ID: 626439
Sample Name: pjT3uuMrF1
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:18:53
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

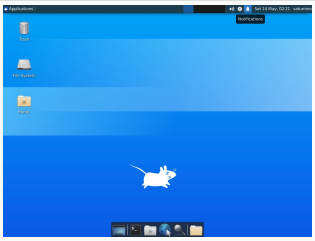
Linux Analysis Report

pjT3uuMrF1

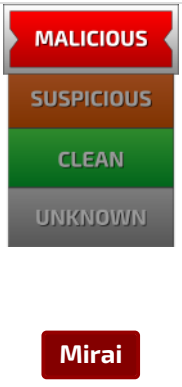
Overview

General Information

Sample Name:	pjT3uuMrF1
Analysis ID:	626439
MD5:	e8511d7655b6bb.
SHA1:	0d946d9f597a16..
SHA256:	156bf5a274c0b1..
Tags:	32 arm elf mirai
Infos:	



Detection

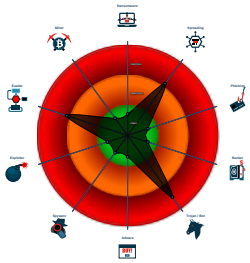


Score:	92
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Snort IDS alert for network traffic
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample contains only a LOAD segm…
- Yara signature match
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…

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:	626439
Start date and time: 14/05/202202:18:53	2022-05-14 02:18:53 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pjT3uuMrF1
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:	mal92.spre.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/pjT3uuMrF1
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	kebabware installed

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- pjT3uuMrF1 (PID: 6230, Parent: 6125, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/pjT3uuMrF1
  - pjT3uuMrF1 New Fork (PID: 6232, Parent: 6230)
    - pjT3uuMrF1 New Fork (PID: 6234, Parent: 6232)
    - pjT3uuMrF1 New Fork (PID: 6235, Parent: 6232)
    - pjT3uuMrF1 New Fork (PID: 6238, Parent: 6232)
    - pjT3uuMrF1 New Fork (PID: 6239, Parent: 6232)
    - pjT3uuMrF1 New Fork (PID: 6243, Parent: 6232)
    - pjT3uuMrF1 New Fork (PID: 6245, Parent: 6232)
    - pjT3uuMrF1 New Fork (PID: 6247, Parent: 6232)
    - pjT3uuMrF1 New Fork (PID: 6248, Parent: 6232)
- gnome-session-binary New Fork (PID: 6287, Parent: 1477)
  - sh (PID: 6287, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
  - gsd-print-notifications (PID: 6287, Parent: 1477, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6295, Parent: 6287)
      - gsd-print-notifications New Fork (PID: 6296, Parent: 6295)
        - gsd-printer (PID: 6296, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- xfce4-session New Fork (PID: 6317, Parent: 1900)
  - rm (PID: 6317, Parent: 1900, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /home/saturnino/.cache/sessions/Thunar-2ec9153f1-6fa0-4067-96b1-e5fe875b1e51
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
pjT3uuMrF1	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x807c:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x80eb:$s2: $Id: UPX • 0x809c:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
6234.1.0000000031c29fda.00000000517a471f.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x14f0:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1560:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1620:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
6230.1.0000000031c29fda.00000000517a471f.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x14f0:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1560:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x1620:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3

Source	Rule	Description	Author	Strings
6230.1.000000003d1482af.00000000e83cf7de.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x14028:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6 \xAD\xB3 • 0x14084:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6 \xAD\xB3 • 0x14120:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6 \xAD\xB3
6230.1.000000003d1482af.00000000e83cf7de.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x132cc:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
6230.1.000000003d1482af.00000000e83cf7de.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
Click to see the 5 entries				

Snort Signatures

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.255.83.100

Timestamp:	192.168.2.23172.255.83.10051174555552027153 05/14/22-02:19:57.628001
SID:	2027153
Source Port:	51174
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.143.204.238

Timestamp:	192.168.2.2395.143.204.23852402802027121 05/14/22-02:19:59.979425
SID:	2027121
Source Port:	52402
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.136.115.74

Timestamp:	192.168.2.2395.136.115.7450126802027121 05/14/22-02:21:11.764865
SID:	2027121
Source Port:	50126
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.246.194.226

Timestamp:	192.168.2.23197.246.194.226535663721528352222 05/14/22-02:21:39.028446
SID:	2835222
Source Port:	53566
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.81.179

Timestamp:	192.168.2.23172.65.81.17953844555552027153 05/14/22-02:19:59.137951
SID:	2027153
Source Port:	53844
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.234.231.229	
Timestamp:	192.168.2.23156.234.231.22957116528692027339 05/14/22-02:20:29.429465
SID:	2027339
Source Port:	57116
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.177.82	
Timestamp:	192.168.2.23172.65.177.8248362555552027153 05/14/22-02:21:10.452251
SID:	2027153
Source Port:	48362
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.142.64.151	
Timestamp:	192.168.2.2395.142.64.15133610802027121 05/14/22-02:19:53.342712
SID:	2027121
Source Port:	33610
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.139.94	
Timestamp:	192.168.2.2395.56.139.9459572802027121 05/14/22-02:21:32.727426
SID:	2027121
Source Port:	59572
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.211.103.152	
Timestamp:	192.168.2.2395.211.103.15238686802027121 05/14/22-02:19:47.512944
SID:	2027121
Source Port:	38686
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.31.7.65	
Timestamp:	192.168.2.2395.31.7.6547324802027121 05/14/22-02:20:02.461488
SID:	2027121
Source Port:	47324
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.238.125	
Timestamp:	192.168.2.23172.65.238.12554388555552027153 05/14/22-02:20:08.992019
SID:	2027153
Source Port:	54388
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.189.104.138	
Timestamp:	192.168.2.2395.189.104.13841018802027121 05/14/22-02:20:32.218131
SID:	2027121
Source Port:	41018

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

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.61.121.206

Timestamp:	192.168.2.2395.61.121.20644906802027121 05/14/22-02:20:03.803878
SID:	2027121
Source Port:	44906
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.240.226

Timestamp:	192.168.2.2395.100.240.22653848802027121 05/14/22-02:21:23.038728
SID:	2027121
Source Port:	53848
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.187.125

Timestamp:	192.168.2.23172.65.187.12539084555552027153 05/14/22-02:20:37.047910
SID:	2027153
Source Port:	39084
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.169.96

Timestamp:	192.168.2.2395.216.169.9635526802027121 05/14/22-02:20:28.438174
SID:	2027121
Source Port:	35526
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.9.211.134

Timestamp:	192.168.2.2395.9.211.13445804802027121 05/14/22-02:20:50.335116
SID:	2027121
Source Port:	45804
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.0.203

Timestamp:	192.168.2.2395.159.0.20360034802027121 05/14/22-02:20:28.556099
SID:	2027121
Source Port:	60034
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.7.39

Timestamp:	192.168.2.2395.159.7.3947180802027121 05/14/22-02:21:16.327351
SID:	2027121
Source Port:	47180
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.29.180	
Timestamp:	192.168.2.2395.56.29.18036084802027121 05/14/22-02:20:48.149836
SID:	2027121
Source Port:	36084
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.109.124	
Timestamp:	192.168.2.23172.65.109.12442672555552027153 05/14/22-02:21:06.678651
SID:	2027153
Source Port:	42672
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.80.250	
Timestamp:	192.168.2.23172.65.80.25057792555552027153 05/14/22-02:19:50.996196
SID:	2027153
Source Port:	57792
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.203.183	
Timestamp:	192.168.2.23172.65.203.18340090555552027153 05/14/22-02:19:57.645189
SID:	2027153
Source Port:	40090
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.244.124.62	
Timestamp:	192.168.2.23156.244.124.6254780528692027339 05/14/22-02:21:19.394819
SID:	2027339
Source Port:	54780
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.65.111.192	
Timestamp:	192.168.2.2395.65.111.19238106802027121 05/14/22-02:20:56.002880
SID:	2027121
Source Port:	38106
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.250.91.131	
Timestamp:	192.168.2.23156.250.91.13145570528692027339 05/14/22-02:20:29.395003
SID:	2027339
Source Port:	45570
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.33.214	
Timestamp:	192.168.2.2395.159.33.21456926802027121 05/14/22-02:20:54.820107
SID:	2027121
Source Port:	56926

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

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.234.194	
Timestamp:	192.168.2.23172.65.234.19437462555552027153 05/14/22-02:19:47.505957
SID:	2027153
Source Port:	37462
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 98.159.33.194	
Timestamp:	192.168.2.2398.159.33.19449528555552027153 05/14/22-02:20:13.406392
SID:	2027153
Source Port:	49528
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.8.62	
Timestamp:	192.168.2.2395.216.8.6260662802027121 05/14/22-02:20:26.047138
SID:	2027121
Source Port:	60662
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.60.119	
Timestamp:	192.168.2.2395.100.60.11932814802027121 05/14/22-02:19:52.635703
SID:	2027121
Source Port:	32814
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.107.229.36	
Timestamp:	192.168.2.2395.107.229.3633744802027121 05/14/22-02:21:14.075300
SID:	2027121
Source Port:	33744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.4.72	
Timestamp:	192.168.2.23172.65.4.7238672555552027153 05/14/22-02:20:18.663856
SID:	2027153
Source Port:	38672
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.245.84.157	
Timestamp:	192.168.2.2395.245.84.15734900802027121 05/14/22-02:20:23.687567
SID:	2027121
Source Port:	34900
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.164.58	
Timestamp:	192.168.2.2395.101.164.5855826802027121 05/14/22-02:20:39.296946
SID:	2027121
Source Port:	55826
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.215.239.146	
Timestamp:	192.168.2.2395.215.239.14640644802027121 05/14/22-02:21:03.782018
SID:	2027121
Source Port:	40644
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.179.202.205	
Timestamp:	192.168.2.2395.179.202.20535652802027121 05/14/22-02:20:29.974289
SID:	2027121
Source Port:	35652
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.65.49.228	
Timestamp:	192.168.2.2395.65.49.22848088802027121 05/14/22-02:20:28.494212
SID:	2027121
Source Port:	48088
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.155.78	
Timestamp:	192.168.2.23172.65.155.7835938555552027153 05/14/22-02:20:03.389982
SID:	2027153
Source Port:	35938
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.28.188	
Timestamp:	192.168.2.23172.65.28.18837548555552027153 05/14/22-02:21:10.434822
SID:	2027153
Source Port:	37548
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.217.140	
Timestamp:	192.168.2.2395.56.217.14057738802027121 05/14/22-02:20:32.203958
SID:	2027121
Source Port:	57738
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.124.219	
Timestamp:	192.168.2.2395.100.124.21940064802027121 05/14/22-02:21:03.799358
SID:	2027121
Source Port:	40064

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

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.135.200.33	
Timestamp:	192.168.2.23112.135.200.3347048802027121 05/14/22-02:20:26.004599
SID:	2027121
Source Port:	47048
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.163.168.109	
Timestamp:	192.168.2.2395.163.168.10943244802027121 05/14/22-02:20:50.298257
SID:	2027121
Source Port:	43244
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.254.28	
Timestamp:	192.168.2.23172.65.254.2849556555552027153 05/14/22-02:20:53.942992
SID:	2027153
Source Port:	49556
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.237.77.45	
Timestamp:	192.168.2.23197.237.77.4548226372152835222 05/14/22-02:21:12.221258
SID:	2835222
Source Port:	48226
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.28.223.127	
Timestamp:	192.168.2.2395.28.223.12760158802027121 05/14/22-02:19:54.571832
SID:	2027121
Source Port:	60158
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.208.221	
Timestamp:	192.168.2.23172.65.208.22147180555552027153 05/14/22-02:21:15.003517
SID:	2027153
Source Port:	47180
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.141.209.237	
Timestamp:	192.168.2.2395.141.209.23753648802027121 05/14/22-02:21:16.255320
SID:	2027121
Source Port:	53648
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.173.176	
Timestamp:	192.168.2.2395.217.173.17642360802027121 05/14/22-02:19:59.979314
SID:	2027121
Source Port:	42360
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.254.198	
Timestamp:	192.168.2.23172.65.254.19839484555552027153 05/14/22-02:19:49.942206
SID:	2027153
Source Port:	39484
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.156.252	
Timestamp:	192.168.2.2395.217.156.25245090802027121 05/14/22-02:20:55.948104
SID:	2027121
Source Port:	45090
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.100.22	
Timestamp:	192.168.2.23172.65.100.2259092555552027153 05/14/22-02:20:55.145336
SID:	2027153
Source Port:	59092
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.121.177.221	
Timestamp:	192.168.2.23112.121.177.22134130802027121 05/14/22-02:20:44.359761
SID:	2027121
Source Port:	34130
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.51.29	
Timestamp:	192.168.2.2395.159.51.2953666802027121 05/14/22-02:19:52.694475
SID:	2027121
Source Port:	53666
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.215.101.81	
Timestamp:	192.168.2.23112.215.101.8160170802027121 05/14/22-02:20:38.895103
SID:	2027121
Source Port:	60170
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.22.163	
Timestamp:	192.168.2.2395.101.22.16334682802027121 05/14/22-02:21:28.995999
SID:	2027121
Source Port:	34682

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

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.165.133.145	
Timestamp:	192.168.2.2395.165.133.14534562802027121 05/14/22-02:20:37.016015
SID:	2027121
Source Port:	34562
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.220.152	
Timestamp:	192.168.2.23172.65.220.15233210555552027153 05/14/22-02:19:47.522649
SID:	2027153
Source Port:	33210
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.226.94	
Timestamp:	192.168.2.23172.65.226.9456510555552027153 05/14/22-02:20:26.128722
SID:	2027153
Source Port:	56510
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.98.68	
Timestamp:	192.168.2.23172.65.98.6846890555552027153 05/14/22-02:20:51.595727
SID:	2027153
Source Port:	46890
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 98.159.224.19	
Timestamp:	192.168.2.2398.159.224.1937196555552027153 05/14/22-02:21:10.525505
SID:	2027153
Source Port:	37196
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.100.90	
Timestamp:	192.168.2.2395.217.100.9050666802027121 05/14/22-02:20:07.909211
SID:	2027121
Source Port:	50666
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.173.188.17	
Timestamp:	192.168.2.2395.173.188.1753452802027121 05/14/22-02:21:16.301756
SID:	2027121
Source Port:	53452
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.163.40.130	
Timestamp:	192.168.2.2395.163.40.13056302802027121 05/14/22-02:20:17.767623
SID:	2027121
Source Port:	56302
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.205.61.159	
Timestamp:	192.168.2.2395.205.61.15945412802027121 05/14/22-02:21:23.140530
SID:	2027121
Source Port:	45412
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.152.91	
Timestamp:	192.168.2.2395.217.152.9160996802027121 05/14/22-02:21:29.005358
SID:	2027121
Source Port:	60996
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.106.58.150	
Timestamp:	192.168.2.23112.106.58.15039318802027121 05/14/22-02:20:02.405864
SID:	2027121
Source Port:	39318
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.179.60.106	
Timestamp:	192.168.2.23112.179.60.10652164802027121 05/14/22-02:19:47.485907
SID:	2027121
Source Port:	52164
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.14.216	
Timestamp:	192.168.2.2395.216.14.21637572802027121 05/14/22-02:20:40.548225
SID:	2027121
Source Port:	37572
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.70.156	
Timestamp:	192.168.2.23172.65.70.15634830555552027153 05/14/22-02:21:29.853316
SID:	2027153
Source Port:	34830
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.241.119.167	
Timestamp:	192.168.2.23156.241.119.167513365286920273 39 05/14/22-02:21:38.199643
SID:	2027339
Source Port:	51336

Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.234.111	
Timestamp:	192.168.2.2395.56.234.11157896802027121 05/14/22-02:20:26.254878
SID:	2027121
Source Port:	57896
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.233.22.202	
Timestamp:	192.168.2.2395.233.22.20254454802027121 05/14/22-02:19:59.937809
SID:	2027121
Source Port:	54454
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.111.244.253	
Timestamp:	192.168.2.2395.111.244.25339608802027121 05/14/22-02:20:58.081431
SID:	2027121
Source Port:	39608
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.140.156.43	
Timestamp:	192.168.2.2395.140.156.4346396802027121 05/14/22-02:20:48.022368
SID:	2027121
Source Port:	46396
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.242.104	
Timestamp:	192.168.2.2395.101.242.10450832802027121 05/14/22-02:19:54.491456
SID:	2027121
Source Port:	50832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.97.132.130	
Timestamp:	192.168.2.23172.97.132.13055154555552027153 05/14/22-02:19:45.321580
SID:	2027153
Source Port:	55154
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.161.182.2	
Timestamp:	192.168.2.2395.161.182.236966802027121 05/14/22-02:20:39.165687
SID:	2027121
Source Port:	36966
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.223.151	
Timestamp:	192.168.2.2395.56.223.15134538802027121 05/14/22-02:20:15.032748
SID:	2027121
Source Port:	34538
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.57.74.33	
Timestamp:	192.168.2.2395.57.74.3350396802027121 05/14/22-02:19:54.640711
SID:	2027121
Source Port:	50396
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.215.86	
Timestamp:	192.168.2.2395.217.215.8660962802027121 05/14/22-02:20:20.205596
SID:	2027121
Source Port:	60962
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.5.49	
Timestamp:	192.168.2.23172.65.5.4944762555552027153 05/14/22-02:20:15.566625
SID:	2027153
Source Port:	44762
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.121.57	
Timestamp:	192.168.2.2395.217.121.5748134802027121 05/14/22-02:20:47.995507
SID:	2027121
Source Port:	48134
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.146.58	
Timestamp:	192.168.2.23172.65.146.5845536555552027153 05/14/22-02:20:53.942910
SID:	2027153
Source Port:	45536
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.55.164	
Timestamp:	192.168.2.2395.159.55.16432974802027121 05/14/22-02:20:28.550766
SID:	2027121
Source Port:	32974
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.152.195	
Timestamp:	192.168.2.23172.65.152.19558680555552027153 05/14/22-02:21:15.003655
SID:	2027153
Source Port:	58680

Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.50.29	
Timestamp:	192.168.2.2395.101.50.2936210802027121 05/14/22-02:20:58.196781
SID:	2027121
Source Port:	36210
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.245.84.201	
Timestamp:	192.168.2.23172.245.84.20155974555552027153 05/14/22-02:20:21.837542
SID:	2027153
Source Port:	55974
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.211.3.47	
Timestamp:	192.168.2.2395.211.3.4758028802027121 05/14/22-02:21:11.754876
SID:	2027121
Source Port:	58028
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.46.167	
Timestamp:	192.168.2.23172.65.46.167368785555552027153 05/14/22-02:20:26.128840
SID:	2027153
Source Port:	36878
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.61.121.206	
Timestamp:	192.168.2.2395.61.121.20644884802027121 05/14/22-02:20:02.452312
SID:	2027121
Source Port:	44884
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.32.133	
Timestamp:	192.168.2.2395.100.32.13358682802027121 05/14/22-02:20:12.238521
SID:	2027121
Source Port:	58682
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.79.32.42	
Timestamp:	192.168.2.23112.79.32.4242658802027121 05/14/22-02:20:23.608445
SID:	2027121
Source Port:	42658
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.123.205	
Timestamp:	192.168.2.2395.100.123.20540996802027121 05/14/22-02:21:00.525492
SID:	2027121
Source Port:	40996
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.255.113	
Timestamp:	192.168.2.23172.65.255.11347180555552027153 05/14/22-02:19:54.382118
SID:	2027153
Source Port:	47180
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.214.235.126	
Timestamp:	192.168.2.2395.214.235.12633216802027121 05/14/22-02:20:07.909063
SID:	2027121
Source Port:	33216
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.224.25.142	
Timestamp:	192.168.2.23156.224.25.14240106528692027339 05/14/22-02:20:47.247262
SID:	2027339
Source Port:	40106
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.87.254.43	
Timestamp:	192.168.2.2395.87.254.4357278802027121 05/14/22-02:19:53.372300
SID:	2027121
Source Port:	57278
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.131.149.114	
Timestamp:	192.168.2.2395.131.149.11457714802027121 05/14/22-02:21:34.904086
SID:	2027121
Source Port:	57714
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.147.80	
Timestamp:	192.168.2.2395.217.147.8037940802027121 05/14/22-02:20:37.002920
SID:	2027121
Source Port:	37940
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.85.88	
Timestamp:	192.168.2.2395.101.85.8852956802027121 05/14/22-02:20:58.119066
SID:	2027121
Source Port:	52956

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

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.97.128	
Timestamp:	192.168.2.23172.65.97.12843836555552027153 05/14/22-02:21:31.954750
SID:	2027153
Source Port:	43836
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.143.229.49	
Timestamp:	192.168.2.2395.143.229.4937410802027121 05/14/22-02:20:47.942900
SID:	2027121
Source Port:	37410
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.231.189	
Timestamp:	192.168.2.23172.65.231.18936138555552027153 05/14/22-02:20:26.126595
SID:	2027153
Source Port:	36138
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.245.77.54	
Timestamp:	192.168.2.23172.245.77.5443396555552027153 05/14/22-02:19:50.861365
SID:	2027153
Source Port:	43396
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.96.216	
Timestamp:	192.168.2.2395.101.96.21634304802027121 05/14/22-02:21:00.513758
SID:	2027121
Source Port:	34304
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.215.170.31	
Timestamp:	192.168.2.2395.215.170.3138548802027121 05/14/22-02:20:52.527746
SID:	2027121
Source Port:	38548
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.252.56.125	
Timestamp:	192.168.2.2395.252.56.12541832802027121 05/14/22-02:21:34.895934
SID:	2027121
Source Port:	41832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.58.75.108	
Timestamp:	192.168.2.2395.58.75.10847170802027121 05/14/22-02:21:11.847346
SID:	2027121
Source Port:	47170
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.30.92	
Timestamp:	192.168.2.2395.159.30.9250334802027121 05/14/22-02:21:25.371312
SID:	2027121
Source Port:	50334
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.131.136.65	
Timestamp:	192.168.2.2395.131.136.6544472802027121 05/14/22-02:20:26.033464
SID:	2027121
Source Port:	44472
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.142.75.181	
Timestamp:	192.168.2.2395.142.75.18149820802027121 05/14/22-02:20:55.954772
SID:	2027121
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.241.13.97	
Timestamp:	192.168.2.23156.241.13.9738248528692027339 05/14/22-02:19:49.315222
SID:	2027339
Source Port:	38248
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.227.114	
Timestamp:	192.168.2.23172.65.227.11452622555552027153 05/14/22-02:21:06.661307
SID:	2027153
Source Port:	52622
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.225.159.182	
Timestamp:	192.168.2.23156.225.159.18250730528692027339 05/14/22-02:20:25.835892
SID:	2027339
Source Port:	50730
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.209.146.210	
Timestamp:	192.168.2.2395.209.146.21050540802027121 05/14/22-02:20:38.689489
SID:	2027121
Source Port:	50540

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

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.163.133	
Timestamp:	192.168.2.23172.65.163.13350650555552027153 05/14/22-02:20:39.493185
SID:	2027153
Source Port:	50650
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.213.40.5	
Timestamp:	192.168.2.2395.213.40.556526802027121 05/14/22-02:20:28.445974
SID:	2027121
Source Port:	56526
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.180.165.203	
Timestamp:	192.168.2.2395.180.165.20354376802027121 05/14/22-02:20:29.989309
SID:	2027121
Source Port:	54376
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.166.120.72	
Timestamp:	192.168.2.2395.166.120.7254750802027121 05/14/22-02:21:23.057590
SID:	2027121
Source Port:	54750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.255.80.6	
Timestamp:	192.168.2.23172.255.80.660084555552027153 05/14/22-02:20:08.975191
SID:	2027153
Source Port:	60084
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.238.33	
Timestamp:	192.168.2.2395.101.238.3342720802027121 05/14/22-02:20:17.717017
SID:	2027121
Source Port:	42720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.179.156.25	
Timestamp:	192.168.2.2395.179.156.2557406802027121 05/14/22-02:20:02.429434
SID:	2027121
Source Port:	57406
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.210.226	
Timestamp:	192.168.2.2395.101.210.22652942802027121 05/14/22-02:20:35.416113
SID:	2027121
Source Port:	52942
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.169.202.100	
Timestamp:	192.168.2.23112.169.202.10050322802027121 05/14/22-02:21:05.146467
SID:	2027121
Source Port:	50322
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.213.201.60	
Timestamp:	192.168.2.2395.213.201.6045874802027121 05/14/22-02:19:52.681868
SID:	2027121
Source Port:	45874
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.255.83.91	
Timestamp:	192.168.2.23172.255.83.9140446555552027153 05/14/22-02:21:07.857174
SID:	2027153
Source Port:	40446
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.170.196.184	
Timestamp:	192.168.2.2395.170.196.18440608802027121 05/14/22-02:20:29.987583
SID:	2027121
Source Port:	40608
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.50.85	
Timestamp:	192.168.2.2395.159.50.8551920802027121 05/14/22-02:20:46.769425
SID:	2027121
Source Port:	51920
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.60.102	
Timestamp:	192.168.2.23172.65.60.10237828555552027153 05/14/22-02:20:51.595839
SID:	2027153
Source Port:	37828
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.245.250.142	
Timestamp:	192.168.2.23172.245.250.14248988555552027153 05/14/22-02:20:55.340538
SID:	2027153
Source Port:	48988

Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.117.110.47	
Timestamp:	192.168.2.2395.117.110.4739132802027121 05/14/22-02:19:54.486284
SID:	2027121
Source Port:	39132
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.100.58	
Timestamp:	192.168.2.23172.65.100.5848116555552027153 05/14/22-02:20:33.576896
SID:	2027153
Source Port:	48116
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.22.203	
Timestamp:	192.168.2.2395.216.22.20338146802027121 05/14/22-02:21:29.004701
SID:	2027121
Source Port:	38146
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.181.244	
Timestamp:	192.168.2.23172.65.181.24432864555552027153 05/14/22-02:20:08.849218
SID:	2027153
Source Port:	32864
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.93.255	
Timestamp:	192.168.2.23172.65.93.25539622555552027153 05/14/22-02:21:27.712648
SID:	2027153
Source Port:	39622
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.205.109.44	
Timestamp:	192.168.2.2395.205.109.4436654802027121 05/14/22-02:20:28.683925
SID:	2027121
Source Port:	36654
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.249.69.126	
Timestamp:	192.168.2.2395.249.69.12654336802027121 05/14/22-02:20:46.647552
SID:	2027121
Source Port:	54336
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.140.157.174	
Timestamp:	192.168.2.2395.140.157.17438300802027121 05/14/22-02:20:58.303872
SID:	2027121
Source Port:	38300
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.211.102.29	
Timestamp:	192.168.2.2395.211.102.2938412802027121 05/14/22-02:20:55.931558
SID:	2027121
Source Port:	38412
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.253.89	
Timestamp:	192.168.2.2395.56.253.8939030802027121 05/14/22-02:20:46.744227
SID:	2027121
Source Port:	39030
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.168.248.174	
Timestamp:	192.168.2.2395.168.248.17436364802027121 05/14/22-02:19:46.145602
SID:	2027121
Source Port:	36364
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.65.73.151	
Timestamp:	192.168.2.2395.65.73.15159576802027121 05/14/22-02:20:37.010160
SID:	2027121
Source Port:	59576
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.155.62	
Timestamp:	192.168.2.23172.65.155.6251970555552027153 05/14/22-02:19:47.505809
SID:	2027153
Source Port:	51970
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.211.70.227	
Timestamp:	192.168.2.23112.211.70.22750280802027121 05/14/22-02:19:53.094256
SID:	2027121
Source Port:	50280
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 98.159.33.50	
Timestamp:	192.168.2.2398.159.33.5059304555552027153 05/14/22-02:20:51.688681
SID:	2027153
Source Port:	59304

Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.74.158

Timestamp:	192.168.2.2395.100.74.15834890802027121 05/14/22-02:21:41.908330
SID:	2027121
Source Port:	34890
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.79.119.172

Timestamp:	192.168.2.2395.79.119.17258308802027121 05/14/22-02:20:02.472815
SID:	2027121
Source Port:	58308
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.179.231.252

Timestamp:	192.168.2.2395.179.231.25254070802027121 05/14/22-02:20:36.835389
SID:	2027121
Source Port:	54070
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.165.141.17

Timestamp:	192.168.2.2395.165.141.1752550802027121 05/14/22-02:20:13.742226
SID:	2027121
Source Port:	52550
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.246.86

Timestamp:	192.168.2.23172.65.246.8633864555552027153 05/14/22-02:20:23.034239
SID:	2027153
Source Port:	33864
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.180.163.75

Timestamp:	192.168.2.2395.180.163.7541450802027121 05/14/22-02:19:46.154023
SID:	2027121
Source Port:	41450
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.140.52

Timestamp:	192.168.2.2395.217.140.5242126802027121 05/14/22-02:21:20.773526
SID:	2027121
Source Port:	42126
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.226.103.188	
Timestamp:	192.168.2.23156.226.103.18840742528692027339 05/14/22-02:20:20.197589
SID:	2027339
Source Port:	40742
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.168.6.119	
Timestamp:	192.168.2.23112.168.6.11954502802027121 05/14/22-02:20:26.062520
SID:	2027121
Source Port:	54502
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.252.1.155	
Timestamp:	192.168.2.2395.252.1.15559942802027121 05/14/22-02:20:52.532968
SID:	2027121
Source Port:	59942
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.175.112.178	
Timestamp:	192.168.2.2395.175.112.17855928802027121 05/14/22-02:20:55.951615
SID:	2027121
Source Port:	55928
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.197.133	
Timestamp:	192.168.2.23172.65.197.13350746555552027153 05/14/22-02:19:52.156166
SID:	2027153
Source Port:	50746
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.226.54.94	
Timestamp:	192.168.2.23156.226.54.94347205286920273 39 05/14/22-02:20:37.007206
SID:	2027339
Source Port:	34720
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.31.137.231	
Timestamp:	192.168.2.2395.31.137.23139652802027121 05/14/22-02:19:58.907121
SID:	2027121
Source Port:	39652
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.68.121	
Timestamp:	192.168.2.23172.65.68.12155652555552027153 05/14/22-02:21:20.746079
SID:	2027153
Source Port:	55652

Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.215.115	
Timestamp:	192.168.2.23172.65.215.11559892555552027153 05/14/22-02:21:25.372980
SID:	2027153
Source Port:	59892
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.20.83	
Timestamp:	192.168.2.2395.217.20.8343432802027121 05/14/22-02:20:35.403881
SID:	2027121
Source Port:	43432
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.213.134.116	
Timestamp:	192.168.2.2395.213.134.11649508802027121 05/14/22-02:20:17.990482
SID:	2027121
Source Port:	49508
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.79.207.121	
Timestamp:	192.168.2.2341.79.207.12158786372152835222 05/14/22-02:19:44.065785
SID:	2835222
Source Port:	58786
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.245.89	
Timestamp:	192.168.2.23172.65.245.8939670555552027153 05/14/22-02:21:23.054578
SID:	2027153
Source Port:	39670
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.173.110.51	
Timestamp:	192.168.2.2395.173.110.5153424802027121 05/14/22-02:20:13.713836
SID:	2027121
Source Port:	53424
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.182.65	
Timestamp:	192.168.2.2395.100.182.6546118802027121 05/14/22-02:20:28.675028
SID:	2027121
Source Port:	46118
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.225.39	
Timestamp:	192.168.2.23172.65.225.3953180555552027153 05/14/22-02:20:49.354114
SID:	2027153
Source Port:	53180
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.213.135.6	
Timestamp:	192.168.2.2395.213.135.654294802027121 05/14/22-02:20:23.671991
SID:	2027121
Source Port:	54294
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.50.66	
Timestamp:	192.168.2.2395.100.50.6657492802027121 05/14/22-02:20:13.699597
SID:	2027121
Source Port:	57492
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.32.133	
Timestamp:	192.168.2.2395.100.32.13358698802027121 05/14/22-02:20:13.688657
SID:	2027121
Source Port:	58698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.223.177	
Timestamp:	192.168.2.23172.65.223.17758740555552027153 05/14/22-02:21:31.972177
SID:	2027153
Source Port:	58740
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.129.32	
Timestamp:	192.168.2.2395.56.129.3258322802027121 05/14/22-02:20:08.154351
SID:	2027121
Source Port:	58322
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.254.36.105	
Timestamp:	192.168.2.23156.254.36.10533430528692027339 05/14/22-02:21:42.664037
SID:	2027339
Source Port:	33430
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.235.159	
Timestamp:	192.168.2.23172.65.235.15937460555552027153 05/14/22-02:21:18.255396
SID:	2027153
Source Port:	37460

Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.130.153.194	−
Timestamp:	192.168.2.2395.130.153.19445406802027121 05/14/22-02:19:46.130154
SID:	2027121
Source Port:	45406
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.81.132.230	−
Timestamp:	192.168.2.23172.81.132.23054932555552027153 05/14/22-02:20:55.243185
SID:	2027153
Source Port:	54932
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.67.139.30	−
Timestamp:	192.168.2.2395.67.139.3048052802027121 05/14/22-02:21:23.021939
SID:	2027121
Source Port:	48052
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.126.215	−
Timestamp:	192.168.2.23172.65.126.21549052555552027153 05/14/22-02:20:55.145531
SID:	2027153
Source Port:	49052
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.215.208.100	−
Timestamp:	192.168.2.2395.215.208.10044116802027121 05/14/22-02:20:11.932503
SID:	2027121
Source Port:	44116
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.161.129.147	−
Timestamp:	192.168.2.2395.161.129.14741284802027121 05/14/22-02:20:28.494539
SID:	2027121
Source Port:	41284
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.154.217.95	−
Timestamp:	192.168.2.2395.154.217.9559972802027121 05/14/22-02:20:47.972023
SID:	2027121
Source Port:	59972
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.49.216.139	
Timestamp:	192.168.2.2395.49.216.13936748802027121 05/14/22-02:19:48.985166
SID:	2027121
Source Port:	36748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.123.178	
Timestamp:	192.168.2.2395.100.123.17840392802027121 05/14/22-02:20:00.008786
SID:	2027121
Source Port:	40392
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.177.159	
Timestamp:	192.168.2.2395.100.177.15936576802027121 05/14/22-02:20:47.978053
SID:	2027121
Source Port:	36576
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.10.65	
Timestamp:	192.168.2.23172.65.10.6541558555552027153 05/14/22-02:19:41.124619
SID:	2027153
Source Port:	41558
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.61.35	
Timestamp:	192.168.2.2395.56.61.3540458802027121 05/14/22-02:20:20.282000
SID:	2027121
Source Port:	40458
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.199.65.70	
Timestamp:	192.168.2.23112.199.65.7034510802027121 05/14/22-02:19:54.462588
SID:	2027121
Source Port:	34510
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.247.3.225	
Timestamp:	192.168.2.23172.247.3.225371045555552027153 05/14/22-02:20:30.363275
SID:	2027153
Source Port:	37104
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.244.73.209	
Timestamp:	192.168.2.23156.244.73.20959122528692027339 05/14/22-02:20:43.778827
SID:	2027339
Source Port:	59122

Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.211.114	
Timestamp:	192.168.2.23172.65.211.11441284555552027153 05/14/22-02:21:29.853420
SID:	2027153
Source Port:	41284
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.22.69	
Timestamp:	192.168.2.2395.56.22.6955278802027121 05/14/22-02:20:26.260830
SID:	2027121
Source Port:	55278
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.168.58.16	
Timestamp:	192.168.2.2395.168.58.1648764802027121 05/14/22-02:20:26.110701
SID:	2027121
Source Port:	48764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.245.211.240	
Timestamp:	192.168.2.23172.245.211.240454585555552027153 05/14/22-02:19:52.139359
SID:	2027153
Source Port:	45458
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.85.25.43	
Timestamp:	192.168.2.2395.85.25.4345908802027121 05/14/22-02:20:13.713545
SID:	2027121
Source Port:	45908
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.103.94.78	
Timestamp:	192.168.2.2395.103.94.7859840802027121 05/14/22-02:21:23.075620
SID:	2027121
Source Port:	59840
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.99.213	
Timestamp:	192.168.2.2395.216.99.21346012802027121 05/14/22-02:20:50.314457
SID:	2027121
Source Port:	46012
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.154.210.138	
Timestamp:	192.168.2.2395.154.210.13841746802027121 05/14/22-02:20:29.923500
SID:	2027121
Source Port:	41746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.166.235	
Timestamp:	192.168.2.23172.65.166.23540510555552027153 05/14/22-02:20:18.663926
SID:	2027153
Source Port:	40510
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.140.152.60	
Timestamp:	192.168.2.2395.140.152.6056948802027121 05/14/22-02:20:58.168915
SID:	2027121
Source Port:	56948
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.218.205	
Timestamp:	192.168.2.23172.65.218.20539286555552027153 05/14/22-02:19:45.210598
SID:	2027153
Source Port:	39286
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.67.254.8	
Timestamp:	192.168.2.2395.67.254.845916802027121 05/14/22-02:20:50.411338
SID:	2027121
Source Port:	45916
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.94.223	
Timestamp:	192.168.2.2395.101.94.22359806802027121 05/14/22-02:20:52.525988
SID:	2027121
Source Port:	59806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.211.117.105	
Timestamp:	192.168.2.2395.211.117.10540092802027121 05/14/22-02:20:17.709606
SID:	2027121
Source Port:	40092
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.236.36	
Timestamp:	192.168.2.23172.65.236.3652408555552027153 05/14/22-02:20:13.316366
SID:	2027153
Source Port:	52408

Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.41.243	
Timestamp:	192.168.2.2395.101.41.24350612802027121 05/14/22-02:20:08.506868
SID:	2027121
Source Port:	50612
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.221.124	
Timestamp:	192.168.2.2395.100.221.12455808802027121 05/14/22-02:20:46.643939
SID:	2027121
Source Port:	55808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.85.3.8	
Timestamp:	192.168.2.2395.85.3.838146802027121 05/14/22-02:20:54.768744
SID:	2027121
Source Port:	38146
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.106.43	
Timestamp:	192.168.2.23172.65.106.4347764555552027153 05/14/22-02:20:49.336809
SID:	2027153
Source Port:	47764
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.126.204	
Timestamp:	192.168.2.23172.65.126.20444174555552027153 05/14/22-02:21:04.074579
SID:	2027153
Source Port:	44174
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.102.111	
Timestamp:	192.168.2.23172.65.102.11154778555552027153 05/14/22-02:20:37.064924
SID:	2027153
Source Port:	54778
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.55.165	
Timestamp:	192.168.2.23172.65.55.16553072555552027153 05/14/22-02:21:10.451979
SID:	2027153
Source Port:	53072
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.238.155	
Timestamp:	192.168.2.23172.65.238.15539812555552027153 05/14/22-02:20:15.584199
SID:	2027153
Source Port:	39812
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.48.204	
Timestamp:	192.168.2.23172.65.48.20460354555552027153 05/14/22-02:21:29.870634
SID:	2027153
Source Port:	60354
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.0.238	
Timestamp:	192.168.2.2395.159.0.23847072802027121 05/14/22-02:19:46.170608
SID:	2027121
Source Port:	47072
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.182.102	
Timestamp:	192.168.2.23172.65.182.10258972555552027153 05/14/22-02:20:51.596070
SID:	2027153
Source Port:	58972
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.58.157.140	
Timestamp:	192.168.2.2395.58.157.14049154802027121 05/14/22-02:20:52.612041
SID:	2027121
Source Port:	49154
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.158.181.247	
Timestamp:	192.168.2.2395.158.181.24746568802027121 05/14/22-02:21:41.997139
SID:	2027121
Source Port:	46568
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.71.29	
Timestamp:	192.168.2.2395.101.71.2948646802027121 05/14/22-02:20:26.090268
SID:	2027121
Source Port:	48646
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.72.11.206	
Timestamp:	192.168.2.23112.72.11.20659084802027121 05/14/22-02:19:47.583781
SID:	2027121
Source Port:	59084

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

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.21.155	
Timestamp:	192.168.2.23172.65.21.15535856555552027153 05/14/22-02:20:51.595566
SID:	2027153
Source Port:	35856
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.150.232	
Timestamp:	192.168.2.23172.65.150.232482465555552027153 05/14/22-02:21:18.255502
SID:	2027153
Source Port:	48246
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.89.187.102	
Timestamp:	192.168.2.2395.89.187.10258358802027121 05/14/22-02:20:17.684228
SID:	2027121
Source Port:	58358
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.179.195.106	
Timestamp:	192.168.2.2395.179.195.10640482802027121 05/14/22-02:20:52.518767
SID:	2027121
Source Port:	40482
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.99.89	
Timestamp:	192.168.2.23172.65.99.8937294555552027153 05/14/22-02:20:49.336736
SID:	2027153
Source Port:	37294
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.23.54	
Timestamp:	192.168.2.2395.159.23.5440212802027121 05/14/22-02:20:36.885865
SID:	2027121
Source Port:	40212
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.214.251.138	
Timestamp:	192.168.2.2395.214.251.13845916802027121 05/14/22-02:20:40.684147
SID:	2027121
Source Port:	45916
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.148.205	
Timestamp:	192.168.2.23172.65.148.20538814555552027153 05/14/22-02:20:57.564197
SID:	2027153
Source Port:	38814
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.189.87	
Timestamp:	192.168.2.23172.65.189.8747034555552027153 05/14/22-02:20:16.017978
SID:	2027153
Source Port:	47034
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.1.208	
Timestamp:	192.168.2.23172.65.1.20842544555552027153 05/14/22-02:20:39.510465
SID:	2027153
Source Port:	42544
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.51.20.50	
Timestamp:	192.168.2.2395.51.20.5055028802027121 05/14/22-02:20:43.929385
SID:	2027121
Source Port:	55028
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.250.69	
Timestamp:	192.168.2.23172.65.250.6935864555552027153 05/14/22-02:20:01.298980
SID:	2027153
Source Port:	35864
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.245.77.59	
Timestamp:	192.168.2.23172.245.77.5953270555552027153 05/14/22-02:19:52.182191
SID:	2027153
Source Port:	53270
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.190.105	
Timestamp:	192.168.2.23172.65.190.10558068555552027153 05/14/22-02:20:18.663728
SID:	2027153
Source Port:	58068
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.99.213	
Timestamp:	192.168.2.2395.216.99.21346096802027121 05/14/22-02:20:52.532593
SID:	2027121
Source Port:	46096

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

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.164.248.243	
Timestamp:	192.168.2.23112.164.248.24352370802027121 05/14/22-02:20:44.164196
SID:	2027121
Source Port:	52370
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.187.118	
Timestamp:	192.168.2.23172.65.187.11833690555552027153 05/14/22-02:21:25.372611
SID:	2027153
Source Port:	33690
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.255.81.249	
Timestamp:	192.168.2.23172.255.81.24951928555552027153 05/14/22-02:20:37.030447
SID:	2027153
Source Port:	51928
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.105.186	
Timestamp:	192.168.2.2395.217.105.18639746802027121 05/14/22-02:20:26.046847
SID:	2027121
Source Port:	39746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.212.135.172	
Timestamp:	192.168.2.2395.212.135.17251110802027121 05/14/22-02:20:32.203168
SID:	2027121
Source Port:	51110
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.77.28	
Timestamp:	192.168.2.2395.56.77.2843922802027121 05/14/22-02:19:52.752680
SID:	2027121
Source Port:	43922
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.88.166.60	
Timestamp:	192.168.2.2395.88.166.6043526802027121 05/14/22-02:20:58.091978
SID:	2027121
Source Port:	43526
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.249.180	
Timestamp:	192.168.2.2395.216.249.18055858802027121 05/14/22-02:19:48.967211
SID:	2027121
Source Port:	55858
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.129.58.148	
Timestamp:	192.168.2.2395.129.58.14840528802027121 05/14/22-02:19:59.897192
SID:	2027121
Source Port:	40528
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.130.41.57	
Timestamp:	192.168.2.2395.130.41.5755030802027121 05/14/22-02:21:39.694247
SID:	2027121
Source Port:	55030
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.247.23.149	
Timestamp:	192.168.2.23156.247.23.14933140528692027339 05/14/22-02:20:04.128716
SID:	2027339
Source Port:	33140
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.145.154	
Timestamp:	192.168.2.2395.216.145.15458058802027121 05/14/22-02:20:43.914921
SID:	2027121
Source Port:	58058
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.174.218.181	
Timestamp:	192.168.2.2395.174.218.18143366802027121 05/14/22-02:20:08.056947
SID:	2027121
Source Port:	43366
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.203.43.205	
Timestamp:	192.168.2.2395.203.43.20546484802027121 05/14/22-02:19:48.978854
SID:	2027121
Source Port:	46484
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.67.207.249	
Timestamp:	192.168.2.2395.67.207.24937450802027121 05/14/22-02:20:13.786820
SID:	2027121
Source Port:	37450

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

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.158.247	
Timestamp:	192.168.2.23172.65.158.24753372555552027153 05/14/22-02:21:29.853164
SID:	2027153
Source Port:	53372
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.174.79	
Timestamp:	192.168.2.23172.65.174.7959670555552027153 05/14/22-02:21:29.853526
SID:	2027153
Source Port:	59670
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.211.168.70	
Timestamp:	192.168.2.23112.211.168.7051170802027121 05/14/22-02:20:44.370088
SID:	2027121
Source Port:	51170
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.183.14.150	
Timestamp:	192.168.2.2395.183.14.15040654802027121 05/14/22-02:20:28.453314
SID:	2027121
Source Port:	40654
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.110.156.28	
Timestamp:	192.168.2.2395.110.156.2850126802027121 05/14/22-02:20:37.002385
SID:	2027121
Source Port:	50126
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.255.123.231	
Timestamp:	192.168.2.2395.255.123.23145990802027121 05/14/22-02:20:58.151438
SID:	2027121
Source Port:	45990
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.218.36	
Timestamp:	192.168.2.2395.216.218.3652794802027121 05/14/22-02:20:36.849112
SID:	2027121
Source Port:	52794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.57.137.44	
Timestamp:	192.168.2.2395.57.137.4435764802027121 05/14/22-02:19:47.603593
SID:	2027121
Source Port:	35764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.237.52	
Timestamp:	192.168.2.2395.217.237.5248506802027121 05/14/22-02:19:59.979384
SID:	2027121
Source Port:	48506
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.143.191	
Timestamp:	192.168.2.23172.65.143.19140842555552027153 05/14/22-02:20:01.315968
SID:	2027153
Source Port:	40842
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.157.119	
Timestamp:	192.168.2.23172.65.157.11938330555552027153 05/14/22-02:21:10.434660
SID:	2027153
Source Port:	38330
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.67.236.104	
Timestamp:	192.168.2.2395.67.236.10434772802027121 05/14/22-02:21:12.051253
SID:	2027121
Source Port:	34772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.130.30	
Timestamp:	192.168.2.23172.65.130.3049426555552027153 05/14/22-02:20:15.584018
SID:	2027153
Source Port:	49426
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.211.77.133	
Timestamp:	192.168.2.2395.211.77.13344586802027121 05/14/22-02:20:11.849716
SID:	2027121
Source Port:	44586
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.113.205	
Timestamp:	192.168.2.2395.100.113.20547404802027121 05/14/22-02:20:58.154043
SID:	2027121
Source Port:	47404

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

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.123.81	
Timestamp:	192.168.2.2395.216.123.8133790802027121 05/14/22-02:20:14.957069
SID:	2027121
Source Port:	33790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.164.215.28	
Timestamp:	192.168.2.2395.164.215.2837200802027121 05/14/22-02:19:59.939204
SID:	2027121
Source Port:	37200
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.156.129	
Timestamp:	192.168.2.23172.65.156.129455145555552027153 05/14/22-02:21:37.096756
SID:	2027153
Source Port:	45514
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.142.35.111	
Timestamp:	192.168.2.2395.142.35.11147804802027121 05/14/22-02:20:20.225240
SID:	2027121
Source Port:	47804
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.128.199	
Timestamp:	192.168.2.2395.56.128.19952794802027121 05/14/22-02:21:25.420858
SID:	2027121
Source Port:	52794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.179.134.154	
Timestamp:	192.168.2.2395.179.134.15433580802027121 05/14/22-02:21:30.293865
SID:	2027121
Source Port:	33580
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.114.235	
Timestamp:	192.168.2.2395.100.114.23559868802027121 05/14/22-02:20:43.921036
SID:	2027121
Source Port:	59868
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.71.190.163	
Timestamp:	192.168.2.2395.71.190.16349970802027121 05/14/22-02:21:09.608021
SID:	2027121
Source Port:	49970
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.56.81.2	
Timestamp:	192.168.2.2395.56.81.233788802027121 05/14/22-02:20:17.887528
SID:	2027121
Source Port:	33788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.179.217.3	
Timestamp:	192.168.2.2395.179.217.343272802027121 05/14/22-02:20:36.987400
SID:	2027121
Source Port:	43272
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.174.24.164	
Timestamp:	192.168.2.2395.174.24.16455000802027121 05/14/22-02:20:54.836620
SID:	2027121
Source Port:	55000
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.60.23	
Timestamp:	192.168.2.2395.159.60.2346124802027121 05/14/22-02:19:49.002413
SID:	2027121
Source Port:	46124
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.123.96.92	
Timestamp:	192.168.2.2395.123.96.9247868802027121 05/14/22-02:21:23.157498
SID:	2027121
Source Port:	47868
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.142.201.73	
Timestamp:	192.168.2.2395.142.201.7333410802027121 05/14/22-02:19:59.919200
SID:	2027121
Source Port:	33410
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.250.21.9	
Timestamp:	192.168.2.23156.250.21.933852528692027339 05/14/22-02:21:37.167899
SID:	2027339
Source Port:	33852

Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.162.42.65	
Timestamp:	192.168.2.23112.162.42.6537238802027121 05/14/22-02:21:05.132195
SID:	2027121
Source Port:	37238
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.65.90.207	
Timestamp:	192.168.2.2395.65.90.20744420802027121 05/14/22-02:19:59.922507
SID:	2027121
Source Port:	44420
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.246.55	
Timestamp:	192.168.2.23172.65.246.5550246555552027153 05/14/22-02:21:07.858957
SID:	2027153
Source Port:	50246
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.153.75	
Timestamp:	192.168.2.23172.65.153.7557824555552027153 05/14/22-02:20:33.577012
SID:	2027153
Source Port:	57824
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.158.35.5	
Timestamp:	192.168.2.2395.158.35.552018802027121 05/14/22-02:21:18.541626
SID:	2027121
Source Port:	52018
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.121.194	
Timestamp:	192.168.2.23172.65.121.1944774855555202715 3 05/14/22-02:21:37.097695
SID:	2027153
Source Port:	47748
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.46.92	
Timestamp:	192.168.2.23172.65.46.9249768555552027153 05/14/22-02:19:50.762314
SID:	2027153
Source Port:	49768
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.183.39.56	
Timestamp:	192.168.2.2395.183.39.5652654802027121 05/14/22-02:20:40.567791
SID:	2027121
Source Port:	52654
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.25.1	
Timestamp:	192.168.2.23172.65.25.133590555552027153 05/14/22-02:20:16.586055
SID:	2027153
Source Port:	33590
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.119.246	
Timestamp:	192.168.2.23172.65.119.24644332555552027153 05/14/22-02:20:53.960011
SID:	2027153
Source Port:	44332
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.254.47.99	
Timestamp:	192.168.2.23156.254.47.9944390528692027339 05/14/22-02:20:39.243330
SID:	2027339
Source Port:	44390
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.159.56.229	
Timestamp:	192.168.2.2395.159.56.22951360802027121 05/14/22-02:21:27.667354
SID:	2027121
Source Port:	51360
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.255.0.229	
Timestamp:	192.168.2.2395.255.0.22943012802027121 05/14/22-02:20:07.917097
SID:	2027121
Source Port:	43012
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.190.251	
Timestamp:	192.168.2.2395.100.190.25152178802027121 05/14/22-02:20:20.214296
SID:	2027121
Source Port:	52178
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.245.10.47	
Timestamp:	192.168.2.23172.245.10.4747618555552027153 05/14/22-02:20:49.434338
SID:	2027153
Source Port:	47618

Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.250.139	
Timestamp:	192.168.2.2395.101.250.13939170802027121 05/14/22-02:20:20.235206
SID:	2027121
Source Port:	39170
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.219.71	
Timestamp:	192.168.2.2395.216.219.7147596802027121 05/14/22-02:20:54.835828
SID:	2027121
Source Port:	47596
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.171.51	
Timestamp:	192.168.2.23172.65.171.5156360555552027153 05/14/22-02:20:01.321931
SID:	2027153
Source Port:	56360
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.175.109	
Timestamp:	192.168.2.2395.101.175.10953748802027121 05/14/22-02:20:50.354166
SID:	2027121
Source Port:	53748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.226.41	
Timestamp:	192.168.2.2395.100.226.4159506802027121 05/14/22-02:20:17.686181
SID:	2027121
Source Port:	59506
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.0.46	
Timestamp:	192.168.2.23172.65.0.4637458555552027153 05/14/22-02:19:47.505878
SID:	2027153
Source Port:	37458
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.67.253	
Timestamp:	192.168.2.23172.65.67.25360136555552027153 05/14/22-02:20:18.646690
SID:	2027153
Source Port:	60136
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.254.111.149	
Timestamp:	192.168.2.23156.254.111.14935796528692027339 05/14/22-02:20:16.671077
SID:	2027339
Source Port:	35796
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.227.197.138	
Timestamp:	192.168.2.2395.227.197.13838594802027121 05/14/22-02:20:54.812324
SID:	2027121
Source Port:	38594
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.226.77.149	
Timestamp:	192.168.2.23156.226.77.14938194528692027339 05/14/22-02:21:01.673878
SID:	2027339
Source Port:	38194
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.107.238.8	
Timestamp:	192.168.2.2395.107.238.842926802027121 05/14/22-02:19:52.672564
SID:	2027121
Source Port:	42926
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.211.116.27	
Timestamp:	192.168.2.2395.211.116.2738146802027121 05/14/22-02:21:00.478796
SID:	2027121
Source Port:	38146
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.197.61.81	
Timestamp:	192.168.2.2395.197.61.8138884802027121 05/14/22-02:19:49.022506
SID:	2027121
Source Port:	38884
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.249.48	
Timestamp:	192.168.2.23172.65.249.4833940555552027153 05/14/22-02:20:51.595958
SID:	2027153
Source Port:	33940
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.135.243	
Timestamp:	192.168.2.2395.217.135.24342834802027121 05/14/22-02:20:55.988944
SID:	2027121
Source Port:	42834

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

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.218.199	
Timestamp:	192.168.2.23172.65.218.19958436555552027153 05/14/22-02:21:00.626814
SID:	2027153
Source Port:	58436
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.255.82.183	
Timestamp:	192.168.2.23172.255.82.18351098555552027153 05/14/22-02:20:05.589101
SID:	2027153
Source Port:	51098
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.119.63	
Timestamp:	192.168.2.2395.100.119.6334312802027121 05/14/22-02:20:14.964785
SID:	2027121
Source Port:	34312
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.125.231	
Timestamp:	192.168.2.2395.100.125.23157540802027121 05/14/22-02:20:07.915542
SID:	2027121
Source Port:	57540
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.159.235	
Timestamp:	192.168.2.2395.101.159.23540704802027121 05/14/22-02:20:08.033202
SID:	2027121
Source Port:	40704
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.140.228.9	
Timestamp:	192.168.2.2395.140.228.956792802027121 05/14/22-02:20:20.211824
SID:	2027121
Source Port:	56792
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.233.120	
Timestamp:	192.168.2.23172.65.233.12042736555552027153 05/14/22-02:20:49.353885
SID:	2027153
Source Port:	42736
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.98.192	
Timestamp:	192.168.2.2395.101.98.19232930802027121 05/14/22-02:20:39.136961
SID:	2027121
Source Port:	32930
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.221.4	
Timestamp:	192.168.2.2395.100.221.435126802027121 05/14/22-02:21:03.799748
SID:	2027121
Source Port:	35126
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.167.25.166	
Timestamp:	192.168.2.2395.167.25.16656372802027121 05/14/22-02:20:17.985650
SID:	2027121
Source Port:	56372
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.244.68.201	
Timestamp:	192.168.2.23156.244.68.20160120528692027339 05/14/22-02:20:47.294814
SID:	2027339
Source Port:	60120
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.60.156.108	
Timestamp:	192.168.2.2395.60.156.10853860802027121 05/14/22-02:21:00.524361
SID:	2027121
Source Port:	53860
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.111.225.144	
Timestamp:	192.168.2.2395.111.225.14434616802027121 05/14/22-02:20:47.933416
SID:	2027121
Source Port:	34616
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.186.95	
Timestamp:	192.168.2.2395.216.186.9556522802027121 05/14/22-02:20:52.533423
SID:	2027121
Source Port:	56522
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.210.63.28	
Timestamp:	192.168.2.2395.210.63.2846488802027121 05/14/22-02:20:55.950179
SID:	2027121
Source Port:	46488

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

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.37.132.190	
Timestamp:	192.168.2.2395.37.132.19058958802027121 05/14/22-02:21:20.792308
SID:	2027121
Source Port:	58958
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.234.78	
Timestamp:	192.168.2.2395.101.234.7854962802027121 05/14/22-02:21:16.191228
SID:	2027121
Source Port:	54962
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.115.180	
Timestamp:	192.168.2.23172.65.115.180554625555552027153 05/14/22-02:20:23.051525
SID:	2027153
Source Port:	55462
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.179.190.178	
Timestamp:	192.168.2.2395.179.190.17858986802027121 05/14/22-02:21:16.214470
SID:	2027121
Source Port:	58986
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.76.255.195	
Timestamp:	192.168.2.2395.76.255.19543592802027121 05/14/22-02:20:08.094888
SID:	2027121
Source Port:	43592
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.134.9	
Timestamp:	192.168.2.23172.65.134.933166555552027153 05/14/22-02:20:29.195623
SID:	2027153
Source Port:	33166
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 112.160.255.79	
Timestamp:	192.168.2.23112.160.255.7934852802027121 05/14/22-02:19:50.372101
SID:	2027121
Source Port:	34852
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.65.94	
Timestamp:	192.168.2.2395.100.65.9453664802027121 05/14/22-02:21:38.570286
SID:	2027121
Source Port:	53664
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.131.48.130	
Timestamp:	192.168.2.2395.131.48.13042684802027121 05/14/22-02:20:11.856209
SID:	2027121
Source Port:	42684
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.85.55.72	
Timestamp:	192.168.2.2395.85.55.7252754802027121 05/14/22-02:19:54.487454
SID:	2027121
Source Port:	52754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.35.160	
Timestamp:	192.168.2.2395.217.35.16059362802027121 05/14/22-02:19:54.503319
SID:	2027121
Source Port:	59362
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.161.204.90	
Timestamp:	192.168.2.2395.161.204.9052190802027121 05/14/22-02:20:44.023393
SID:	2027121
Source Port:	52190
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.182.108.11	
Timestamp:	192.168.2.2395.182.108.1138782802027121 05/14/22-02:20:11.824320
SID:	2027121
Source Port:	38782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 184.175.126.201	
Timestamp:	192.168.2.23184.175.126.20139598555552027153 05/14/22-02:21:07.841944
SID:	2027153
Source Port:	39598
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.181.95	
Timestamp:	192.168.2.2395.217.181.9536450802027121 05/14/22-02:19:59.875020
SID:	2027121
Source Port:	36450

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

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.199.112	
Timestamp:	192.168.2.23172.65.199.11259008555552027153 05/14/22-02:19:56.454379
SID:	2027153
Source Port:	59008
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.193.33	
Timestamp:	192.168.2.23172.65.193.3352616555552027153 05/14/22-02:20:08.849355
SID:	2027153
Source Port:	52616
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.213.235.224	
Timestamp:	192.168.2.2395.213.235.22448522802027121 05/14/22-02:19:54.520285
SID:	2027121
Source Port:	48522
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.110.132.142	
Timestamp:	192.168.2.2395.110.132.14254226802027121 05/14/22-02:20:17.684118
SID:	2027121
Source Port:	54226
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.216.145.72	
Timestamp:	192.168.2.2395.216.145.7241036802027121 05/14/22-02:20:47.995662
SID:	2027121
Source Port:	41036
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.109.2	
Timestamp:	192.168.2.23172.65.109.235052555552027153 05/14/22-02:20:37.065066
SID:	2027153
Source Port:	35052
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.166.198.5	
Timestamp:	192.168.2.2395.166.198.559512802027121 05/14/22-02:21:03.779525
SID:	2027121
Source Port:	59512
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.31.189	
Timestamp:	192.168.2.23172.65.31.18950858555552027153 05/14/22-02:20:49.354007
SID:	2027153
Source Port:	50858
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.241.110.20	
Timestamp:	192.168.2.23156.241.110.2058068528692027339 05/14/22-02:20:03.905573
SID:	2027339
Source Port:	58068
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.200.11	
Timestamp:	192.168.2.23172.65.200.1135036555552027153 05/14/22-02:20:53.942796
SID:	2027153
Source Port:	35036
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.179.4	
Timestamp:	192.168.2.23172.65.179.441482555552027153 05/14/22-02:20:26.128794
SID:	2027153
Source Port:	41482
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.105.191	
Timestamp:	192.168.2.23172.65.105.19149352555552027153 05/14/22-02:20:08.866235
SID:	2027153
Source Port:	49352
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.112.154	
Timestamp:	192.168.2.23172.65.112.15449832555552027153 05/14/22-02:19:47.506025
SID:	2027153
Source Port:	49832
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.238.49.121	
Timestamp:	192.168.2.23156.238.49.121482005286920273339 05/14/22-02:21:15.972363
SID:	2027339
Source Port:	48200
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.128.133.25	
Timestamp:	192.168.2.2395.128.133.2537696802027121 05/14/22-02:20:54.832547
SID:	2027121
Source Port:	37696

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

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.181.228.221	−
Timestamp:	192.168.2.2395.181.228.22134872802027121 05/14/22-02:20:52.551576
SID:	2027121
Source Port:	34872
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.69.121	−
Timestamp:	192.168.2.2395.100.69.12146056802027121 05/14/22-02:20:36.978503
SID:	2027121
Source Port:	46056
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.95.171	−
Timestamp:	192.168.2.2395.100.95.17146834802027121 05/14/22-02:20:29.920129
SID:	2027121
Source Port:	46834
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.100.193.209	−
Timestamp:	192.168.2.2395.100.193.20939220802027121 05/14/22-02:21:34.953417
SID:	2027121
Source Port:	39220
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.241.97.193	−
Timestamp:	192.168.2.23156.241.97.193516085286920273339 05/14/22-02:21:15.948106
SID:	2027339
Source Port:	51608
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.205.43.210	−
Timestamp:	192.168.2.2395.205.43.21034894802027121 05/14/22-02:21:16.310408
SID:	2027121
Source Port:	34894
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.68.89.190	−
Timestamp:	192.168.2.2395.68.89.19059850802027121 05/14/22-02:20:37.007379
SID:	2027121
Source Port:	59850
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.217.110.151

Timestamp:	192.168.2.2395.217.110.15145094802027121 05/14/22-02:20:52.574667
SID:	2027121
Source Port:	45094
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.217.214

Timestamp:	192.168.2.23172.65.217.21441418555552027153 05/14/22-02:21:27.712807
SID:	2027153
Source Port:	41418
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.64.45

Timestamp:	192.168.2.23172.65.64.4550134555552027153 05/14/22-02:21:15.021175
SID:	2027153
Source Port:	50134
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.153.187

Timestamp:	192.168.2.2395.101.153.18759730802027121 05/14/22-02:21:00.437923
SID:	2027121
Source Port:	59730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Malicious sample detected (through community Yara rule)

Sample tries to kill multiple processes (SIGKILL)

Data Obfuscation

Sample is packed with UPX

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

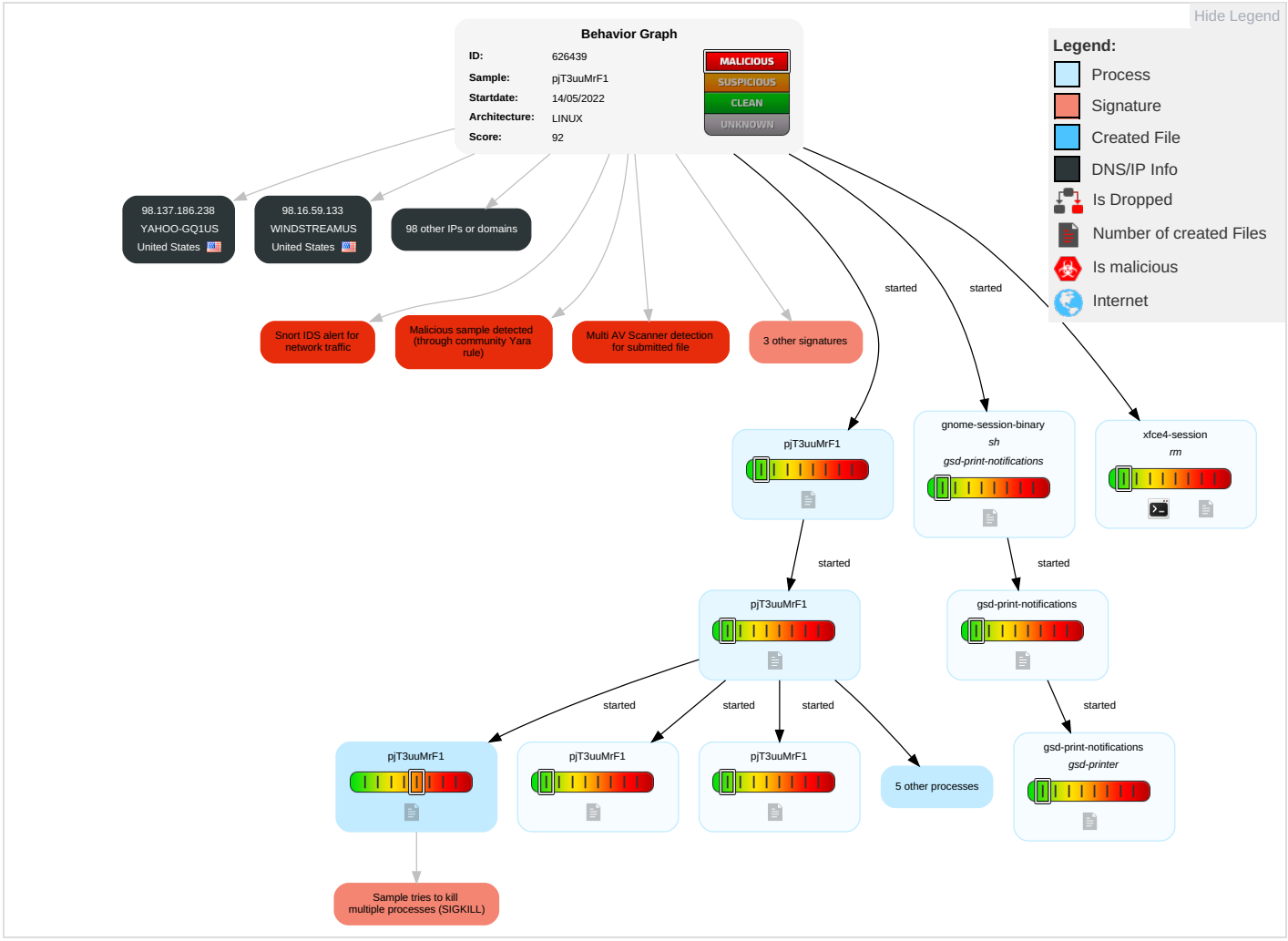
Mitre Att&ck Matrix

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	1 Obfuscated Files or Information	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	1 File Deletion	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	3 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	4 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	3 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

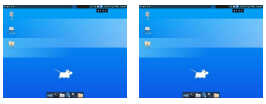
Behavior Graph

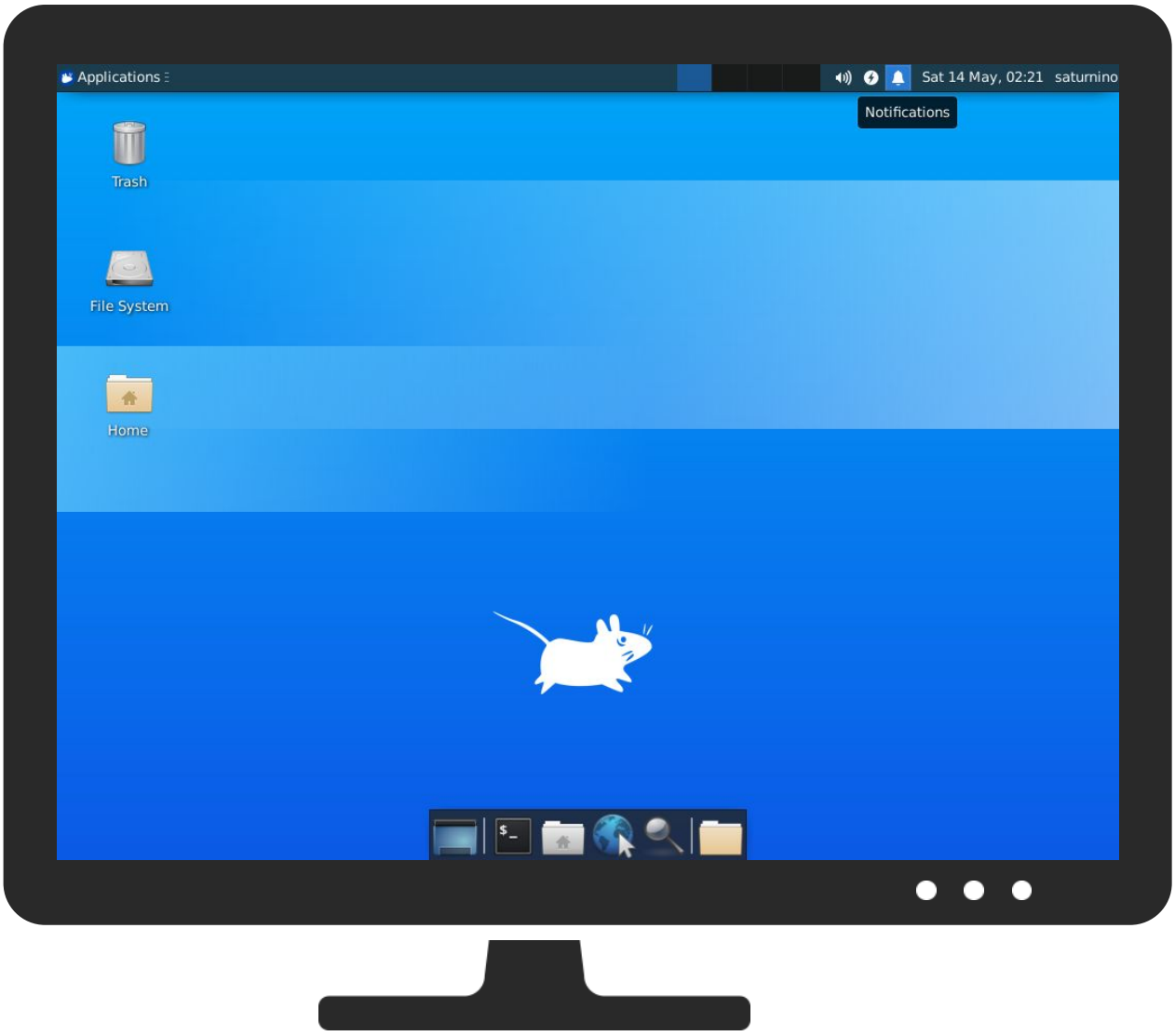


Screenshots

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
pjT3uuMrF1	30%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:80/tmUnblock.cgi	0%	Virustotal		Browse
http://127.0.0.1:80/tmUnblock.cgi	0%	Avira URL Cloud	safe	
http://103.136.43.52/bin	0%	Avira URL Cloud	safe	
http://103.136.43.52/zyxel.sh;	0%	Avira URL Cloud	safe	
http://103.136.43.52/bins/Tsunami.mips;	100%	Avira URL Cloud	malware	
http://103.136.43.52/bins/Tsunami.x86	0%	Avira URL Cloud	safe	
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

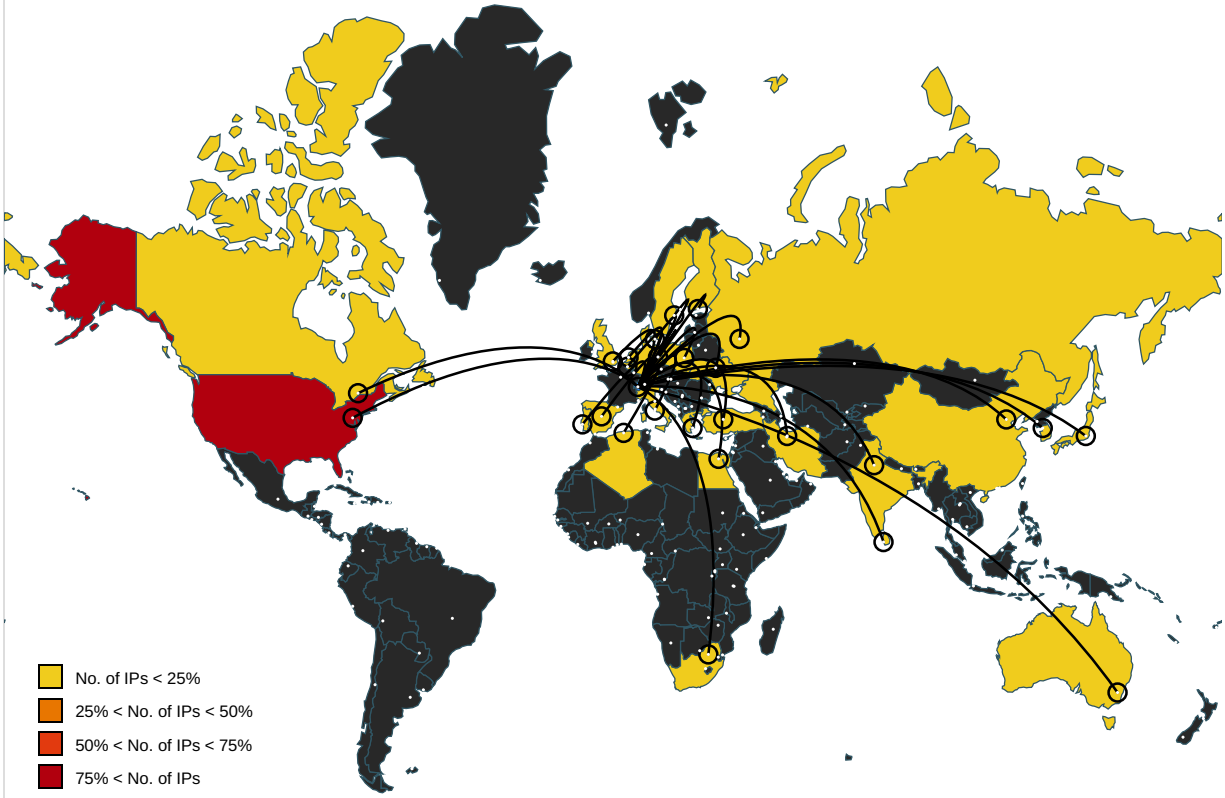
No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/tmUnblock.cgi	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.119.50.247	unknown	United States		20001	TWC-20001-PACWESTUS	false
184.14.83.56	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
95.142.40.179	unknown	Russian Federation		210079	EUROBYTEEurobyteLLCMoscowRussiaRU	false
98.63.246.128	unknown	United States		7922	COMCAST-7922US	false
98.40.24.35	unknown	United States		7922	COMCAST-7922US	false
98.34.189.138	unknown	United States		7922	COMCAST-7922US	false
98.109.42.180	unknown	United States		701	UUNETUS	false
197.231.215.3	unknown	unknown		36974	AFNET-ASCI	false
85.136.26.166	unknown	Spain		12357	COMUNITELSPAINES	false
41.145.255.171	unknown	South Africa		5713	SAIX-NETZA	false
98.26.162.86	unknown	United States		11426	TWC-11426-CAROLINASUS	false
112.4.118.153	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
85.246.119.51	unknown	Portugal		3243	MEO-RESIDENCIALPT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.142.108.15	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
118.243.197.117	unknown	Japan		4685	ASAHI-NETAsahiNetJP	false
112.135.36.69	unknown	Sri Lanka		9329	SLTINT-AS-APSriLankaTelecomInternetLK	false
118.31.117.207	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
94.114.237.14	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
95.19.23.90	unknown	Spain		12479	UNI2-ASES	false
184.37.225.211	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
94.151.70.233	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
62.74.130.50	unknown	Greece		12361	PANAFONET-ASAthensGreeceGR	false
212.53.57.210	unknown	Russian Federation		12335	TARIORU	false
184.43.77.3	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
184.192.180.47	unknown	United States		10507	SPCSUS	false
172.174.11.192	unknown	United States		7018	ATT-INTERNET4US	false
31.138.151.7	unknown	Netherlands		15480	VFNL-ASVodafoneNLAutonomousSystemNL	false
98.212.79.2	unknown	United States		7922	COMCAST-7922US	false
41.122.213.2	unknown	South Africa		16637	MTNNS-ASZA	false
62.152.157.231	unknown	Poland		1902	PAN-NETDeutscheTelekomPan-NetsroSK	false
62.118.118.98	unknown	Russian Federation		8359	MTSRU	false
95.124.218.217	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
31.97.234.255	unknown	United Kingdom		12576	EELtdGB	false
184.196.87.187	unknown	United States		10507	SPCSUS	false
94.227.247.130	unknown	Belgium		6848	TELENET-ASBE	false
172.253.94.196	unknown	United States		15169	GOOGLEUS	false
98.223.166.4	unknown	United States		7922	COMCAST-7922US	false
172.75.35.22	unknown	United States		11426	TWC-11426-CAROLINASUS	false
42.30.91.61	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
94.27.69.153	unknown	Ukraine		12530	GOLDENTELECOM-UKRAINEKyivstarPJSCUA	false
184.111.71.51	unknown	United States		7922	COMCAST-7922US	false
184.250.93.56	unknown	United States		10507	SPCSUS	false
184.14.83.60	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
62.13.69.248	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
94.79.152.6	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
42.43.212.19	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
62.81.143.21	unknown	Spain		6739	ONO-ASCableuropa-ONOES	false
172.98.191.71	unknown	United States		18779	EGIHOSTINGUS	false
85.33.215.229	unknown	Italy		3269	ASN-IBSNAZIT	false
85.150.105.206	unknown	Netherlands		5390	EURONETNL	false
98.34.189.112	unknown	United States		7922	COMCAST-7922US	false
62.69.168.204	unknown	Finland		59766	ASWICITYIT	false
98.224.197.245	unknown	United States		7922	COMCAST-7922US	false
98.10.209.93	unknown	United States		11351	TWC-11351-NORTHEASTUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.195.139.153	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
172.99.210.153	unknown	Reserved		395799	SVBUS	false
197.86.54.147	unknown	South Africa		10474	OPTINETZA	false
85.188.64.232	unknown	Sweden		35445	JKP-SE	false
172.229.225.222	unknown	United States		16625	AKAMAI-ASUS	false
37.147.10.185	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
197.185.6.12	unknown	South Africa		37105	NEOLOGY-ASZA	false
85.246.119.66	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
172.3.178.81	unknown	United States		7018	ATT-INTERNET4US	false
98.53.239.36	unknown	United States		7922	COMCAST-7922US	false
62.74.130.74	unknown	Greece		12361	PANAFONET-ASAthensGreeceGR	false
62.31.100.57	unknown	United Kingdom		5089	NTLGB	false
197.143.201.76	unknown	Algeria		36891	ICOSNET-ASDZ	false
98.153.107.49	unknown	United States		20001	TWC-20001-PACWESTUS	false
184.250.68.89	unknown	United States		10507	SPCSUS	false
184.150.128.217	unknown	Canada		577	BACOMCA	false
172.229.225.217	unknown	United States		16625	AKAMAI-ASUS	false
94.124.54.5	unknown	Italy		47986	PRJINF-ASIT	false
94.39.13.3	unknown	Italy		8612	TISCALI-IT	false
85.225.228.58	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
118.94.183.235	unknown	India		9500	VODAFONE-TRANSIT-ASVodafoneNZLtdNZ	false
172.44.154.205	unknown	United States		21928	T-MOBILE-AS21928US	false
85.173.96.248	unknown	Russian Federation		43132	KBT-ASBranchformerKabbalktelecomRU	false
31.142.125.244	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
98.10.234.39	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
98.98.91.107	unknown	United States		7018	ATT-INTERNET4US	false
98.72.203.158	unknown	United States		7018	ATT-INTERNET4US	false
95.82.243.198	unknown	Russian Federation		12668	MIRALOGIC-ASRU	false
94.76.139.158	unknown	Spain		29119	SERVIHOSTING-ASAireNetworksES	false
172.48.225.102	unknown	United States		21928	T-MOBILE-AS21928US	false
156.197.234.63	unknown	Egypt		8452	TE-ASTE-ASEG	false
172.126.245.202	unknown	United States		7018	ATT-INTERNET4US	false
172.195.251.41	unknown	Australia		18747	IFX18747US	false
197.50.56.102	unknown	Egypt		8452	TE-ASTE-ASEG	false
2.181.161.140	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
118.123.57.166	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
98.137.186.238	unknown	United States		36647	YAHOO-GQ1US	false
98.16.59.133	unknown	United States		7029	WINDSTREAMUS	false
94.78.205.79	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
184.9.231.55	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
178.137.157.52	unknown	Ukraine		15895	KSNET-ASUA	false
184.184.230.139	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
62.83.246.199	unknown	Spain		12430	VODAFONE_ESES	false
98.26.162.47	unknown	United States		11426	TWC-11426-CAROLINASUS	false
98.37.89.113	unknown	United States		7922	COMCAST-7922US	false
184.188.248.219	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.9582958851671375
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	pjT3uuMrF1
File size:	35008
MD5:	e8511d7655b6bb7a2e95a8a71945c87f
SHA1:	0d946d9f597a16bead0e8df270902105fe3662af
SHA256:	156bf5a274c0b19bb4941117a16e7c9be568d70c811199086145df079be80b36
SHA512:	67d8aabd546118f7a8fca53668606bedc7f21f35a106d3c3ee630801747a3755bfc27b065883d0a22b1f549b2c20f26ef348572fb8f24c296e14a78738716251
SSDEEP:	768:Pn9PmZnrFuKv/IT3/a6NoCbbz4Dmg09NqI56lETUS8u9q3UEL3:tiHl6NGD3GNPiETUhTL3
TLSH:	C3F2F2E09746BC7742300EBBE7450D8A27ECCB74D0DAB6171622990CBEEA490DA7524B
File Content Preview:	.ELF.....(.....4.....4. ... (.....u...u.....Z...Z...Z.....Q.td.....OUPX!.....S...S.....^.....?.E.h;....#..$.....:W..'.x.....F..O..]m...`..c..g....>.(...P.K.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0

ELF header	
Entry Point Address:	0xf588
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x8775	0x8775	3.9906	0x5	R E	0x8000		
LOAD	0x5a90	0x25a90	0x25a90	0x0	0x0	0.0000	0x6	RW	0x8000		
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
192.168.2.23172.255.83.100511745555520271530 5/14/22-02:19:57.628001	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51174	55555	192.168.2.23	172.255.83.100
192.168.2.2395.143.204.23852402802027121 05/14/22-02:19:59.979425	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52402	80	192.168.2.23	95.143.204.238
192.168.2.2395.136.115.74501268020271210 5/14/22-02:21:11.764865	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50126	80	192.168.2.23	95.136.115.74
192.168.2.23197.246.194.226535663721528352220 5/14/22-02:21:39.028446	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53566	37215	192.168.2.23	197.246.194.226
192.168.2.23172.65.81.179538445555520271530 5/14/22-02:19:59.137951	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	53844	55555	192.168.2.23	172.65.81.179
192.168.2.23156.234.231.229571165286920273390 5/14/22-02:20:29.429465	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57116	52869	192.168.2.23	156.234.231.229
192.168.2.23172.65.177.8248362555552027153 05/14/22-02:21:10.452251	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48362	55555	192.168.2.23	172.65.177.82
192.168.2.2395.142.64.151336108020271210 5/14/22-02:19:53.342712	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33610	80	192.168.2.23	95.142.64.151
192.168.2.2395.56.139.945957280202712105/14/22-02:21:32.727426	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59572	80	192.168.2.23	95.56.139.94
192.168.2.2395.211.103.152386868020271210 5/14/22-02:19:47.512944	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38686	80	192.168.2.23	95.211.103.152
192.168.2.2395.31.7.6547324802027121 05/14/22-02:20:02.461488	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47324	80	192.168.2.23	95.31.7.65

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.238.125543885555520271535/14/22-02:20:08.992019	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	54388	55555	192.168.2.23	172.65.238.125
192.168.2.2395.189.104.138410188020271215/14/22-02:20:32.218131	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41018	80	192.168.2.23	95.189.104.138
192.168.2.2395.61.121.206449068020271215/14/22-02:20:03.803878	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44906	80	192.168.2.23	95.61.121.206
192.168.2.2395.100.240.226538488020271215/14/22-02:21:23.038728	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53848	80	192.168.2.23	95.100.240.226
192.168.2.23172.65.187.125390845555520271535/14/22-02:20:37.047910	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39084	55555	192.168.2.23	172.65.187.125
192.168.2.2395.216.169.96355268020271215/14/22-02:20:28.438174	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35526	80	192.168.2.23	95.216.169.96
192.168.2.2395.9.211.134458048020271215/14/22-02:20:50.335116	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45804	80	192.168.2.23	95.9.211.134
192.168.2.2395.159.0.203600348020271215/14/22-02:20:28.556099	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60034	80	192.168.2.23	95.159.0.203
192.168.2.2395.159.7.39471808020271215/14/22-02:21:16.327351	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47180	80	192.168.2.23	95.159.7.39
192.168.2.2395.56.29.180360848020271215/14/22-02:20:48.149836	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36084	80	192.168.2.23	95.56.29.180
192.168.2.23172.65.109.124426725555520271535/14/22-02:21:06.678651	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	42672	55555	192.168.2.23	172.65.109.124
192.168.2.23172.65.80.250577925555520271535/14/22-02:19:50.996196	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	57792	55555	192.168.2.23	172.65.80.250
192.168.2.23172.65.203.183400905555520271535/14/22-02:19:57.645189	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40090	55555	192.168.2.23	172.65.203.183
192.168.2.23156.244.124.62547805286920273395/14/22-02:21:19.394819	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54780	52869	192.168.2.23	156.244.124.62
192.168.2.2395.65.111.192381068020271215/14/22-02:20:56.002880	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38106	80	192.168.2.23	95.65.111.192
192.168.2.23156.250.91.131455705286920273395/14/22-02:20:29.395003	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	45570	52869	192.168.2.23	156.250.91.131
192.168.2.2395.159.33.214569268020271215/14/22-02:20:54.820107	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56926	80	192.168.2.23	95.159.33.214
192.168.2.23172.65.234.194374625555520271535/14/22-02:19:47.505957	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37462	55555	192.168.2.23	172.65.234.194
192.168.2.2398.159.33.194495285555520271535/14/22-02:20:13.406392	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49528	55555	192.168.2.23	98.159.33.194

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.216.8.6260662802027121 05/14/22-02:20:26.047138	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60662	80	192.168.2.23	95.216.8.62
192.168.2.2395.100.60.119328148020271 21 05/14/22-02:19:52.635703	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	32814	80	192.168.2.23	95.100.60.119
192.168.2.2395.107.229.3633744802027121 05/14/22-02:21:14.075300	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33744	80	192.168.2.23	95.107.229.36
192.168.2.23172.65.4.7238672255552027153 05/14/22-02:20:18.663856	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	38672	55555	192.168.2.23	172.65.4.72
192.168.2.2395.245.84.157349008020271 21 05/14/22-02:20:23.687567	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34900	80	192.168.2.23	95.245.84.157
192.168.2.2395.101.164.5855826802027121 05/14/22-02:20:39.296946	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55826	80	192.168.2.23	95.101.164.58
192.168.2.2395.215.239.14640644802027121 05/14/22-02:21:03.782018	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40644	80	192.168.2.23	95.215.239.146
192.168.2.2395.179.202.20535652802027121 05/14/22-02:20:29.974289	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35652	80	192.168.2.23	95.179.202.205
192.168.2.2395.65.49.22848088802027121 05/14/22-02:20:28.494212	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48088	80	192.168.2.23	95.65.49.228
192.168.2.23172.65.155.783593855552027153 05/14/22-02:20:03.389982	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35938	55555	192.168.2.23	172.65.155.78
192.168.2.23172.65.28.188375485552027153 05/14/22-02:21:10.434822	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37548	55555	192.168.2.23	172.65.28.188
192.168.2.2395.56.217.14057738802027121 05/14/22-02:20:32.203958	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57738	80	192.168.2.23	95.56.217.140
192.168.2.2395.100.124.21940064802027121 05/14/22-02:21:03.799358	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40064	80	192.168.2.23	95.100.124.219
192.168.2.23112.135.200.3347048802027121 05/14/22-02:20:26.004599	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47048	80	192.168.2.23	112.135.200.33
192.168.2.2395.163.168.10943244802027121 05/14/22-02:20:50.298257	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43244	80	192.168.2.23	95.163.168.109
192.168.2.23172.65.254.2849556555552027153 05/14/22-02:20:53.942992	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49556	55555	192.168.2.23	172.65.254.28
192.168.2.23197.237.77.4548226372152835222 05/14/22-02:21:12.221258	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48226	37215	192.168.2.23	197.237.77.45
192.168.2.2395.28.223.12760158802027121 05/14/22-02:19:54.571832	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60158	80	192.168.2.23	95.28.223.127
192.168.2.23172.65.208.2214718055552027153 05/14/22-02:21:15.003517	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47180	55555	192.168.2.23	172.65.208.221

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.141.209.23753648802027121 05/14/22-02:21:16.255320	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53648	80	192.168.2.23	95.141.209.237
192.168.2.2395.217.173.17642360802027121 05/14/22-02:19:59.979314	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42360	80	192.168.2.23	95.217.173.176
192.168.2.23172.65.254.19839484555552027153 05/14/22-02:19:49.942206	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39484	55555	192.168.2.23	172.65.254.198
192.168.2.2395.217.156.25245090802027121 05/14/22-02:20:55.948104	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45090	80	192.168.2.23	95.217.156.252
192.168.2.23172.65.100.225909255552027153 05/14/22-02:20:55.145336	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59092	55555	192.168.2.23	172.65.100.22
192.168.2.23112.121.177.22134130802027121 05/14/22-02:20:44.359761	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34130	80	192.168.2.23	112.121.177.221
192.168.2.2395.159.51.2953666802027121 05/14/22-02:19:52.694475	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53666	80	192.168.2.23	95.159.51.29
192.168.2.23112.215.101.8160170802027121 05/14/22-02:20:38.895103	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60170	80	192.168.2.23	112.215.101.81
192.168.2.2395.101.22.16334682802027121 05/14/22-02:21:28.995999	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34682	80	192.168.2.23	95.101.22.163
192.168.2.2395.165.133.14534562802027121 05/14/22-02:20:37.016015	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34562	80	192.168.2.23	95.165.133.145
192.168.2.23172.65.220.15233210555552027153 05/14/22-02:19:47.522649	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33210	55555	192.168.2.23	172.65.220.152
192.168.2.23172.65.226.945651055552027153 05/14/22-02:20:26.128722	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56510	55555	192.168.2.23	172.65.226.94
192.168.2.23172.65.98.684689055552027153 05/14/22-02:20:51.595727	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	46890	55555	192.168.2.23	172.65.98.68
192.168.2.2398.159.224.1937196555552027153 05/14/22-02:21:10.525505	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37196	55555	192.168.2.23	98.159.224.19
192.168.2.2395.217.100.9050666802027121 05/14/22-02:20:07.909211	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50666	80	192.168.2.23	95.217.100.90
192.168.2.2395.173.188.1753452802027121 05/14/22-02:21:16.301756	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53452	80	192.168.2.23	95.173.188.17
192.168.2.2395.163.40.13056302802027121 05/14/22-02:20:17.767623	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56302	80	192.168.2.23	95.163.40.130
192.168.2.2395.205.61.159454128020271 21 05/14/22-02:21:23.140530	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45412	80	192.168.2.23	95.205.61.159
192.168.2.2395.217.152.9160996802027121 05/14/22-02:21:29.005358	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60996	80	192.168.2.23	95.217.152.91

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23112.106.58.15039318802027121 05/14/22-02:20:02.405864	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39318	80	192.168.2.23	112.106.58.150
192.168.2.23112.179.60.10652164802027121 05/14/22-02:19:47.485907	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52164	80	192.168.2.23	112.179.60.106
192.168.2.2395.216.14.21637572802027121 05/14/22-02:20:40.548225	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37572	80	192.168.2.23	95.216.14.216
192.168.2.23172.65.70.15634830555552027153 05/14/22-02:21:29.853316	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	34830	55555	192.168.2.23	172.65.70.156
192.168.2.23156.241.119.167513365286920273 39 05/14/22-02:21:38.199643	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	51336	52869	192.168.2.23	156.241.119.167
192.168.2.2395.56.234.11157896802027121 05/14/22-02:20:26.254878	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57896	80	192.168.2.23	95.56.234.111
192.168.2.2395.233.22.20254454802027121 05/14/22-02:19:59.937809	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54454	80	192.168.2.23	95.233.22.202
192.168.2.2395.111.244.25339608802027121 05/14/22-02:20:58.081431	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39608	80	192.168.2.23	95.111.244.253
192.168.2.2395.140.156.4346396802027121 05/14/22-02:20:48.022368	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46396	80	192.168.2.23	95.140.156.43
192.168.2.2395.101.242.10450832802027121 05/14/22-02:19:54.491456	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50832	80	192.168.2.23	95.101.242.104
192.168.2.23172.97.132.13055154555552027153 05/14/22-02:19:45.321580	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	55154	55555	192.168.2.23	172.97.132.130
192.168.2.2395.161.182.236966802027121 05/14/22-02:20:39.165687	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36966	80	192.168.2.23	95.161.182.2
192.168.2.2395.56.223.15134538802027121 05/14/22-02:20:15.032748	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34538	80	192.168.2.23	95.56.223.151
192.168.2.2395.57.74.3350396802027121 05/14/22-02:19:54.640711	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50396	80	192.168.2.23	95.57.74.33
192.168.2.2395.217.215.8660962802027121 05/14/22-02:20:20.205596	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60962	80	192.168.2.23	95.217.215.86
192.168.2.23172.65.5.4944762555552027153 05/14/22-02:20:15.566625	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44762	55555	192.168.2.23	172.65.5.49
192.168.2.2395.217.121.5748134802027121 05/14/22-02:20:47.995507	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48134	80	192.168.2.23	95.217.121.57
192.168.2.23172.65.146.5845536555552027153 05/14/22-02:20:53.942910	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	45536	55555	192.168.2.23	172.65.146.58
192.168.2.2395.159.55.16432974802027121 05/14/22-02:20:28.550766	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	32974	80	192.168.2.23	95.159.55.164

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.152.1955868055552027153 05/14/22-02:21:15.003655	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	58680	55555	192.168.2.23	172.65.152.195
192.168.2.2395.101.50.2936210802027121 05/14/22-02:20:58.196781	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36210	80	192.168.2.23	95.101.50.29
192.168.2.23172.245.84.201559745555552027153 05/14/22-02:20:21.837542	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	55974	55555	192.168.2.23	172.245.84.201
192.168.2.2395.211.3.4758028802027121 05/14/22-02:21:11.754876	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58028	80	192.168.2.23	95.211.3.47
192.168.2.23172.65.46.167736878555552027153 05/14/22-02:20:26.128840	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	36878	55555	192.168.2.23	172.65.46.167
192.168.2.2395.61.121.20644884802027121 05/14/22-02:20:02.452312	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44884	80	192.168.2.23	95.61.121.206
192.168.2.2395.100.32.13358682802027121 05/14/22-02:20:12.238521	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58682	80	192.168.2.23	95.100.32.133
192.168.2.23112.79.32.4242658802027121 05/14/22-02:20:23.608445	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42658	80	192.168.2.23	112.79.32.42
192.168.2.2395.100.123.20540996802027121 05/14/22-02:21:00.525492	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40996	80	192.168.2.23	95.100.123.205
192.168.2.23172.65.255.1134718055552027153 05/14/22-02:19:54.382118	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47180	55555	192.168.2.23	172.65.255.113
192.168.2.2395.214.235.12633216802027121 05/14/22-02:20:07.909063	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33216	80	192.168.2.23	95.214.235.126
192.168.2.23156.224.25.14240106528692027339 05/14/22-02:20:47.247262	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	40106	52869	192.168.2.23	156.224.25.142
192.168.2.2395.87.254.4357278802027121 05/14/22-02:19:53.372300	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57278	80	192.168.2.23	95.87.254.43
192.168.2.2395.131.149.11457714802027121 05/14/22-02:21:34.904086	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57714	80	192.168.2.23	95.131.149.114
192.168.2.2395.217.147.8037940802027121 05/14/22-02:20:37.002920	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37940	80	192.168.2.23	95.217.147.80
192.168.2.2395.101.85.8852956802027121 05/14/22-02:20:58.119066	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52956	80	192.168.2.23	95.101.85.88
192.168.2.23172.65.97.128483836555552027153 05/14/22-02:21:31.954750	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	43836	55555	192.168.2.23	172.65.97.128
192.168.2.2395.143.229.4937410802027121 05/14/22-02:20:47.942900	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37410	80	192.168.2.23	95.143.229.49
192.168.2.23172.65.231.1893613855552027153 05/14/22-02:20:26.126595	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	36138	55555	192.168.2.23	172.65.231.189

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.245.77.5 443396555552027153 05/14/22-02:19:50.861365	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	43396	55555	192.168.2.23	172.245.77.54
192.168.2.2395.101.96.216 34304802027121 05/14/22-02:21:00.513758	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34304	80	192.168.2.23	95.101.96.216
192.168.2.2395.215.170.3 138548802027121 05/14/22-02:20:52.527746	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38548	80	192.168.2.23	95.215.170.31
192.168.2.2395.252.56.12 541832802027121 05/14/22-02:21:34.895934	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41832	80	192.168.2.23	95.252.56.125
192.168.2.2395.58.75.108 47170802027121 05/14/22-02:21:11.847346	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47170	80	192.168.2.23	95.58.75.108
192.168.2.2395.159.30.92 50334802027121 05/14/22-02:21:25.371312	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50334	80	192.168.2.23	95.159.30.92
192.168.2.2395.131.136.6 544472802027121 05/14/22-02:20:26.033464	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44472	80	192.168.2.23	95.131.136.65
192.168.2.2395.142.75.18 149820802027121 05/14/22-02:20:55.954772	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	49820	80	192.168.2.23	95.142.75.181
192.168.2.23156.241.13.9 738248528692027339 05/14/22-02:19:49.315222	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38248	52869	192.168.2.23	156.241.13.97
192.168.2.23172.65.227.1 1452622555552027153 05/14/22-02:21:06.661307	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	52622	55555	192.168.2.23	172.65.227.114
192.168.2.23156.225.159. 18250730528692027339 05/14/22-02:20:25.835892	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	50730	52869	192.168.2.23	156.225.159.182
192.168.2.2395.209.146.2 1050540802027121 05/14/22-02:20:38.689489	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50540	80	192.168.2.23	95.209.146.210
192.168.2.23172.65.163.1 3350650555552027153 05/14/22-02:20:39.493185	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	50650	55555	192.168.2.23	172.65.163.133
192.168.2.2395.213.40.55 6526802027121 05/14/22-02:20:28.445974	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56526	80	192.168.2.23	95.213.40.5
192.168.2.2395.180.165.2 0354376802027121 05/14/22-02:20:29.989309	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54376	80	192.168.2.23	95.180.165.203
192.168.2.2395.166.120.7 254750802027121 05/14/22-02:21:23.057590	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54750	80	192.168.2.23	95.166.120.72
192.168.2.23172.255.80.6 60084555552027153 05/14/22-02:20:08.975191	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60084	55555	192.168.2.23	172.255.80.6
192.168.2.2395.101.238.3 342720802027121 05/14/22-02:20:17.717017	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42720	80	192.168.2.23	95.101.238.33
192.168.2.2395.179.156.2 557406802027121 05/14/22-02:20:02.429434	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57406	80	192.168.2.23	95.179.156.25

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.101.210.22652942802027121 05/14/22-02:20:35.416113	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52942	80	192.168.2.23	95.101.210.226
192.168.2.23112.169.202.100503228020271 21 05/14/22-02:21:05.146467	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50322	80	192.168.2.23	112.169.202.100
192.168.2.2395.213.201.6045874802027121 05/14/22-02:19:52.681868	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45874	80	192.168.2.23	95.213.201.60
192.168.2.23172.255.83.9140446555552027153 05/14/22-02:21:07.857174	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40446	55555	192.168.2.23	172.255.83.91
192.168.2.2395.170.196.18440608802027121 05/14/22-02:20:29.987583	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40608	80	192.168.2.23	95.170.196.184
192.168.2.2395.159.50.8551920802027121 05/14/22-02:20:46.769425	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	51920	80	192.168.2.23	95.159.50.85
192.168.2.23172.65.60.10237828555552027153 05/14/22-02:20:51.595839	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37828	55555	192.168.2.23	172.65.60.102
192.168.2.23172.245.250.14248988555552027153 05/14/22-02:20:55.340538	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48988	55555	192.168.2.23	172.245.250.142
192.168.2.2395.117.110.4739132802027121 05/14/22-02:19:54.486284	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39132	80	192.168.2.23	95.117.110.47
192.168.2.23172.65.100.5848116555552027153 05/14/22-02:20:33.576896	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48116	55555	192.168.2.23	172.65.100.58
192.168.2.2395.216.22.203381468020271 21 05/14/22-02:21:29.004701	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38146	80	192.168.2.23	95.216.22.203
192.168.2.23172.65.181.2443286455555 2027153 05/14/22-02:20:08.849218	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	32864	55555	192.168.2.23	172.65.181.244
192.168.2.23172.65.93.25539622555552027153 05/14/22-02:21:27.712648	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39622	55555	192.168.2.23	172.65.93.255
192.168.2.2395.205.109.4436654802027121 05/14/22-02:20:28.683925	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36654	80	192.168.2.23	95.205.109.44
192.168.2.2395.249.69.126543368020271 21 05/14/22-02:20:46.647552	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54336	80	192.168.2.23	95.249.69.126
192.168.2.2395.140.157.1743830080202712 1 05/14/22-02:20:58.303872	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38300	80	192.168.2.23	95.140.157.174
192.168.2.2395.211.102.2938412802027121 05/14/22-02:20:55.931558	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38412	80	192.168.2.23	95.211.102.29
192.168.2.2395.56.253.8939030802027121 05/14/22-02:20:46.744227	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39030	80	192.168.2.23	95.56.253.89
192.168.2.2395.168.248.1743636480202712 1 05/14/22-02:19:46.145602	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36364	80	192.168.2.23	95.168.248.174

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.65.73.151 59576802027121 05/14/22-02:20:37.010160	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59576	80	192.168.2.23	95.65.73.151
192.168.2.23172.65.155.62 51970555552027153 05/14/22-02:19:47.505809	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51970	55555	192.168.2.23	172.65.155.62
192.168.2.23112.211.70.227 50280802027121 05/14/22-02:19:53.094256	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50280	80	192.168.2.23	112.211.70.227
192.168.2.2398.159.33.50 59304555552027153 05/14/22-02:20:51.688681	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59304	55555	192.168.2.23	98.159.33.50
192.168.2.2395.100.74.158 34890802027121 05/14/22-02:21:41.908330	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34890	80	192.168.2.23	95.100.74.158
192.168.2.2395.79.119.172 58308802027121 05/14/22-02:20:02.472815	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58308	80	192.168.2.23	95.79.119.172
192.168.2.2395.179.231.252 54070802027121 05/14/22-02:20:36.835389	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54070	80	192.168.2.23	95.179.231.252
192.168.2.2395.165.141.17 52550802027121 05/14/22-02:20:13.742226	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52550	80	192.168.2.23	95.165.141.17
192.168.2.23172.65.246.86 33864555552027153 05/14/22-02:20:23.034239	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33864	55555	192.168.2.23	172.65.246.86
192.168.2.2395.180.163.75 41450802027121 05/14/22-02:19:46.154023	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41450	80	192.168.2.23	95.180.163.75
192.168.2.2395.217.140.52 42126802027121 05/14/22-02:21:20.773526	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42126	80	192.168.2.23	95.217.140.52
192.168.2.23156.226.103.188 4074252869202733 9 05/14/22-02:20:20.197589	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	40742	52869	192.168.2.23	156.226.103.188
192.168.2.23112.168.6.119 54502802027121 05/14/22-02:20:26.062520	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54502	80	192.168.2.23	112.168.6.119
192.168.2.2395.252.1.155 59942802027121 05/14/22-02:20:52.532968	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59942	80	192.168.2.23	95.252.1.155
192.168.2.2395.175.112.17 855928802027121 05/14/22-02:20:55.951615	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55928	80	192.168.2.23	95.175.112.178
192.168.2.23172.65.197.133 5074655555202715 3 05/14/22-02:19:52.156166	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	50746	55555	192.168.2.23	172.65.197.133
192.168.2.23156.226.54.94 34720528692027339 05/14/22-02:20:37.007206	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34720	52869	192.168.2.23	156.226.54.94
192.168.2.2395.31.137.23 139652802027121 05/14/22-02:19:58.907121	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39652	80	192.168.2.23	95.31.137.231
192.168.2.23172.65.68.121 55652555552027153 05/14/22-02:21:20.746079	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	55652	55555	192.168.2.23	172.65.68.121

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.215.1155989255552027153 05/14/22-02:21:25.372980	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59892	55555	192.168.2.23	172.65.215.115
192.168.2.2395.217.20.8343432802027121 05/14/22-02:20:35.403881	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43432	80	192.168.2.23	95.217.20.83
192.168.2.2395.213.134.11649508802027121 05/14/22-02:20:17.990482	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	49508	80	192.168.2.23	95.213.134.116
192.168.2.2341.79.207.12158786372152835222 05/14/22-02:19:44.065785	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58786	37215	192.168.2.23	41.79.207.121
192.168.2.23172.65.245.893967055552027153 05/14/22-02:21:23.054578	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39670	55555	192.168.2.23	172.65.245.89
192.168.2.2395.173.110.5153424802027121 05/14/22-02:20:13.713836	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53424	80	192.168.2.23	95.173.110.51
192.168.2.2395.100.182.6546118802027121 05/14/22-02:20:28.675028	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46118	80	192.168.2.23	95.100.182.65
192.168.2.23172.65.225.3953180555552027153 05/14/22-02:20:49.354114	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	53180	55555	192.168.2.23	172.65.225.39
192.168.2.2395.213.135.654294802027121 05/14/22-02:20:23.671991	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54294	80	192.168.2.23	95.213.135.6
192.168.2.2395.100.50.6657492802027121 05/14/22-02:20:13.699597	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57492	80	192.168.2.23	95.100.50.66
192.168.2.2395.100.32.13358698802027121 05/14/22-02:20:13.688657	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58698	80	192.168.2.23	95.100.32.133
192.168.2.23172.65.223.1775874055552027153 05/14/22-02:21:31.972177	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	58740	55555	192.168.2.23	172.65.223.177
192.168.2.2395.56.129.3258322802027121 05/14/22-02:20:08.154351	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58322	80	192.168.2.23	95.56.129.32
192.168.2.23156.254.36.1053343052869027339 05/14/22-02:21:42.664037	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33430	52869	192.168.2.23	156.254.36.105
192.168.2.23172.65.235.1593746055552027153 05/14/22-02:21:18.255396	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37460	55555	192.168.2.23	172.65.235.159
192.168.2.2395.130.153.19445406802027121 05/14/22-02:19:46.130154	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45406	80	192.168.2.23	95.130.153.194
192.168.2.23172.81.132.2305493255552027153 05/14/22-02:20:55.243185	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	54932	55555	192.168.2.23	172.81.132.230
192.168.2.2395.67.139.3048052802027121 05/14/22-02:21:23.021939	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48052	80	192.168.2.23	95.67.139.30
192.168.2.23172.65.126.2154905255552027153 05/14/22-02:20:55.145531	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49052	55555	192.168.2.23	172.65.126.215

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.215.208.10044116802027121 05/14/22-02:20:11.932503	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44116	80	192.168.2.23	95.215.208.100
192.168.2.2395.161.129.14741284802027121 05/14/22-02:20:28.494539	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41284	80	192.168.2.23	95.161.129.147
192.168.2.2395.154.217.9559972802027121 05/14/22-02:20:47.972023	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59972	80	192.168.2.23	95.154.217.95
192.168.2.2395.49.216.13936748802027121 05/14/22-02:19:48.985166	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36748	80	192.168.2.23	95.49.216.139
192.168.2.2395.100.123.17840392802027121 05/14/22-02:20:00.008786	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40392	80	192.168.2.23	95.100.123.178
192.168.2.2395.100.177.15936576802027121 05/14/22-02:20:47.978053	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36576	80	192.168.2.23	95.100.177.159
192.168.2.23172.65.10.654155855555202715 3 05/14/22-02:19:41.124619	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	41558	55555	192.168.2.23	172.65.10.65
192.168.2.2395.56.61.3540458802027121 05/14/22-02:20:20.282000	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40458	80	192.168.2.23	95.56.61.35
192.168.2.23112.199.65.703451080202712 1 05/14/22-02:19:54.462588	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34510	80	192.168.2.23	112.199.65.70
192.168.2.23172.247.3.225370455555202715 3 05/14/22-02:20:30.363275	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37104	55555	192.168.2.23	172.247.3.225
192.168.2.23156.244.73.20959122528692027339 05/14/22-02:20:43.778827	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	59122	52869	192.168.2.23	156.244.73.209
192.168.2.23172.65.211.11441284555552027153 05/14/22-02:21:29.853420	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	41284	55555	192.168.2.23	172.65.211.114
192.168.2.2395.56.22.6955278802027121 05/14/22-02:20:26.260830	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55278	80	192.168.2.23	95.56.22.69
192.168.2.2395.168.58.1648764802027121 05/14/22-02:20:26.110701	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48764	80	192.168.2.23	95.168.58.16
192.168.2.23172.245.211.24045458555552027153 05/14/22-02:19:52.139359	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	45458	55555	192.168.2.23	172.245.211.240
192.168.2.2395.85.25.4345908802027121 05/14/22-02:20:13.713545	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45908	80	192.168.2.23	95.85.25.43
192.168.2.2395.103.94.7859840802027121 05/14/22-02:21:23.075620	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59840	80	192.168.2.23	95.103.94.78
192.168.2.2395.216.99.21346012802027121 05/14/22-02:20:50.314457	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46012	80	192.168.2.23	95.216.99.213
192.168.2.2395.154.210.13841746802027121 05/14/22-02:20:29.923500	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41746	80	192.168.2.23	95.154.210.138

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.166.2354051055552027153 05/14/22-02:20:18.663926	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40510	55555	192.168.2.23	172.65.166.235
192.168.2.2395.140.152.6056948802027121 05/14/22-02:20:58.168915	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56948	80	192.168.2.23	95.140.152.60
192.168.2.23172.65.218.2053928655552027153 05/14/22-02:19:45.210598	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39286	55555	192.168.2.23	172.65.218.205
192.168.2.2395.67.254.845916802027121 05/14/22-02:20:50.411338	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45916	80	192.168.2.23	95.67.254.8
192.168.2.2395.101.94.22359806802027121 05/14/22-02:20:52.525988	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59806	80	192.168.2.23	95.101.94.223
192.168.2.2395.211.117.10540092802027121 05/14/22-02:20:17.709606	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40092	80	192.168.2.23	95.211.117.105
192.168.2.23172.65.236.3652408555552027153 05/14/22-02:20:13.316366	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	52408	55555	192.168.2.23	172.65.236.36
192.168.2.2395.101.41.24350612802027121 05/14/22-02:20:08.506868	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50612	80	192.168.2.23	95.101.41.243
192.168.2.2395.100.221.12455808802027121 05/14/22-02:20:46.643939	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55808	80	192.168.2.23	95.100.221.124
192.168.2.2395.85.3.838146802027121 05/14/22-02:20:54.768744	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38146	80	192.168.2.23	95.85.3.8
192.168.2.23172.65.106.4347764555552027153 05/14/22-02:20:49.336809	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47764	55555	192.168.2.23	172.65.106.43
192.168.2.23172.65.126.2044417455555202715 3 05/14/22-02:21:04.074579	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44174	55555	192.168.2.23	172.65.126.204
192.168.2.23172.65.102.1115477855555202715 3 05/14/22-02:20:37.064924	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	54778	55555	192.168.2.23	172.65.102.111
192.168.2.23172.65.55.16553072555552027153 05/14/22-02:21:10.451979	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	53072	55555	192.168.2.23	172.65.55.165
192.168.2.23172.65.238.1553981255552027153 05/14/22-02:20:15.584199	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39812	55555	192.168.2.23	172.65.238.155
192.168.2.23172.65.48.2046035455552027153 05/14/22-02:21:29.870634	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60354	55555	192.168.2.23	172.65.48.204
192.168.2.2395.159.0.23847072802027121 05/14/22-02:19:46.170608	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47072	80	192.168.2.23	95.159.0.238
192.168.2.23172.65.182.1025897255555202715 3 05/14/22-02:20:51.596070	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	58972	55555	192.168.2.23	172.65.182.102
192.168.2.2395.58.157.14049154802027121 05/14/22-02:20:52.612041	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	49154	80	192.168.2.23	95.58.157.140

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.158.181.24746568802027121 05/14/22-02:21:41.997139	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46568	80	192.168.2.23	95.158.181.247
192.168.2.2395.101.71.2948646802027121 05/14/22-02:20:26.090268	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48646	80	192.168.2.23	95.101.71.29
192.168.2.23112.72.11.20659084802027121 05/14/22-02:19:47.583781	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59084	80	192.168.2.23	112.72.11.206
192.168.2.23172.65.21.15535856555552027153 05/14/22-02:20:51.595566	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35856	55555	192.168.2.23	172.65.21.155
192.168.2.23172.65.150.2324824655552027153 05/14/22-02:21:18.255502	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48246	55555	192.168.2.23	172.65.150.232
192.168.2.2395.89.187.10258358802027121 05/14/22-02:20:17.684228	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58358	80	192.168.2.23	95.89.187.102
192.168.2.2395.179.195.10640482802027121 05/14/22-02:20:52.518767	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40482	80	192.168.2.23	95.179.195.106
192.168.2.23172.65.99.8937294555552027153 05/14/22-02:20:49.336736	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37294	55555	192.168.2.23	172.65.99.89
192.168.2.2395.159.23.5440212802027121 05/14/22-02:20:36.885865	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40212	80	192.168.2.23	95.159.23.54
192.168.2.2395.214.251.13845916802027121 05/14/22-02:20:40.684147	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45916	80	192.168.2.23	95.214.251.138
192.168.2.23172.65.148.2053881455552027153 05/14/22-02:20:57.564197	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	38814	55555	192.168.2.23	172.65.148.205
192.168.2.23172.65.189.874703455552027153 05/14/22-02:20:16.017978	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47034	55555	192.168.2.23	172.65.189.87
192.168.2.23172.65.1.2084254455552027153 05/14/22-02:20:39.510465	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	42544	55555	192.168.2.23	172.65.1.208
192.168.2.2395.51.20.5055028802027121 05/14/22-02:20:43.929385	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55028	80	192.168.2.23	95.51.20.50
192.168.2.23172.65.250.693586455552027153 05/14/22-02:20:01.298980	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35864	55555	192.168.2.23	172.65.250.69
192.168.2.23172.245.77.595327055552027153 05/14/22-02:19:52.182191	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	53270	55555	192.168.2.23	172.245.77.59
192.168.2.23172.65.190.1055806855552027153 05/14/22-02:20:18.663728	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	58068	55555	192.168.2.23	172.65.190.105
192.168.2.2395.216.99.21346096802027121 05/14/22-02:20:52.532593	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46096	80	192.168.2.23	95.216.99.213
192.168.2.23112.164.248.24352370802027121 05/14/22-02:20:44.164196	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52370	80	192.168.2.23	112.164.248.243

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.187.118336905555520271530 5/14/22-02:21:25.372611	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33690	55555	192.168.2.23	172.65.187.118
192.168.2.23172.255.81.249519285555520271530 5/14/22-02:20:37.030447	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51928	55555	192.168.2.23	172.255.81.249
192.168.2.2395.217.105.186397468020271210 5/14/22-02:20:26.046847	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39746	80	192.168.2.23	95.217.105.186
192.168.2.2395.212.135.172511108020271210 5/14/22-02:20:32.203168	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	51110	80	192.168.2.23	95.212.135.172
192.168.2.2395.56.77.2843922802027121 0 5/14/22-02:19:52.752680	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43922	80	192.168.2.23	95.56.77.28
192.168.2.2395.88.166.6043526802027121 0 5/14/22-02:20:58.091978	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43526	80	192.168.2.23	95.88.166.60
192.168.2.2395.216.249.180558588020271210 5/14/22-02:19:48.967211	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55858	80	192.168.2.23	95.216.249.180
192.168.2.2395.129.58.148405288020271210 5/14/22-02:19:59.897192	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40528	80	192.168.2.23	95.129.58.148
192.168.2.2395.130.41.575503080202712 10 5/14/22-02:21:39.694247	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55030	80	192.168.2.23	95.130.41.57
192.168.2.23156.247.23.14933140528692027339 05/14/22-02:20:04.128716	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33140	52869	192.168.2.23	156.247.23.149
192.168.2.2395.216.145.154580588020271210 5/14/22-02:20:43.914921	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58058	80	192.168.2.23	95.216.145.154
192.168.2.2395.174.218.181433668020271210 5/14/22-02:20:08.056947	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43366	80	192.168.2.23	95.174.218.181
192.168.2.2395.203.43.205464848020271210 5/14/22-02:19:48.978854	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46484	80	192.168.2.23	95.203.43.205
192.168.2.2395.67.207.249374508020271210 5/14/22-02:20:13.786820	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37450	80	192.168.2.23	95.67.207.249
192.168.2.23172.65.158.247533725555520271530 5/14/22-02:21:29.853164	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	53372	55555	192.168.2.23	172.65.158.247
192.168.2.23172.65.174.795967055555520271530 5/14/22-02:21:29.853526	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59670	55555	192.168.2.23	172.65.174.79
192.168.2.23112.211.168.70511708020271210 5/14/22-02:20:44.370088	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	51170	80	192.168.2.23	112.211.168.70
192.168.2.2395.183.14.150406548020271210 5/14/22-02:20:28.453314	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40654	80	192.168.2.23	95.183.14.150
192.168.2.2395.110.156.28501268020271210 5/14/22-02:20:37.002385	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50126	80	192.168.2.23	95.110.156.28

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.255.123.23145990802027121 05/14/22-02:20:58.151438	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45990	80	192.168.2.23	95.255.123.231
192.168.2.2395.216.218.3652794802027121 05/14/22-02:20:36.849112	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52794	80	192.168.2.23	95.216.218.36
192.168.2.2395.57.137.4435764802027121 05/14/22-02:19:47.603593	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35764	80	192.168.2.23	95.57.137.44
192.168.2.2395.217.237.5248506802027121 05/14/22-02:19:59.979384	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48506	80	192.168.2.23	95.217.237.52
192.168.2.23172.65.143.1914084255555202715305/14/22-02:20:01.315968	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40842	55555	192.168.2.23	172.65.143.191
192.168.2.23172.65.157.1193833055555202715305/14/22-02:21:10.434660	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	38330	55555	192.168.2.23	172.65.157.119
192.168.2.2395.67.236.10434772802027121 05/14/22-02:21:12.051253	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34772	80	192.168.2.23	95.67.236.104
192.168.2.23172.65.130.3049426555552027153 05/14/22-02:20:15.584018	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49426	55555	192.168.2.23	172.65.130.30
192.168.2.2395.211.77.13344586802027121 05/14/22-02:20:11.849716	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44586	80	192.168.2.23	95.211.77.133
192.168.2.2395.100.113.20547404802027121 05/14/22-02:20:58.154043	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47404	80	192.168.2.23	95.100.113.205
192.168.2.2395.216.123.8133790802027121 05/14/22-02:20:14.957069	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33790	80	192.168.2.23	95.216.123.81
192.168.2.2395.164.215.2837200802027121 05/14/22-02:19:59.939204	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37200	80	192.168.2.23	95.164.215.28
192.168.2.23172.65.156.1294551455552027153 05/14/22-02:21:37.096756	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	45514	55555	192.168.2.23	172.65.156.129
192.168.2.2395.142.35.11147804802027121 05/14/22-02:20:20.225240	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47804	80	192.168.2.23	95.142.35.111
192.168.2.2395.56.128.19952794802027121 05/14/22-02:21:25.420858	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52794	80	192.168.2.23	95.56.128.199
192.168.2.2395.179.134.15433580802027121 05/14/22-02:21:30.293865	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33580	80	192.168.2.23	95.179.134.154
192.168.2.2395.100.114.23559868802027121 05/14/22-02:20:43.921036	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59868	80	192.168.2.23	95.100.114.235
192.168.2.2395.71.190.16349970802027121 05/14/22-02:21:09.608021	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	49970	80	192.168.2.23	95.71.190.163
192.168.2.2395.56.81.233788802027121 05/14/22-02:20:17.887528	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33788	80	192.168.2.23	95.56.81.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.179.217.343272802027121 05/14/22-02:20:36.987400	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43272	80	192.168.2.23	95.179.217.3
192.168.2.2395.174.24.164550008020271210 5/14/22-02:20:54.836620	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55000	80	192.168.2.23	95.174.24.164
192.168.2.2395.159.60.2346124802027121 05/14/22-02:19:49.002413	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46124	80	192.168.2.23	95.159.60.23
192.168.2.2395.123.96.9247868802027121 05/14/22-02:21:23.157498	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47868	80	192.168.2.23	95.123.96.92
192.168.2.2395.142.201.7333410802027121 05/14/22-02:19:59.919200	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33410	80	192.168.2.23	95.142.201.73
192.168.2.23156.250.21.933852528692027339 05/14/22-02:21:37.167899	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33852	52869	192.168.2.23	156.250.21.9
192.168.2.23112.162.42.6537238802027121 05/14/22-02:21:05.132195	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37238	80	192.168.2.23	112.162.42.65
192.168.2.2395.65.90.20744420802027121 05/14/22-02:19:59.922507	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44420	80	192.168.2.23	95.65.90.207
192.168.2.23172.65.246.555024655552027153 05/14/22-02:21:07.858957	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	50246	55555	192.168.2.23	172.65.246.55
192.168.2.23172.65.153.755782455552027153 05/14/22-02:20:33.577012	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	57824	55555	192.168.2.23	172.65.153.75
192.168.2.2395.158.35.552018802027121 05/14/22-02:21:18.541626	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52018	80	192.168.2.23	95.158.35.5
192.168.2.23172.65.121.1944774855552027153 05/14/22-02:21:37.097695	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47748	55555	192.168.2.23	172.65.121.194
192.168.2.23172.65.46.9249768555552027153 05/14/22-02:19:50.762314	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49768	55555	192.168.2.23	172.65.46.92
192.168.2.2395.183.39.5652654802027121 05/14/22-02:20:40.567791	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52654	80	192.168.2.23	95.183.39.56
192.168.2.23172.65.25.133590555552027153 05/14/22-02:20:16.586055	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33590	55555	192.168.2.23	172.65.25.1
192.168.2.23172.65.119.2464433255552027153 05/14/22-02:20:53.960011	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44332	55555	192.168.2.23	172.65.119.246
192.168.2.23156.254.47.994439052869202733 9 05/14/22-02:20:39.243330	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44390	52869	192.168.2.23	156.254.47.99
192.168.2.2395.159.56.22951360802027121 05/14/22-02:21:27.667354	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	51360	80	192.168.2.23	95.159.56.229
192.168.2.2395.255.0.22943012802027121 05/14/22-02:20:07.917097	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43012	80	192.168.2.23	95.255.0.229

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.100.190.25152178802027121 05/14/22-02:20:20.214296	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52178	80	192.168.2.23	95.100.190.251
192.168.2.23172.245.10.4747618555552027153 05/14/22-02:20:49.434338	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47618	55555	192.168.2.23	172.245.10.47
192.168.2.2395.101.250.13939170802027121 05/14/22-02:20:20.235206	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39170	80	192.168.2.23	95.101.250.139
192.168.2.2395.216.219.7147596802027121 05/14/22-02:20:54.835828	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47596	80	192.168.2.23	95.216.219.71
192.168.2.23172.65.171.5156360555552027153 05/14/22-02:20:01.321931	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56360	55555	192.168.2.23	172.65.171.51
192.168.2.2395.101.175.10953748802027121 05/14/22-02:20:50.354166	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53748	80	192.168.2.23	95.101.175.109
192.168.2.2395.100.226.4159506802027121 05/14/22-02:20:17.686181	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59506	80	192.168.2.23	95.100.226.41
192.168.2.23172.65.0.4637458555552027153 05/14/22-02:19:47.505878	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37458	55555	192.168.2.23	172.65.0.46
192.168.2.23172.65.67.25360136555552027153 05/14/22-02:20:18.646690	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60136	55555	192.168.2.23	172.65.67.253
192.168.2.23156.254.111.14935796528692027339 05/14/22-02:20:16.671077	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	35796	52869	192.168.2.23	156.254.111.149
192.168.2.2395.227.197.13838594802027121 05/14/22-02:20:54.812324	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38594	80	192.168.2.23	95.227.197.138
192.168.2.23156.226.77.14938194528692027339 05/14/22-02:21:01.673878	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38194	52869	192.168.2.23	156.226.77.149
192.168.2.2395.107.238.842926802027121 05/14/22-02:19:52.672564	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42926	80	192.168.2.23	95.107.238.8
192.168.2.2395.211.116.2738146802027121 05/14/22-02:21:00.478796	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38146	80	192.168.2.23	95.211.116.27
192.168.2.2395.197.61.8138884802027121 05/14/22-02:19:49.022506	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38884	80	192.168.2.23	95.197.61.81
192.168.2.23172.65.249.4833940555552027153 05/14/22-02:20:51.595958	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33940	55555	192.168.2.23	172.65.249.48
192.168.2.2395.217.135.24342834802027121 05/14/22-02:20:55.988944	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42834	80	192.168.2.23	95.217.135.243
192.168.2.23172.65.218.19958436555552027153 05/14/22-02:21:00.626814	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	58436	55555	192.168.2.23	172.65.218.199
192.168.2.23172.255.82.1835109855555552027153 05/14/22-02:20:05.589101	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51098	55555	192.168.2.23	172.255.82.183

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.100.119.6334312802027121 05/14/22-02:20:14.964785	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34312	80	192.168.2.23	95.100.119.63
192.168.2.2395.100.125.23157540802027121 05/14/22-02:20:07.915542	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57540	80	192.168.2.23	95.100.125.231
192.168.2.2395.101.159.23540704802027121 05/14/22-02:20:08.033202	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40704	80	192.168.2.23	95.101.159.235
192.168.2.2395.140.228.956792802027121 05/14/22-02:20:20.211824	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56792	80	192.168.2.23	95.140.228.9
192.168.2.23172.65.233.120427365555552027153 05/14/22-02:20:49.353885	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	42736	55555	192.168.2.23	172.65.233.120
192.168.2.2395.101.98.19232930802027121 05/14/22-02:20:39.136961	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	32930	80	192.168.2.23	95.101.98.192
192.168.2.2395.100.221.435126802027121 05/14/22-02:21:03.799748	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35126	80	192.168.2.23	95.100.221.4
192.168.2.2395.167.25.16656372802027121 05/14/22-02:20:17.985650	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56372	80	192.168.2.23	95.167.25.166
192.168.2.23156.244.68.20160120528692027339 05/14/22-02:20:47.294814	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	60120	52869	192.168.2.23	156.244.68.201
192.168.2.2395.60.156.10853860802027121 05/14/22-02:21:00.524361	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53860	80	192.168.2.23	95.60.156.108
192.168.2.2395.111.225.14434616802027121 05/14/22-02:20:47.933416	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34616	80	192.168.2.23	95.111.225.144
192.168.2.2395.216.186.9556522802027121 05/14/22-02:20:52.533423	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56522	80	192.168.2.23	95.216.186.95
192.168.2.2395.210.63.2846488802027121 05/14/22-02:20:55.950179	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46488	80	192.168.2.23	95.210.63.28
192.168.2.2395.37.132.19058958802027121 05/14/22-02:21:20.792308	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58958	80	192.168.2.23	95.37.132.190
192.168.2.2395.101.234.785496802027121 05/14/22-02:21:16.191228	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54962	80	192.168.2.23	95.101.234.78
192.168.2.23172.65.115.18055462555552027153 05/14/22-02:20:23.051525	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	55462	55555	192.168.2.23	172.65.115.180
192.168.2.2395.179.190.17858986802027121 05/14/22-02:21:16.214470	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58986	80	192.168.2.23	95.179.190.178
192.168.2.2395.76.255.19543592802027121 05/14/22-02:20:08.094888	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43592	80	192.168.2.23	95.76.255.195
192.168.2.23172.65.134.933166555552027153 05/14/22-02:20:29.195623	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33166	55555	192.168.2.23	172.65.134.9

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23112.160.255.7934852802027121 05/14/22-02:19:50.372101	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34852	80	192.168.2.23	112.160.255.79
192.168.2.2395.100.65.9453664802027121 05/14/22-02:21:38.570286	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53664	80	192.168.2.23	95.100.65.94
192.168.2.2395.131.48.13042684802027121 05/14/22-02:20:11.856209	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42684	80	192.168.2.23	95.131.48.130
192.168.2.2395.85.55.7252754802027121 05/14/22-02:19:54.487454	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52754	80	192.168.2.23	95.85.55.72
192.168.2.2395.217.35.16059362802027121 05/14/22-02:19:54.503319	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59362	80	192.168.2.23	95.217.35.160
192.168.2.2395.161.204.9052190802027121 05/14/22-02:20:44.023393	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52190	80	192.168.2.23	95.161.204.90
192.168.2.2395.182.108.1138782802027121 05/14/22-02:20:11.824320	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38782	80	192.168.2.23	95.182.108.11
192.168.2.23184.175.126.20139598555552027153 05/14/22-02:21:07.841944	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39598	55555	192.168.2.23	184.175.126.201
192.168.2.2395.217.181.9536450802027121 05/14/22-02:19:59.875020	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36450	80	192.168.2.23	95.217.181.95
192.168.2.23172.65.199.1125900855555552027153 05/14/22-02:19:56.454379	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59008	55555	192.168.2.23	172.65.199.112
192.168.2.23172.65.193.335261655555552027153 05/14/22-02:20:08.849355	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	52616	55555	192.168.2.23	172.65.193.33
192.168.2.2395.213.235.22448522802027121 05/14/22-02:19:54.520285	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48522	80	192.168.2.23	95.213.235.224
192.168.2.2395.110.132.14254226802027121 05/14/22-02:20:17.684118	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54226	80	192.168.2.23	95.110.132.142
192.168.2.2395.216.145.7241036802027121 05/14/22-02:20:47.995662	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41036	80	192.168.2.23	95.216.145.72
192.168.2.23172.65.109.235052555552027153 05/14/22-02:20:37.065066	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35052	55555	192.168.2.23	172.65.109.2
192.168.2.2395.166.198.559512802027121 05/14/22-02:21:03.779525	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59512	80	192.168.2.23	95.166.198.5
192.168.2.23172.65.31.18950858555552027153 05/14/22-02:20:49.354007	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	50858	55555	192.168.2.23	172.65.31.189
192.168.2.23156.241.110.2058068528692027339 05/14/22-02:20:03.905573	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58068	52869	192.168.2.23	156.241.110.20
192.168.2.23172.65.200.1135036555552027153 05/14/22-02:20:53.942796	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35036	55555	192.168.2.23	172.65.200.11

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.179.44148255555202715305/14/22-02:20:26.128794	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	41482	55555	192.168.2.23	172.65.179.4
192.168.2.23172.65.105.19149352555552027153 05/14/22-02:20:08.866235	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49352	55555	192.168.2.23	172.65.105.191
192.168.2.23172.65.112.15449832555552027153 05/14/22-02:19:47.506025	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49832	55555	192.168.2.23	172.65.112.154
192.168.2.23156.238.49.121482005286920273390 5/14/22-02:21:15.972363	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48200	52869	192.168.2.23	156.238.49.121
192.168.2.2395.128.133.25376968020271210 5/14/22-02:20:54.832547	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37696	80	192.168.2.23	95.128.133.25
192.168.2.2395.181.228.221348728020271210 5/14/22-02:20:52.551576	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34872	80	192.168.2.23	95.181.228.221
192.168.2.2395.100.69.121460568020271210 5/14/22-02:20:36.978503	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46056	80	192.168.2.23	95.100.69.121
192.168.2.2395.100.95.171468348020271210 5/14/22-02:20:29.920129	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46834	80	192.168.2.23	95.100.95.171
192.168.2.2395.100.193.209392208020271210 5/14/22-02:21:34.953417	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39220	80	192.168.2.23	95.100.193.209
192.168.2.23156.241.97.193516085286920273390 5/14/22-02:21:15.948106	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	51608	52869	192.168.2.23	156.241.97.193
192.168.2.2395.205.43.210348948020271210 5/14/22-02:21:16.310408	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34894	80	192.168.2.23	95.205.43.210
192.168.2.2395.68.89.19059850802027121 05/14/22-02:20:37.007379	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59850	80	192.168.2.23	95.68.89.190
192.168.2.2395.217.110.151450948020271210 5/14/22-02:20:52.574667	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45094	80	192.168.2.23	95.217.110.151
192.168.2.23172.65.217.21441418555552027153 05/14/22-02:21:27.712807	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	41418	55555	192.168.2.23	172.65.217.214
192.168.2.23172.65.64.455013455555202715305/14/22-02:21:15.021175	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	50134	55555	192.168.2.23	172.65.64.45
192.168.2.2395.101.153.187597308020271210 5/14/22-02:21:00.437923	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59730	80	192.168.2.23	95.101.153.187

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:80
- 192.168.0.14:80

System Behavior

Analysis Process: pjT3uuMrF1 PID: **6230**, Parent PID: **6125**

General

Start time:	02:19:38
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	/tmp/pjT3uuMrF1
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: pjT3uuMrF1 PID: **6232**, Parent PID: **6230**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: pjT3uuMrF1 PID: **6234**, Parent PID: **6232**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: pjT3uuMrF1 PID: **6235**, Parent PID: **6232**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: pjT3uuMrF1 PID: **6238**, Parent PID: **6232**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: pjT3uuMrF1 PID: **6239**, Parent PID: **6232**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: pjT3uuMrF1 PID: **6243**, Parent PID: **6232**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: pjT3uuMrF1 PID: **6245**, Parent PID: **6232**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: pjT3uuMrF1 PID: **6247**, Parent PID: **6232**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: pjT3uuMrF1 PID: **6248**, Parent PID: **6232**

General

Start time:	02:19:39
Start date:	14/05/2022
Path:	/tmp/pjT3uuMrF1
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-binary PID: **6287**, Parent PID: **1477**

General

Start time:	02:20:56
Start date:	14/05/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6287**, Parent PID: **1477**

General

Start time:	02:20:56
Start date:	14/05/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-print-notifications PID: **6287**, Parent PID: **1477**

General

Start time:	02:20:56
Start date:	14/05/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	/usr/libexec/gsd-print-notifications
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

File Activities

File Read

Analysis Process: gsd-print-notifications PID: **6295**, Parent PID: **6287**

General

Start time:	02:20:57
Start date:	14/05/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: **6296**, Parent PID: **6295**

General

Start time:	02:20:57
Start date:	14/05/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

File Activities

Directory Enumerated

Analysis Process: gsd-printer PID: **6296**, Parent PID: **1**

General

Start time:	02:20:57
Start date:	14/05/2022
Path:	/usr/libexec/gsd-printer
Arguments:	/usr/libexec/gsd-printer
File size:	31120 bytes
MD5 hash:	7995828cf98c315fd55f2ffb3b22384d

File Activities

File Read

Analysis Process: xfce4-session PID: **6317**, Parent PID: **1900**

General

Start time:	02:21:29
Start date:	14/05/2022
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: rm PID: **6317**, Parent PID: **1900**

General

Start time:	02:21:29
Start date:	14/05/2022
Path:	/usr/bin/rm
Arguments:	rm -f /home/saturnino/.cache/sessions/Thunar-2ec9153f1-6fa0-4067-96b1-e5fe875b1e51
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read