:46:52
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: kuCwPmEwdM PID: **6291**, Parent PID: **6236**

General

Start time:	12:48:13
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: kuCwPmEwdM PID: **6293**, Parent PID: **6291**

General

Start time:	12:48:13
Start date:	27/05/2022
Path:	/tmp/kuCwPmEwdM
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c