

ID: 626433
Sample Name: VC3SWrkssz
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:03:07
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report VC3SWrkssz 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
General Information 4
Warnings 4
Runtime Messages 4
Process Tree 5
Yara Signatures 5
Initial Sample 5
Memory Dumps 5
Snort Signatures 6
Joe Sandbox Signatures 49
AV Detection 49
Networking 49
System Summary 49
Data Obfuscation 49
Hooking and other Techniques for Hiding and Protection 49
Stealing of Sensitive Information 49
Remote Access Functionality 49
Mitre Att&ck Matrix 49
Malware Configuration 50
Behavior Graph 50
Screenshots 51
Thumbnails 51
Antivirus, Machine Learning and Genetic Malware Detection 52
Initial Sample 52
Dropped Files 52
Domains 52
URLs 52
Domains and IPs 53
Contacted Domains 53
Contacted URLs 53
URLs from Memory and Binaries 53
World Map of Contacted IPs 53
Public IPs 53
Joe Sandbox View / Context 55
IPs 55
Domains 55
ASNs 56
JA3 Fingerprints 56
Dropped Files 56
Created / dropped Files 56
Static File Info 56
General 56
Static ELF Info 56
ELF header 56
Program Segments 57
Network Behavior 57
Snort IDS Alerts 57
Network Port Distribution 74
TCP Packets 74
HTTP Request Dependency Graph 74
System Behavior 74
Analysis Process: VC3SWrkssz PID: 6223, Parent PID: 6121 74
General 74
File Activities 74
File Read 74
Analysis Process: VC3SWrkssz PID: 6226, Parent PID: 6223 74
General 74
Analysis Process: VC3SWrkssz PID: 6228, Parent PID: 6226 75
General 75
Analysis Process: VC3SWrkssz PID: 6229, Parent PID: 6226 75
General 75
Analysis Process: VC3SWrkssz PID: 6231, Parent PID: 6226 75
General 75
Analysis Process: VC3SWrkssz PID: 6232, Parent PID: 6226 75
General 75
Analysis Process: VC3SWrkssz PID: 6235, Parent PID: 6226 75
General 75
Analysis Process: VC3SWrkssz PID: 6236, Parent PID: 6226 75

Copyright Joe Security LLC 2022

General 75
Analysis Process: VC3SWrkssz PID: 6239, Parent PID: 6226 76
General 76
Analysis Process: VC3SWrkssz PID: 6241, Parent PID: 6226 76
General 76
File Activities 76
File Read 76
Directory Enumerated 76
Analysis Process: gnome-session-binary PID: 6281, Parent PID: 1477 76
General 76
Analysis Process: sh PID: 6281, Parent PID: 1477 76
General 76
File Activities 76
File Read 76
Analysis Process: gsd-print-notifications PID: 6281, Parent PID: 1477 76
General 76
File Activities 77
File Read 77
Analysis Process: gsd-print-notifications PID: 6287, Parent PID: 6281 77
General 77
Analysis Process: gsd-print-notifications PID: 6288, Parent PID: 6287 77
General 77
File Activities 77
Directory Enumerated 77
Analysis Process: gsd-printer PID: 6288, Parent PID: 1 77
General 77
File Activities 77
File Read 77
Analysis Process: xfce4-session PID: 6311, Parent PID: 1900 77
General 77
Analysis Process: rm PID: 6311, Parent PID: 1900 77
General 77
File Activities 78
File Deleted 78
File Read 78

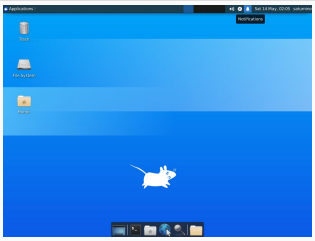
Linux Analysis Report

VC3SWrkssz

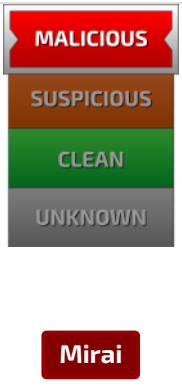
Overview

General Information

Sample Name:	VC3SWrkssz
Analysis ID:	626433
MD5:	981e959599e29b.
SHA1:	258686ffea44f41..
SHA256:	dc80f285f9f5077..
Tags:	32 elf mips mirai
Infos:	



Detection



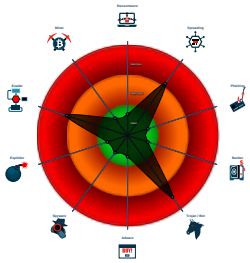
Mirai

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:	626433
Start date and time: 14/05/202202:03:07	2022-05-14 02:03:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VC3SWrkssz
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/VC3SWrkssz
PID:	6223
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	kebabware installed

Copyright Joe Security LLC 2022

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- VC3SWrkssz (PID: 6223, Parent: 6121, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/VC3SWrkssz
  - VC3SWrkssz New Fork (PID: 6226, Parent: 6223)
    - VC3SWrkssz New Fork (PID: 6228, Parent: 6226)
    - VC3SWrkssz New Fork (PID: 6229, Parent: 6226)
    - VC3SWrkssz New Fork (PID: 6231, Parent: 6226)
    - VC3SWrkssz New Fork (PID: 6232, Parent: 6226)
    - VC3SWrkssz New Fork (PID: 6235, Parent: 6226)
    - VC3SWrkssz New Fork (PID: 6236, Parent: 6226)
    - VC3SWrkssz New Fork (PID: 6239, Parent: 6226)
    - VC3SWrkssz New Fork (PID: 6241, Parent: 6226)
- gnome-session-binary New Fork (PID: 6281, Parent: 1477)
  - sh (PID: 6281, 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: 6281, Parent: 1477, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6287, Parent: 6281)
      - gsd-print-notifications New Fork (PID: 6288, Parent: 6287)
        - gsd-printer (PID: 6288, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- xfce4-session New Fork (PID: 6311, Parent: 1900)
  - rm (PID: 6311, 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
VC3SWrkssz	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x85d0:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x863f:$s2: $Id: UPX • 0x85f0:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
6228.1.000000008254e41a.0000000043337d44.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:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
6223.1.000000008254e41a.0000000043337d44.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x14f0:$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
6223.1.0000000051b72c78.000000009a6fa781.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	• 0x21d60:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6 \xAD\xB3 • 0x21dbc:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6 \xAD\xB3 • 0x21e58:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6 \xAD\xB3
6223.1.0000000051b72c78.000000009a6fa781.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x20fe0:$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
6223.1.0000000051b72c78.000000009a6fa781.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: 172.65.225.198

Timestamp:	192.168.2.23172.65.225.19835486555552027153 05/14/22-02:04:11.637927
SID:	2027153
Source Port:	35486
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: 156.245.55.125

Timestamp:	192.168.2.23156.245.55.12540780528692027339 05/14/22-02:05:10.063522
SID:	2027339
Source Port:	40780
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: 88.221.247.46

Timestamp:	192.168.2.2388.221.247.4656298802027121 05/14/22-02:05:16.496663
SID:	2027121
Source Port:	56298
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: 172.65.64.98

Timestamp:	192.168.2.23172.65.64.9842844555552027153 05/14/22-02:05:20.995117
SID:	2027153
Source Port:	42844
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: 172.65.48.26

Timestamp:	192.168.2.23172.65.48.26459065555552027153 05/14/22-02:05:54.037647
SID:	2027153
Source Port:	45906
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.218.156.214	
Timestamp:	192.168.2.2388.218.156.21445324802027121 05/14/22-02:05:04.368184
SID:	2027121
Source Port:	45324
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: 172.65.123.78	
Timestamp:	192.168.2.23172.65.123.7840044555552027153 05/14/22-02:04:34.703644
SID:	2027153
Source Port:	40044
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: 95.209.159.210	
Timestamp:	192.168.2.2395.209.159.21034302802027121 05/14/22-02:04:45.560206
SID:	2027121
Source Port:	34302
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: 156.226.79.26	
Timestamp:	192.168.2.23156.226.79.2647988528692027339 05/14/22-02:04:47.625880
SID:	2027339
Source Port:	47988
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: 88.100.202.197	
Timestamp:	192.168.2.2388.100.202.19760688802027121 05/14/22-02:04:17.306136
SID:	2027121
Source Port:	60688
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: 95.94.67.15	
Timestamp:	192.168.2.2395.94.67.1535236802027121 05/14/22-02:04:02.248726
SID:	2027121
Source Port:	35236
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: 88.198.233.197	
Timestamp:	192.168.2.2388.198.233.19751822802027121 05/14/22-02:04:21.714018
SID:	2027121
Source Port:	51822
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: 88.160.72.151	
Timestamp:	192.168.2.2388.160.72.15148858802027121 05/14/22-02:04:55.282834
SID:	2027121
Source Port:	48858

Copyright Joe Security LLC 2022

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: 172.65.175.160	
Timestamp:	192.168.2.23172.65.175.16044936555552027153 05/14/22-02:05:43.540529
SID:	2027153
Source Port:	44936
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: 172.65.246.67	
Timestamp:	192.168.2.23172.65.246.6760502555552027153 05/14/22-02:05:45.978345
SID:	2027153
Source Port:	60502
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: 172.65.245.156	
Timestamp:	192.168.2.23172.65.245.15651872555552027153 05/14/22-02:04:27.970733
SID:	2027153
Source Port:	51872
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: 88.221.43.153	
Timestamp:	192.168.2.2388.221.43.15360046802027121 05/14/22-02:04:49.296960
SID:	2027121
Source Port:	60046
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: 172.65.40.184	
Timestamp:	192.168.2.23172.65.40.18455754555552027153 05/14/22-02:04:34.721447
SID:	2027153
Source Port:	55754
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: 95.170.142.91	
Timestamp:	192.168.2.2395.170.142.9154540802027121 05/14/22-02:05:16.526766
SID:	2027121
Source Port:	54540
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: 172.65.243.174	
Timestamp:	192.168.2.23172.65.243.17456044555552027153 05/14/22-02:05:43.557862
SID:	2027153
Source Port:	56044
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.83.120.54	
Timestamp:	192.168.2.2388.83.120.5454084802027121 05/14/22-02:04:55.111233
SID:	2027121
Source Port:	54084
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: 156.254.55.121	
Timestamp:	192.168.2.23156.254.55.12150998528692027339 05/14/22-02:04:39.323189
SID:	2027339
Source Port:	50998
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: 172.65.247.44	
Timestamp:	192.168.2.23172.65.247.4456996555552027153 05/14/22-02:04:27.965299
SID:	2027153
Source Port:	56996
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: 88.12.181.235	
Timestamp:	192.168.2.2388.12.181.23545164802027121 05/14/22-02:05:06.625031
SID:	2027121
Source Port:	45164
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: 172.65.66.149	
Timestamp:	192.168.2.23172.65.66.14948008555552027153 05/14/22-02:05:09.761803
SID:	2027153
Source Port:	48008
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: 172.65.35.55	
Timestamp:	192.168.2.23172.65.35.5552384555552027153 05/14/22-02:05:54.037779
SID:	2027153
Source Port:	52384
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: 156.238.52.233	
Timestamp:	192.168.2.23156.238.52.233443165286920273339 05/14/22-02:04:03.540343
SID:	2027339
Source Port:	44316
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: 95.101.124.7	
Timestamp:	192.168.2.2395.101.124.744862802027121 05/14/22-02:04:07.843399
SID:	2027121
Source Port:	44862

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: 88.151.120.239	−
Timestamp:	192.168.2.2388.151.120.23954210802027121 05/14/22-02:04:04.413192
SID:	2027121
Source Port:	54210
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: 197.234.59.176	−
Timestamp:	192.168.2.23197.234.59.176401983721528352222 05/14/22-02:04:48.680620
SID:	2835222
Source Port:	40198
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: 88.221.227.223	−
Timestamp:	192.168.2.2388.221.227.22344588802027121 05/14/22-02:04:55.265828
SID:	2027121
Source Port:	44588
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: 172.65.176.123	−
Timestamp:	192.168.2.23172.65.176.12349208555552027153 05/14/22-02:04:01.919544
SID:	2027153
Source Port:	49208
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: 88.116.145.172	−
Timestamp:	192.168.2.2388.116.145.17253718802027121 05/14/22-02:04:19.393127
SID:	2027121
Source Port:	53718
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: 95.188.114.161	−
Timestamp:	192.168.2.2395.188.114.16159740802027121 05/14/22-02:03:57.828010
SID:	2027121
Source Port:	59740
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: 172.65.210.80	−
Timestamp:	192.168.2.23172.65.210.8052764555552027153 05/14/22-02:04:07.308990
SID:	2027153
Source Port:	52764
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.130.227.219	
Timestamp:	192.168.2.2395.130.227.21954724802027121 05/14/22-02:04:09.253114
SID:	2027121
Source Port:	54724
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: 95.73.184.98	
Timestamp:	192.168.2.2395.73.184.9855062802027121 05/14/22-02:05:00.755463
SID:	2027121
Source Port:	55062
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: 156.245.46.107	
Timestamp:	192.168.2.23156.245.46.10746162528692027339 05/14/22-02:04:51.923330
SID:	2027339
Source Port:	46162
Destination Port:	52869
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: 156.247.21.129	
Timestamp:	192.168.2.23156.247.21.12942964528692027339 05/14/22-02:05:32.842628
SID:	2027339
Source Port:	42964
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: 95.166.126.94	
Timestamp:	192.168.2.2395.166.126.9450592802027121 05/14/22-02:04:25.514613
SID:	2027121
Source Port:	50592
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: 95.217.139.189	
Timestamp:	192.168.2.2395.217.139.18940702802027121 05/14/22-02:04:23.234556
SID:	2027121
Source Port:	40702
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: 172.245.58.78	
Timestamp:	192.168.2.23172.245.58.7852418555552027153 05/14/22-02:05:24.859914
SID:	2027153
Source Port:	52418
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: 172.65.244.246	
Timestamp:	192.168.2.23172.65.244.24633926555552027153 05/14/22-02:04:52.963336
SID:	2027153
Source Port:	33926

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: 172.65.167.212	−
Timestamp:	192.168.2.23172.65.167.21250504555552027153 05/14/22-02:05:46.355886
SID:	2027153
Source Port:	50504
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: 95.34.6.150	−
Timestamp:	192.168.2.2395.34.6.15055186802027121 05/14/22-02:04:11.024463
SID:	2027121
Source Port:	55186
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: 95.100.227.126	−
Timestamp:	192.168.2.2395.100.227.12641560802027121 05/14/22-02:04:19.423556
SID:	2027121
Source Port:	41560
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: 88.150.188.185	−
Timestamp:	192.168.2.2388.150.188.18546066802027121 05/14/22-02:05:22.993162
SID:	2027121
Source Port:	46066
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: 172.65.44.25	−
Timestamp:	192.168.2.23172.65.44.2540066555552027153 05/14/22-02:03:55.485637
SID:	2027153
Source Port:	40066
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: 95.216.50.138	−
Timestamp:	192.168.2.2395.216.50.13837606802027121 05/14/22-02:04:01.004807
SID:	2027121
Source Port:	37606
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: 95.211.210.93	−
Timestamp:	192.168.2.2395.211.210.9335332802027121 05/14/22-02:04:40.769456
SID:	2027121
Source Port:	35332
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.41.92	
Timestamp:	192.168.2.23172.65.41.9237008555552027153 05/14/22-02:04:22.454733
SID:	2027153
Source Port:	37008
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: 88.221.247.20	
Timestamp:	192.168.2.2388.221.247.2036634802027121 05/14/22-02:04:41.120142
SID:	2027121
Source Port:	36634
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: 172.65.207.224	
Timestamp:	192.168.2.23172.65.207.22452754555552027153 05/14/22-02:04:46.156570
SID:	2027153
Source Port:	52754
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: 156.230.24.148	
Timestamp:	192.168.2.23156.230.24.14839870528692027339 05/14/22-02:04:37.094159
SID:	2027339
Source Port:	39870
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: 88.208.209.13	
Timestamp:	192.168.2.2388.208.209.1350344802027121 05/14/22-02:04:13.122146
SID:	2027121
Source Port:	50344
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: 95.100.228.240	
Timestamp:	192.168.2.2395.100.228.24052510802027121 05/14/22-02:04:11.012752
SID:	2027121
Source Port:	52510
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: 88.221.99.59	
Timestamp:	192.168.2.2388.221.99.5954200802027121 05/14/22-02:04:04.419952
SID:	2027121
Source Port:	54200
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: 172.65.86.63	
Timestamp:	192.168.2.23172.65.86.6346324555552027153 05/14/22-02:03:58.555530
SID:	2027153
Source Port:	46324

Copyright Joe Security LLC 2022

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: 172.65.253.163

Timestamp:	192.168.2.23172.65.253.16356128555552027153 05/14/22-02:04:24.881877
SID:	2027153
Source Port:	56128
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: 95.59.181.200

Timestamp:	192.168.2.2395.59.181.20043136802027121 05/14/22-02:05:19.833635
SID:	2027121
Source Port:	43136
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: 95.100.207.121

Timestamp:	192.168.2.2395.100.207.12150102802027121 05/14/22-02:04:21.836564
SID:	2027121
Source Port:	50102
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: 156.241.14.132

Timestamp:	192.168.2.23156.241.14.132546725286920273339 05/14/22-02:04:16.821957
SID:	2027339
Source Port:	54672
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: 95.158.153.184

Timestamp:	192.168.2.2395.158.153.18444468802027121 05/14/22-02:05:16.432488
SID:	2027121
Source Port:	44468
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: 172.65.241.236

Timestamp:	192.168.2.23172.65.241.23657156555552027153 05/14/22-02:04:39.318465
SID:	2027153
Source Port:	57156
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: 156.226.94.189

Timestamp:	192.168.2.23156.226.94.18941406528692027339 05/14/22-02:05:39.652328
SID:	2027339
Source Port:	41406
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.129.188.92	
Timestamp:	192.168.2.2388.129.188.9241166802027121 05/14/22-02:04:19.399830
SID:	2027121
Source Port:	41166
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: 172.65.166.22	
Timestamp:	192.168.2.23172.65.166.2240758555552027153 05/14/22-02:05:46.355727
SID:	2027153
Source Port:	40758
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: 95.183.38.118	
Timestamp:	192.168.2.2395.183.38.11852836802027121 05/14/22-02:04:50.334131
SID:	2027121
Source Port:	52836
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: 88.135.148.195	
Timestamp:	192.168.2.2388.135.148.19540620802027121 05/14/22-02:04:55.124093
SID:	2027121
Source Port:	40620
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: 172.65.75.62	
Timestamp:	192.168.2.23172.65.75.6257084555552027153 05/14/22-02:05:34.766951
SID:	2027153
Source Port:	57084
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: 172.65.204.101	
Timestamp:	192.168.2.23172.65.204.10138326555552027153 05/14/22-02:04:43.912984
SID:	2027153
Source Port:	38326
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: 95.180.140.24	
Timestamp:	192.168.2.2395.180.140.2447310802027121 05/14/22-02:04:36.685245
SID:	2027121
Source Port:	47310
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: 88.195.2.157	
Timestamp:	192.168.2.2388.195.2.15755260802027121 05/14/22-02:04:04.435272
SID:	2027121
Source Port:	55260

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: 88.151.120.239	
Timestamp:	192.168.2.2388.151.120.23954354802027121 05/14/22-02:04:10.940346
SID:	2027121
Source Port:	54354
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: 172.65.67.90	
Timestamp:	192.168.2.23172.65.67.9056662555552027153 05/14/22-02:04:56.047288
SID:	2027153
Source Port:	56662
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: 172.65.102.51	
Timestamp:	192.168.2.23172.65.102.5144754555552027153 05/14/22-02:04:56.030167
SID:	2027153
Source Port:	44754
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: 95.128.74.80	
Timestamp:	192.168.2.2395.128.74.8046640802027121 05/14/22-02:04:17.251115
SID:	2027121
Source Port:	46640
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: 172.65.164.17	
Timestamp:	192.168.2.23172.65.164.1748162555552027153 05/14/22-02:04:22.472015
SID:	2027153
Source Port:	48162
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: 88.83.121.221	
Timestamp:	192.168.2.2388.83.121.22158894802027121 05/14/22-02:04:27.640751
SID:	2027121
Source Port:	58894
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: 95.169.219.254	
Timestamp:	192.168.2.2395.169.219.25434272802027121 05/14/22-02:04:45.846183
SID:	2027121
Source Port:	34272
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: 184.105.8.37	
Timestamp:	192.168.2.23184.105.8.3736406555552027153 05/14/22-02:05:18.793782
SID:	2027153
Source Port:	36406
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: 95.215.97.139	
Timestamp:	192.168.2.2395.215.97.13935584802027121 05/14/22-02:04:25.532039
SID:	2027121
Source Port:	35584
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: 156.224.15.170	
Timestamp:	192.168.2.23156.224.15.17039200528692027339 05/14/22-02:04:39.797114
SID:	2027339
Source Port:	39200
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: 95.213.15.31	
Timestamp:	192.168.2.2395.213.15.3151808802027121 05/14/22-02:04:17.286891
SID:	2027121
Source Port:	51808
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: 88.218.95.110	
Timestamp:	192.168.2.2388.218.95.11037924802027121 05/14/22-02:05:28.503764
SID:	2027121
Source Port:	37924
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: 95.252.227.99	
Timestamp:	192.168.2.2395.252.227.9960514802027121 05/14/22-02:04:57.392496
SID:	2027121
Source Port:	60514
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: 172.65.167.14	
Timestamp:	192.168.2.23172.65.167.1439002555552027153 05/14/22-02:05:09.758951
SID:	2027153
Source Port:	39002
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: 88.209.80.208	
Timestamp:	192.168.2.2388.209.80.20855570802027121 05/14/22-02:03:55.571475
SID:	2027121
Source Port:	55570

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: 172.245.196.210	
Timestamp:	192.168.2.23172.245.196.21055214555552027153 05/14/22-02:05:06.317529
SID:	2027153
Source Port:	55214
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: 156.244.77.144	
Timestamp:	192.168.2.23156.244.77.144437465286920273339 05/14/22-02:05:07.644328
SID:	2027339
Source Port:	43746
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: 95.56.137.155	
Timestamp:	192.168.2.2395.56.137.15542484802027121 05/14/22-02:04:07.907810
SID:	2027121
Source Port:	42484
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: 156.252.26.142	
Timestamp:	192.168.2.23156.252.26.142589985286920273339 05/14/22-02:04:30.267679
SID:	2027339
Source Port:	58998
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: 172.65.228.156	
Timestamp:	192.168.2.23172.65.228.15633432555552027153 05/14/22-02:05:45.978228
SID:	2027153
Source Port:	33432
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: 95.211.109.39	
Timestamp:	192.168.2.2395.211.109.3948768802027121 05/14/22-02:04:57.363312
SID:	2027121
Source Port:	48768
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: 88.215.16.244	
Timestamp:	192.168.2.2388.215.16.24440964802027121 05/14/22-02:05:36.611945
SID:	2027121
Source Port:	40964
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.250.175.208	
Timestamp:	192.168.2.2388.250.175.20859942802027121 05/14/22-02:05:33.036125
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: 88.221.176.214	
Timestamp:	192.168.2.2388.221.176.21437726802027121 05/14/22-02:05:02.940383
SID:	2027121
Source Port:	37726
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: 156.254.51.133	
Timestamp:	192.168.2.23156.254.51.13348970528692027339 05/14/22-02:05:53.246860
SID:	2027339
Source Port:	48970
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: 95.181.217.215	
Timestamp:	192.168.2.2395.181.217.21542428802027121 05/14/22-02:04:01.013042
SID:	2027121
Source Port:	42428
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: 172.65.149.227	
Timestamp:	192.168.2.23172.65.149.22744978555552027153 05/14/22-02:03:55.468539
SID:	2027153
Source Port:	44978
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: 95.100.151.50	
Timestamp:	192.168.2.2395.100.151.5036050802027121 05/14/22-02:05:04.113713
SID:	2027121
Source Port:	36050
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: 156.226.51.26	
Timestamp:	192.168.2.23156.226.51.26597565286920273 39 05/14/22-02:03:58.608037
SID:	2027339
Source Port:	59756
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: 95.44.136.168	
Timestamp:	192.168.2.2395.44.136.16858910802027121 05/14/22-02:05:06.494711
SID:	2027121
Source Port:	58910

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: 156.245.43.18	−
Timestamp:	192.168.2.23156.245.43.1833638528692027339 05/14/22-02:04:34.638673
SID:	2027339
Source Port:	33638
Destination Port:	52869
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: 156.250.92.81	−
Timestamp:	192.168.2.23156.250.92.8149400528692027339 05/14/22-02:05:30.387325
SID:	2027339
Source Port:	49400
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: 95.101.122.129	−
Timestamp:	192.168.2.2395.101.122.12941910802027121 05/14/22-02:03:57.733650
SID:	2027121
Source Port:	41910
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: 88.198.82.136	−
Timestamp:	192.168.2.2388.198.82.13638664802027121 05/14/22-02:04:36.621117
SID:	2027121
Source Port:	38664
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: 88.207.159.18	−
Timestamp:	192.168.2.2388.207.159.1842422802027121 05/14/22-02:04:04.430182
SID:	2027121
Source Port:	42422
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: 95.56.213.80	−
Timestamp:	192.168.2.2395.56.213.8036770802027121 05/14/22-02:04:50.593818
SID:	2027121
Source Port:	36770
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: 95.159.14.92	−
Timestamp:	192.168.2.2395.159.14.9236796802027121 05/14/22-02:04:01.047400
SID:	2027121
Source Port:	36796
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.101.58.59	
Timestamp:	192.168.2.2395.101.58.5948210802027121 05/14/22-02:05:00.726341
SID:	2027121
Source Port:	48210
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: 172.65.45.60	
Timestamp:	192.168.2.23172.65.45.6035894555552027153 05/14/22-02:04:31.062264
SID:	2027153
Source Port:	35894
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: 95.72.28.184	
Timestamp:	192.168.2.2395.72.28.18446380802027121 05/14/22-02:03:57.766923
SID:	2027121
Source Port:	46380
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: 172.65.174.20	
Timestamp:	192.168.2.23172.65.174.2055300555552027153 05/14/22-02:03:58.555577
SID:	2027153
Source Port:	55300
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: 172.65.2.221	
Timestamp:	192.168.2.23172.65.2.22159362555552027153 05/14/22-02:05:09.758996
SID:	2027153
Source Port:	59362
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: 88.151.120.239	
Timestamp:	192.168.2.2388.151.120.23954256802027121 05/14/22-02:04:07.815463
SID:	2027121
Source Port:	54256
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: 88.221.155.49	
Timestamp:	192.168.2.2388.221.155.4942002802027121 05/14/22-02:05:52.526130
SID:	2027121
Source Port:	42002
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: 184.175.126.56	
Timestamp:	192.168.2.23184.175.126.56517945555552027153 05/14/22-02:05:04.444249
SID:	2027153
Source Port:	51794

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: 172.65.85.56	
Timestamp:	192.168.2.23172.65.85.5640568555552027153 05/14/22-02:04:07.291997
SID:	2027153
Source Port:	40568
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: 88.221.137.238	
Timestamp:	192.168.2.2388.221.137.23833006802027121 05/14/22-02:05:25.192641
SID:	2027121
Source Port:	33006
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: 95.101.69.250	
Timestamp:	192.168.2.2395.101.69.25058292802027121 05/14/22-02:04:01.004594
SID:	2027121
Source Port:	58292
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: 95.101.188.60	
Timestamp:	192.168.2.2395.101.188.6034116802027121 05/14/22-02:04:04.484302
SID:	2027121
Source Port:	34116
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: 88.166.227.133	
Timestamp:	192.168.2.2388.166.227.13336224802027121 05/14/22-02:04:43.350949
SID:	2027121
Source Port:	36224
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: 88.147.126.189	
Timestamp:	192.168.2.2388.147.126.18944674802027121 05/14/22-02:04:45.457773
SID:	2027121
Source Port:	44674
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: 172.65.33.108	
Timestamp:	192.168.2.23172.65.33.10843492555552027153 05/14/22-02:03:58.572506
SID:	2027153
Source Port:	43492
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.201.64.5	
Timestamp:	192.168.2.2388.201.64.538342802027121 05/14/22-02:04:52.868346
SID:	2027121
Source Port:	38342
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: 88.150.171.72	
Timestamp:	192.168.2.2388.150.171.7244640802027121 05/14/22-02:04:09.313085
SID:	2027121
Source Port:	44640
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: 88.99.170.45	
Timestamp:	192.168.2.2388.99.170.4533644802027121 05/14/22-02:04:40.769297
SID:	2027121
Source Port:	33644
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: 95.101.63.88	
Timestamp:	192.168.2.2395.101.63.8838726802027121 05/14/22-02:04:36.682429
SID:	2027121
Source Port:	38726
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: 156.226.106.224	
Timestamp:	192.168.2.23156.226.106.22449930528692027339 05/14/22-02:03:58.604415
SID:	2027339
Source Port:	49930
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: 95.216.51.242	
Timestamp:	192.168.2.2395.216.51.24245628802027121 05/14/22-02:04:17.265531
SID:	2027121
Source Port:	45628
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: 172.65.200.192	
Timestamp:	192.168.2.23172.65.200.19256740555552027153 05/14/22-02:05:46.356024
SID:	2027153
Source Port:	56740
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: 95.87.1.22	
Timestamp:	192.168.2.2395.87.1.2257834802027121 05/14/22-02:04:34.518726
SID:	2027121
Source Port:	57834

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: 88.99.138.240	−
Timestamp:	192.168.2.2388.99.138.24053168802027121 05/14/22-02:04:43.357808
SID:	2027121
Source Port:	53168
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: 172.65.97.115	−
Timestamp:	192.168.2.23172.65.97.11534182555552027153 05/14/22-02:04:19.382917
SID:	2027153
Source Port:	34182
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: 172.65.167.110	−
Timestamp:	192.168.2.23172.65.167.11059028555552027153 05/14/22-02:04:34.685648
SID:	2027153
Source Port:	59028
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: 88.221.227.180	−
Timestamp:	192.168.2.2388.221.227.18053630802027121 05/14/22-02:05:50.047627
SID:	2027121
Source Port:	53630
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: 88.10.175.42	−
Timestamp:	192.168.2.2388.10.175.4242760802027121 05/14/22-02:04:36.714857
SID:	2027121
Source Port:	42760
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: 88.99.214.46	−
Timestamp:	192.168.2.2388.99.214.4635952802027121 05/14/22-02:04:52.770205
SID:	2027121
Source Port:	35952
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: 172.65.211.64	−
Timestamp:	192.168.2.23172.65.211.6450236555552027153 05/14/22-02:05:06.237219
SID:	2027153
Source Port:	50236
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 95.96.2.18	
Timestamp:	192.168.2.2395.96.2.1854422802027121 05/14/22-02:05:45.528566
SID:	2027121
Source Port:	54422
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: 95.216.140.243	
Timestamp:	192.168.2.2395.216.140.24358592802027121 05/14/22-02:04:55.066889
SID:	2027121
Source Port:	58592
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: 88.41.60.18	
Timestamp:	192.168.2.2388.41.60.1836672802027121 05/14/22-02:04:40.877472
SID:	2027121
Source Port:	36672
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: 156.244.102.115	
Timestamp:	192.168.2.23156.244.102.11538702528692027339 05/14/22-02:05:52.813667
SID:	2027339
Source Port:	38702
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: 172.65.95.33	
Timestamp:	192.168.2.23172.65.95.3339672555552027153 05/14/22-02:04:04.184416
SID:	2027153
Source Port:	39672
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: 95.180.146.93	
Timestamp:	192.168.2.2395.180.146.9351564802027121 05/14/22-02:04:34.515139
SID:	2027121
Source Port:	51564
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: 172.65.124.30	
Timestamp:	192.168.2.23172.65.124.3056878555552027153 05/14/22-02:04:39.300441
SID:	2027153
Source Port:	56878
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: 95.52.241.27	
Timestamp:	192.168.2.2395.52.241.2750394802027121 05/14/22-02:04:01.045396
SID:	2027121
Source Port:	50394

Copyright Joe Security LLC 2022

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: 156.244.73.248

Timestamp:	192.168.2.23156.244.73.24855328528692027339 05/14/22-02:05:36.552777
SID:	2027339
Source Port:	55328
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: 88.221.185.192

Timestamp:	192.168.2.2388.221.185.19260438802027121 05/14/22-02:04:43.365152
SID:	2027121
Source Port:	60438
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: 172.65.182.94

Timestamp:	192.168.2.23172.65.182.94464545555552027153 05/14/22-02:05:33.583579
SID:	2027153
Source Port:	46454
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: 172.65.91.115

Timestamp:	192.168.2.23172.65.91.11560806555552027153 05/14/22-02:05:37.001586
SID:	2027153
Source Port:	60806
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: 172.65.57.85

Timestamp:	192.168.2.23172.65.57.8539362555552027153 05/14/22-02:05:41.244138
SID:	2027153
Source Port:	39362
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: 88.87.90.248

Timestamp:	192.168.2.2388.87.90.24859292802027121 05/14/22-02:04:40.936768
SID:	2027121
Source Port:	59292
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: 98.159.33.227

Timestamp:	192.168.2.2398.159.33.22754498555552027153 05/14/22-02:05:24.949664
SID:	2027153
Source Port:	54498
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: 88.221.190.76	
Timestamp:	192.168.2.2388.221.190.7657518802027121 05/14/22-02:04:43.334647
SID:	2027121
Source Port:	57518
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: 172.65.111.104	
Timestamp:	192.168.2.23172.65.111.10460754555552027153 05/14/22-02:05:30.411524
SID:	2027153
Source Port:	60754
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: 95.101.251.46	
Timestamp:	192.168.2.2395.101.251.4640078802027121 05/14/22-02:04:21.759965
SID:	2027121
Source Port:	40078
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: 95.101.188.42	
Timestamp:	192.168.2.2395.101.188.4252034802027121 05/14/22-02:03:55.661108
SID:	2027121
Source Port:	52034
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: 95.46.155.189	
Timestamp:	192.168.2.2395.46.155.18954704802027121 05/14/22-02:05:45.538592
SID:	2027121
Source Port:	54704
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: 95.57.137.245	
Timestamp:	192.168.2.2395.57.137.24547588802027121 05/14/22-02:05:19.828046
SID:	2027121
Source Port:	47588
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: 88.221.127.40	
Timestamp:	192.168.2.2388.221.127.4059250802027121 05/14/22-02:04:58.556033
SID:	2027121
Source Port:	59250
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: 88.221.35.81	
Timestamp:	192.168.2.2388.221.35.8157028802027121 05/14/22-02:04:32.325392
SID:	2027121
Source Port:	57028

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: 88.231.21.154

Timestamp:	192.168.2.2388.231.21.15459472802027121 05/14/22-02:03:57.843382
SID:	2027121
Source Port:	59472
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: 156.250.126.150

Timestamp:	192.168.2.23156.250.126.15040666528692027339 05/14/22-02:05:50.398115
SID:	2027339
Source Port:	40666
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: 172.65.233.234

Timestamp:	192.168.2.23172.65.233.23444670555552027153 05/14/22-02:04:57.329185
SID:	2027153
Source Port:	44670
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: 88.99.27.29

Timestamp:	192.168.2.2388.99.27.2959630802027121 05/14/22-02:04:04.408250
SID:	2027121
Source Port:	59630
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: 95.180.146.25

Timestamp:	192.168.2.2395.180.146.2538416802027121 05/14/22-02:04:30.926544
SID:	2027121
Source Port:	38416
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: 95.216.87.153

Timestamp:	192.168.2.2395.216.87.15359114802027121 05/14/22-02:03:53.362973
SID:	2027121
Source Port:	59114
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: 172.65.86.6

Timestamp:	192.168.2.23172.65.86.641400555552027153 05/14/22-02:04:36.974233
SID:	2027153
Source Port:	41400
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

Copyright Joe Security LLC 2022

ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami) - Source IP: 192.168.2.23 - Destination IP: 88.99.6.153	
Timestamp:	192.168.2.2388.99.6.15337118802027121 05/14/22-02:04:57.386875
SID:	2027121
Source Port:	37118
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: 88.34.183.106	
Timestamp:	192.168.2.2388.34.183.10636654802027121 05/14/22-02:05:33.094042
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: 95.168.168.168	
Timestamp:	192.168.2.2395.168.168.16852616802027121 05/14/22-02:03:57.738061
SID:	2027121
Source Port:	52616
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: 95.183.37.140	
Timestamp:	192.168.2.2395.183.37.14041168802027121 05/14/22-02:04:17.287353
SID:	2027121
Source Port:	41168
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: 95.216.49.245	
Timestamp:	192.168.2.2395.216.49.24535130802027121 05/14/22-02:04:57.381704
SID:	2027121
Source Port:	35130
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: 88.99.32.231	
Timestamp:	192.168.2.2388.99.32.23139366802027121 05/14/22-02:04:29.747000
SID:	2027121
Source Port:	39366
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: 95.223.191.176	
Timestamp:	192.168.2.2395.223.191.17654308802027121 05/14/22-02:04:00.998864
SID:	2027121
Source Port:	54308
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: 95.142.39.190	
Timestamp:	192.168.2.2395.142.39.19040324802027121 05/14/22-02:03:53.377984
SID:	2027121
Source Port:	40324

Copyright Joe Security LLC 2022

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: 95.100.151.50

Timestamp:	192.168.2.2395.100.151.5035770802027121 05/14/22-02:04:55.171540
SID:	2027121
Source Port:	35770
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: 172.65.199.227

Timestamp:	192.168.2.23172.65.199.22734996555552027153 05/14/22-02:05:37.018864
SID:	2027153
Source Port:	34996
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: 172.65.86.14

Timestamp:	192.168.2.23172.65.86.1447446555552027153 05/14/22-02:04:11.654959
SID:	2027153
Source Port:	47446
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: 156.254.70.117

Timestamp:	192.168.2.23156.254.70.11738860528692027339 05/14/22-02:05:37.010525
SID:	2027339
Source Port:	38860
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: 172.65.246.225

Timestamp:	192.168.2.23172.65.246.22549336555552027153 05/14/22-02:04:31.062353
SID:	2027153
Source Port:	49336
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: 88.221.250.120

Timestamp:	192.168.2.2388.221.250.12036710802027121 05/14/22-02:04:30.978771
SID:	2027121
Source Port:	36710
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: 88.218.158.143

Timestamp:	192.168.2.2388.218.158.14353512802027121 05/14/22-02:04:32.244935
SID:	2027121
Source Port:	53512
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: 172.65.105.87	
Timestamp:	192.168.2.23172.65.105.8740248555552027153 05/14/22-02:04:31.062442
SID:	2027153
Source Port:	40248
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: 172.245.113.111	
Timestamp:	192.168.2.23172.245.113.11138934555552027153 05/14/22-02:04:07.379640
SID:	2027153
Source Port:	38934
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: 88.193.184.68	
Timestamp:	192.168.2.2388.193.184.6838586802027121 05/14/22-02:05:47.764684
SID:	2027121
Source Port:	38586
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: 88.151.120.239	
Timestamp:	192.168.2.2388.151.120.23954648802027121 05/14/22-02:04:19.380599
SID:	2027121
Source Port:	54648
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: 156.240.108.229	
Timestamp:	192.168.2.23156.240.108.22955326528692027339 05/14/22-02:04:51.841222
SID:	2027339
Source Port:	55326
Destination Port:	52869
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: 156.226.61.77	
Timestamp:	192.168.2.23156.226.61.7735510528692027339 05/14/22-02:05:03.298472
SID:	2027339
Source Port:	35510
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: 172.245.25.8	
Timestamp:	192.168.2.23172.245.25.841564555552027153 05/14/22-02:05:04.432633
SID:	2027153
Source Port:	41564
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: 88.99.145.75	
Timestamp:	192.168.2.2388.99.145.7544708802027121 05/14/22-02:05:02.936838
SID:	2027121
Source Port:	44708

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: 95.129.189.11	−
Timestamp:	192.168.2.2395.129.189.1153350802027121 05/14/22-02:04:07.881985
SID:	2027121
Source Port:	53350
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: 88.247.119.147	−
Timestamp:	192.168.2.2388.247.119.14756892802027121 05/14/22-02:04:19.409992
SID:	2027121
Source Port:	56892
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: 172.65.48.243	−
Timestamp:	192.168.2.23172.65.48.243410205555552027153 05/14/22-02:04:43.913081
SID:	2027153
Source Port:	41020
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: 95.77.11.18	−
Timestamp:	192.168.2.2395.77.11.1836288802027121 05/14/22-02:05:08.836665
SID:	2027121
Source Port:	36288
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: 95.214.218.124	−
Timestamp:	192.168.2.2395.214.218.12438414802027121 05/14/22-02:04:01.070491
SID:	2027121
Source Port:	38414
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: 95.110.236.22	−
Timestamp:	192.168.2.2395.110.236.2245362802027121 05/14/22-02:04:09.284651
SID:	2027121
Source Port:	45362
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: 95.183.15.221	−
Timestamp:	192.168.2.2395.183.15.22143498802027121 05/14/22-02:04:23.251318
SID:	2027121
Source Port:	43498
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound - Source IP: 192.168.2.23 - Destination IP: 172.65.69.150	
Timestamp:	192.168.2.23172.65.69.15046380555552027153 05/14/22-02:05:37.019008
SID:	2027153
Source Port:	46380
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: 172.65.116.57	
Timestamp:	192.168.2.23172.65.116.5734996555552027153 05/14/22-02:04:24.881978
SID:	2027153
Source Port:	34996
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: 88.147.144.125	
Timestamp:	192.168.2.2388.147.144.12557076802027121 05/14/22-02:04:30.883444
SID:	2027121
Source Port:	57076
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: 172.65.241.93	
Timestamp:	192.168.2.23172.65.241.9347344555552027153 05/14/22-02:04:57.312233
SID:	2027153
Source Port:	47344
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: 172.65.132.196	
Timestamp:	192.168.2.23172.65.132.19643310555552027153 05/14/22-02:05:06.220049
SID:	2027153
Source Port:	43310
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: 95.100.182.172	
Timestamp:	192.168.2.2395.100.182.17258936802027121 05/14/22-02:04:23.192380
SID:	2027121
Source Port:	58936
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: 172.65.201.180	
Timestamp:	192.168.2.23172.65.201.18036496555552027153 05/14/22-02:05:45.978084
SID:	2027153
Source Port:	36496
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: 95.86.206.240	
Timestamp:	192.168.2.2395.86.206.24037732802027121 05/14/22-02:05:28.581595
SID:	2027121
Source Port:	37732

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: 156.245.59.234

Timestamp:	192.168.2.23156.245.59.23446694528692027339 05/14/22-02:05:37.070954
SID:	2027339
Source Port:	46694
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: 172.65.230.26

Timestamp:	192.168.2.23172.65.230.2638578555552027153 05/14/22-02:05:45.960758
SID:	2027153
Source Port:	38578
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: 95.142.39.190

Timestamp:	192.168.2.2395.142.39.19040332802027121 05/14/22-02:03:53.460756
SID:	2027121
Source Port:	40332
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: 95.101.10.131

Timestamp:	192.168.2.2395.101.10.13145578802027121 05/14/22-02:04:34.509938
SID:	2027121
Source Port:	45578
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: 95.111.227.220

Timestamp:	192.168.2.2395.111.227.22049974802027121 05/14/22-02:04:25.535524
SID:	2027121
Source Port:	49974
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: 172.65.79.233

Timestamp:	192.168.2.23172.65.79.23345034555552027153 05/14/22-02:05:54.037713
SID:	2027153
Source Port:	45034
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: 197.44.95.233

Timestamp:	192.168.2.23197.44.95.23339792528692027339 05/14/22-02:05:48.080780
SID:	2027339
Source Port:	39792
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: 95.101.179.218	
Timestamp:	192.168.2.2395.101.179.21840834802027121 05/14/22-02:04:21.731177
SID:	2027121
Source Port:	40834
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: 95.84.209.124	
Timestamp:	192.168.2.2395.84.209.12444178802027121 05/14/22-02:04:34.530155
SID:	2027121
Source Port:	44178
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: 88.221.241.166	
Timestamp:	192.168.2.2388.221.241.16646476802027121 05/14/22-02:04:45.587757
SID:	2027121
Source Port:	46476
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: 172.65.43.96	
Timestamp:	192.168.2.23172.65.43.9648762555552027153 05/14/22-02:04:04.201524
SID:	2027153
Source Port:	48762
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: 172.65.147.21	
Timestamp:	192.168.2.23172.65.147.2144500555552027153 05/14/22-02:05:24.831840
SID:	2027153
Source Port:	44500
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: 88.53.121.223	
Timestamp:	192.168.2.2388.53.121.22358244802027121 05/14/22-02:05:36.550041
SID:	2027121
Source Port:	58244
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: 172.65.244.183	
Timestamp:	192.168.2.23172.65.244.18337580555552027153 05/14/22-02:05:21.335692
SID:	2027153
Source Port:	37580
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: 95.217.234.237	
Timestamp:	192.168.2.2395.217.234.23742976802027121 05/14/22-02:04:45.496386
SID:	2027121
Source Port:	42976

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: 88.22.77.19	−
Timestamp:	192.168.2.2388.22.77.1933586802027121 05/14/22-02:05:16.374618
SID:	2027121
Source Port:	33586
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: 172.245.103.96	−
Timestamp:	192.168.2.23172.245.103.9646626555552027153 05/14/22-02:05:21.142244
SID:	2027153
Source Port:	46626
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: 95.217.177.216	−
Timestamp:	192.168.2.2395.217.177.21652404802027121 05/14/22-02:04:01.012402
SID:	2027121
Source Port:	52404
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: 88.217.172.164	−
Timestamp:	192.168.2.2388.217.172.16433898802027121 05/14/22-02:04:32.232576
SID:	2027121
Source Port:	33898
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: 88.247.4.15	−
Timestamp:	192.168.2.2388.247.4.1542394802027121 05/14/22-02:03:57.818353
SID:	2027121
Source Port:	42394
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: 172.65.190.190	−
Timestamp:	192.168.2.23172.65.190.19056196555552027153 05/14/22-02:05:09.759089
SID:	2027153
Source Port:	56196
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: 88.99.106.220	−
Timestamp:	192.168.2.2388.99.106.22060562802027121 05/14/22-02:04:21.715165
SID:	2027121
Source Port:	60562
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: 88.221.156.35	
Timestamp:	192.168.2.2388.221.156.3548314802027121 05/14/22-02:04:58.613996
SID:	2027121
Source Port:	48314
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: 88.255.170.17	
Timestamp:	192.168.2.2388.255.170.1759020802027121 05/14/22-02:04:37.610970
SID:	2027121
Source Port:	59020
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: 172.65.46.1	
Timestamp:	192.168.2.23172.65.46.159140555552027153 05/14/22-02:05:16.317135
SID:	2027153
Source Port:	59140
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: 95.90.100.253	
Timestamp:	192.168.2.2395.90.100.25360968802027121 05/14/22-02:04:45.495189
SID:	2027121
Source Port:	60968
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: 95.100.10.27	
Timestamp:	192.168.2.2395.100.10.2758494802027121 05/14/22-02:05:23.036314
SID:	2027121
Source Port:	58494
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: 88.151.120.239	
Timestamp:	192.168.2.2388.151.120.23954218802027121 05/14/22-02:04:04.436112
SID:	2027121
Source Port:	54218
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: 95.217.74.29	
Timestamp:	192.168.2.2395.217.74.2949830802027121 05/14/22-02:04:48.048276
SID:	2027121
Source Port:	49830
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: 172.65.41.239	
Timestamp:	192.168.2.23172.65.41.23933628555552027153 05/14/22-02:05:09.761720
SID:	2027153
Source Port:	33628

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: 172.65.91.62	
Timestamp:	192.168.2.23172.65.91.6249884555552027153 05/14/22-02:03:52.401161
SID:	2027153
Source Port:	49884
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: 95.217.171.189	
Timestamp:	192.168.2.2395.217.171.18950806802027121 05/14/22-02:05:03.000835
SID:	2027121
Source Port:	50806
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: 172.245.107.236	
Timestamp:	192.168.2.23172.245.107.236404665555552027153 05/14/22-02:05:04.432766
SID:	2027153
Source Port:	40466
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: 95.211.48.234	
Timestamp:	192.168.2.2395.211.48.23437548802027121 05/14/22-02:04:29.723243
SID:	2027121
Source Port:	37548
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: 95.143.49.238	
Timestamp:	192.168.2.2395.143.49.23841548802027121 05/14/22-02:04:09.265829
SID:	2027121
Source Port:	41548
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: 95.216.113.235	
Timestamp:	192.168.2.2395.216.113.23540052802027121 05/14/22-02:04:19.433599
SID:	2027121
Source Port:	40052
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: 88.99.250.96	
Timestamp:	192.168.2.2388.99.250.9638340802027121 05/14/22-02:03:57.760926
SID:	2027121
Source Port:	38340
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: 95.110.188.58	
Timestamp:	192.168.2.2395.110.188.5850186802027121 05/14/22-02:04:21.767738
SID:	2027121
Source Port:	50186
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: 172.65.147.240	
Timestamp:	192.168.2.23172.65.147.24056508555552027153 05/14/22-02:04:15.724140
SID:	2027153
Source Port:	56508
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: 172.65.7.173	
Timestamp:	192.168.2.23172.65.7.17351778555552027153 05/14/22-02:04:34.703705
SID:	2027153
Source Port:	51778
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: 172.65.227.132	
Timestamp:	192.168.2.23172.65.227.13246070555552027153 05/14/22-02:05:09.758844
SID:	2027153
Source Port:	46070
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: 172.65.94.144	
Timestamp:	192.168.2.23172.65.94.14451176555552027153 05/14/22-02:04:19.383126
SID:	2027153
Source Port:	51176
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: 88.99.0.56	
Timestamp:	192.168.2.2388.99.0.5634224802027121 05/14/22-02:04:40.793936
SID:	2027121
Source Port:	34224
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: 156.245.35.206	
Timestamp:	192.168.2.23156.245.35.20639160528692027339 05/14/22-02:04:01.120042
SID:	2027339
Source Port:	39160
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: 172.65.203.159	
Timestamp:	192.168.2.23172.65.203.15944186555552027153 05/14/22-02:03:58.555655
SID:	2027153
Source Port:	44186

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: 172.65.205.160	
Timestamp:	192.168.2.23172.65.205.16052354555552027153 05/14/22-02:04:49.789360
SID:	2027153
Source Port:	52354
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: 156.226.100.41	
Timestamp:	192.168.2.23156.226.100.4157032528692027339 05/14/22-02:05:04.864593
SID:	2027339
Source Port:	57032
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: 95.216.241.210	
Timestamp:	192.168.2.2395.216.241.21038106802027121 05/14/22-02:04:50.438289
SID:	2027121
Source Port:	38106
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: 88.151.115.26	
Timestamp:	192.168.2.2388.151.115.2648772802027121 05/14/22-02:04:09.698765
SID:	2027121
Source Port:	48772
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: 88.248.100.210	
Timestamp:	192.168.2.2388.248.100.21059808802027121 05/14/22-02:04:45.455125
SID:	2027121
Source Port:	59808
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: 172.65.170.206	
Timestamp:	192.168.2.23172.65.170.20642126555552027153 05/14/22-02:05:04.147038
SID:	2027153
Source Port:	42126
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: 88.221.247.46	
Timestamp:	192.168.2.2388.221.247.4656332802027121 05/14/22-02:05:16.728469
SID:	2027121
Source Port:	56332
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: 95.65.48.22	
Timestamp:	192.168.2.2395.65.48.2244716802027121 05/14/22-02:04:23.241574
SID:	2027121
Source Port:	44716
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: 156.254.86.103	
Timestamp:	192.168.2.23156.254.86.10347550528692027339 05/14/22-02:05:02.793230
SID:	2027339
Source Port:	47550
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: 172.65.116.243	
Timestamp:	192.168.2.23172.65.116.24337208555552027153 05/14/22-02:03:58.555471
SID:	2027153
Source Port:	37208
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: 172.65.196.122	
Timestamp:	192.168.2.23172.65.196.12241800555552027153 05/14/22-02:05:37.001489
SID:	2027153
Source Port:	41800
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: 88.151.50.21	
Timestamp:	192.168.2.2388.151.50.2139518802027121 05/14/22-02:05:23.027466
SID:	2027121
Source Port:	39518
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: 95.245.176.100	
Timestamp:	192.168.2.2395.245.176.10047458802027121 05/14/22-02:04:02.312326
SID:	2027121
Source Port:	47458
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: 156.254.85.23	
Timestamp:	192.168.2.23156.254.85.23456105286920273 39 05/14/22-02:05:12.491233
SID:	2027339
Source Port:	45610
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: 88.198.176.127	
Timestamp:	192.168.2.2388.198.176.12760206802027121 05/14/22-02:04:13.144517
SID:	2027121
Source Port:	60206

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: 88.221.10.202	
Timestamp:	192.168.2.2388.221.10.20254556802027121 05/14/22-02:04:52.747584
SID:	2027121
Source Port:	54556
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: 172.65.36.175	
Timestamp:	192.168.2.23172.65.36.17548486555552027153 05/14/22-02:04:57.312175
SID:	2027153
Source Port:	48486
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: 88.247.120.102	
Timestamp:	192.168.2.2388.247.120.10250276802027121 05/14/22-02:05:50.075434
SID:	2027121
Source Port:	50276
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: 88.221.18.135	
Timestamp:	192.168.2.2388.221.18.13558280802027121 05/14/22-02:04:32.272004
SID:	2027121
Source Port:	58280
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: 95.101.189.56	
Timestamp:	192.168.2.2395.101.189.5648426802027121 05/14/22-02:03:55.661040
SID:	2027121
Source Port:	48426
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: 172.65.214.15	
Timestamp:	192.168.2.23172.65.214.1560194555552027153 05/14/22-02:05:20.978194
SID:	2027153
Source Port:	60194
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: 95.100.77.49	
Timestamp:	192.168.2.2395.100.77.4953544802027121 05/14/22-02:05:23.001580
SID:	2027121
Source Port:	53544
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: 95.91.29.213	
Timestamp:	192.168.2.2395.91.29.21342706802027121 05/14/22-02:05:19.755389
SID:	2027121
Source Port:	42706
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: 172.65.97.200	
Timestamp:	192.168.2.23172.65.97.20051602555552027153 05/14/22-02:04:34.685570
SID:	2027153
Source Port:	51602
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: 95.65.25.23	
Timestamp:	192.168.2.2395.65.25.2359674802027121 05/14/22-02:04:09.303014
SID:	2027121
Source Port:	59674
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: 98.159.33.130	
Timestamp:	192.168.2.2398.159.33.13042202555552027153 05/14/22-02:04:46.257949
SID:	2027153
Source Port:	42202
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: 88.221.136.77	
Timestamp:	192.168.2.2388.221.136.7740648802027121 05/14/22-02:04:43.322465
SID:	2027121
Source Port:	40648
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: 95.101.241.198	
Timestamp:	192.168.2.2395.101.241.19859824802027121 05/14/22-02:04:43.339295
SID:	2027121
Source Port:	59824
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: 95.216.236.178	
Timestamp:	192.168.2.2395.216.236.17850606802027121 05/14/22-02:05:45.541757
SID:	2027121
Source Port:	50606
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: 88.148.137.222	
Timestamp:	192.168.2.2388.148.137.22246540802027121 05/14/22-02:04:40.840279
SID:	2027121
Source Port:	46540

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: 88.221.138.147	
Timestamp:	192.168.2.2388.221.138.14732984802027121 05/14/22-02:05:27.261197
SID:	2027121
Source Port:	32984
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: 95.211.221.121	
Timestamp:	192.168.2.2395.211.221.12139408802027121 05/14/22-02:04:21.756854
SID:	2027121
Source Port:	39408
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: 88.226.220.156	
Timestamp:	192.168.2.2388.226.220.15637282802027121 05/14/22-02:05:04.229140
SID:	2027121
Source Port:	37282
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: 95.148.139.31	
Timestamp:	192.168.2.2395.148.139.3154776802027121 05/14/22-02:04:50.437562
SID:	2027121
Source Port:	54776
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: 88.31.6.113	
Timestamp:	192.168.2.2388.31.6.11359422802027121 05/14/22-02:04:58.535677
SID:	2027121
Source Port:	59422
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: 88.148.49.42	
Timestamp:	192.168.2.2388.148.49.4251404802027121 05/14/22-02:04:48.007218
SID:	2027121
Source Port:	51404
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: 88.99.101.202	
Timestamp:	192.168.2.2388.99.101.20254734802027121 05/14/22-02:04:01.022090
SID:	2027121
Source Port:	54734
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: 172.65.50.231	
Timestamp:	192.168.2.23172.65.50.23143836555552027153 05/14/22-02:05:41.244057
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: 88.202.226.216	
Timestamp:	192.168.2.2388.202.226.21658762802027121 05/14/22-02:04:32.259524
SID:	2027121
Source Port:	58762
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: 172.65.98.138	
Timestamp:	192.168.2.23172.65.98.13860678555552027153 05/14/22-02:04:50.716191
SID:	2027153
Source Port:	60678
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: 172.65.50.68	
Timestamp:	192.168.2.23172.65.50.6848506555552027153 05/14/22-02:04:13.394170
SID:	2027153
Source Port:	48506
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: 172.65.203.91	
Timestamp:	192.168.2.23172.65.203.9147194555552027153 05/14/22-02:05:18.632714
SID:	2027153
Source Port:	47194
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: 172.65.225.222	
Timestamp:	192.168.2.23172.65.225.22251082555552027153 05/14/22-02:04:31.045044
SID:	2027153
Source Port:	51082
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: 95.100.119.33	
Timestamp:	192.168.2.2395.100.119.3360388802027121 05/14/22-02:04:55.076014
SID:	2027121
Source Port:	60388
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: 88.31.225.158	
Timestamp:	192.168.2.2388.31.225.15836930802027121 05/14/22-02:04:58.537628
SID:	2027121
Source Port:	36930

Copyright Joe Security LLC 2022

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: 95.219.212.29

Timestamp:	192.168.2.2395.219.212.2959618802027121 05/14/22-02:05:00.802432
SID:	2027121
Source Port:	59618
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: 172.65.20.200

Timestamp:	192.168.2.23172.65.20.20039984555552027153 05/14/22-02:05:04.335191
SID:	2027153
Source Port:	39984
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: 172.65.105.200

Timestamp:	192.168.2.23172.65.105.20040100555552027153 05/14/22-02:04:46.275094
SID:	2027153
Source Port:	40100
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: 156.244.78.201

Timestamp:	192.168.2.23156.244.78.20139706528692027339 05/14/22-02:05:33.351834
SID:	2027339
Source Port:	39706
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: 172.65.187.28

Timestamp:	192.168.2.23172.65.187.2835410555552027153 05/14/22-02:05:43.557994
SID:	2027153
Source Port:	35410
Destination Port:	55555
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ET CNC Feodo Tracker Reported CnC Server TCP group 20 - Source IP: 192.168.2.23 - Destination IP: 62.75.251.60

Timestamp:	192.168.2.2362.75.251.601461880802404338 05/14/22-02:04:37.171076
SID:	2404338
Source Port:	14618
Destination Port:	8080
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: 172.65.190.182

Timestamp:	192.168.2.23172.65.190.18233602555552027153 05/14/22-02:05:24.831916
SID:	2027153
Source Port:	33602
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: 88.147.251.78	
Timestamp:	192.168.2.2388.147.251.7849714802027121 05/14/22-02:05:52.722920
SID:	2027121
Source Port:	49714
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: 95.216.247.240	
Timestamp:	192.168.2.2395.216.247.24048722802027121 05/14/22-02:03:53.362682
SID:	2027121
Source Port:	48722
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: 88.249.57.159	
Timestamp:	192.168.2.2388.249.57.15956710802027121 05/14/22-02:04:55.177371
SID:	2027121
Source Port:	56710
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: 95.100.222.34	
Timestamp:	192.168.2.2395.100.222.3448534802027121 05/14/22-02:04:57.385948
SID:	2027121
Source Port:	48534
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: 172.65.1.109	
Timestamp:	192.168.2.23172.65.1.10954966555552027153 05/14/22-02:05:45.960834
SID:	2027153
Source Port:	54966
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: 88.79.138.160	
Timestamp:	192.168.2.2388.79.138.16058010802027121 05/14/22-02:04:19.377128
SID:	2027121
Source Port:	58010
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: 95.100.151.50	
Timestamp:	192.168.2.2395.100.151.5035616802027121 05/14/22-02:04:48.074101
SID:	2027121
Source Port:	35616
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: 95.181.22.158	
Timestamp:	192.168.2.2395.181.22.15853724802027121 05/14/22-02:04:19.574675
SID:	2027121
Source Port:	53724

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: 172.65.118.42	
Timestamp:	192.168.2.23172.65.118.4260148555552027153 05/14/22-02:04:27.953786
SID:	2027153
Source Port:	60148
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: 172.65.103.40	
Timestamp:	192.168.2.23172.65.103.4058388555552027153 05/14/22-02:04:42.995871
SID:	2027153
Source Port:	58388
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: 156.226.14.241	
Timestamp:	192.168.2.23156.226.14.241391025286920273 39 05/14/22-02:04:47.287454
SID:	2027339
Source Port:	39102
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: 172.65.76.183	
Timestamp:	192.168.2.23172.65.76.183570285555520271 53 05/14/22-02:05:09.775735
SID:	2027153
Source Port:	57028
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: 156.250.83.86	
Timestamp:	192.168.2.23156.250.83.86543505286920273 39 05/14/22-02:05:12.575619
SID:	2027339
Source Port:	54350
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: 95.100.151.50	
Timestamp:	192.168.2.2395.100.151.5035638802027121 05/14/22-02:04:49.195229
SID:	2027121
Source Port:	35638
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: 95.56.213.156	
Timestamp:	192.168.2.2395.56.213.15642384802027121 05/14/22-02:04:04.659452
SID:	2027121
Source Port:	42384
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: 95.216.27.106	
Timestamp:	192.168.2.2395.216.27.10660464802027121 05/14/22-02:04:45.496679
SID:	2027121
Source Port:	60464
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: 156.226.83.133	
Timestamp:	192.168.2.23156.226.83.13349816528692027339 05/14/22-02:05:07.440596
SID:	2027339
Source Port:	49816
Destination Port:	52869
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

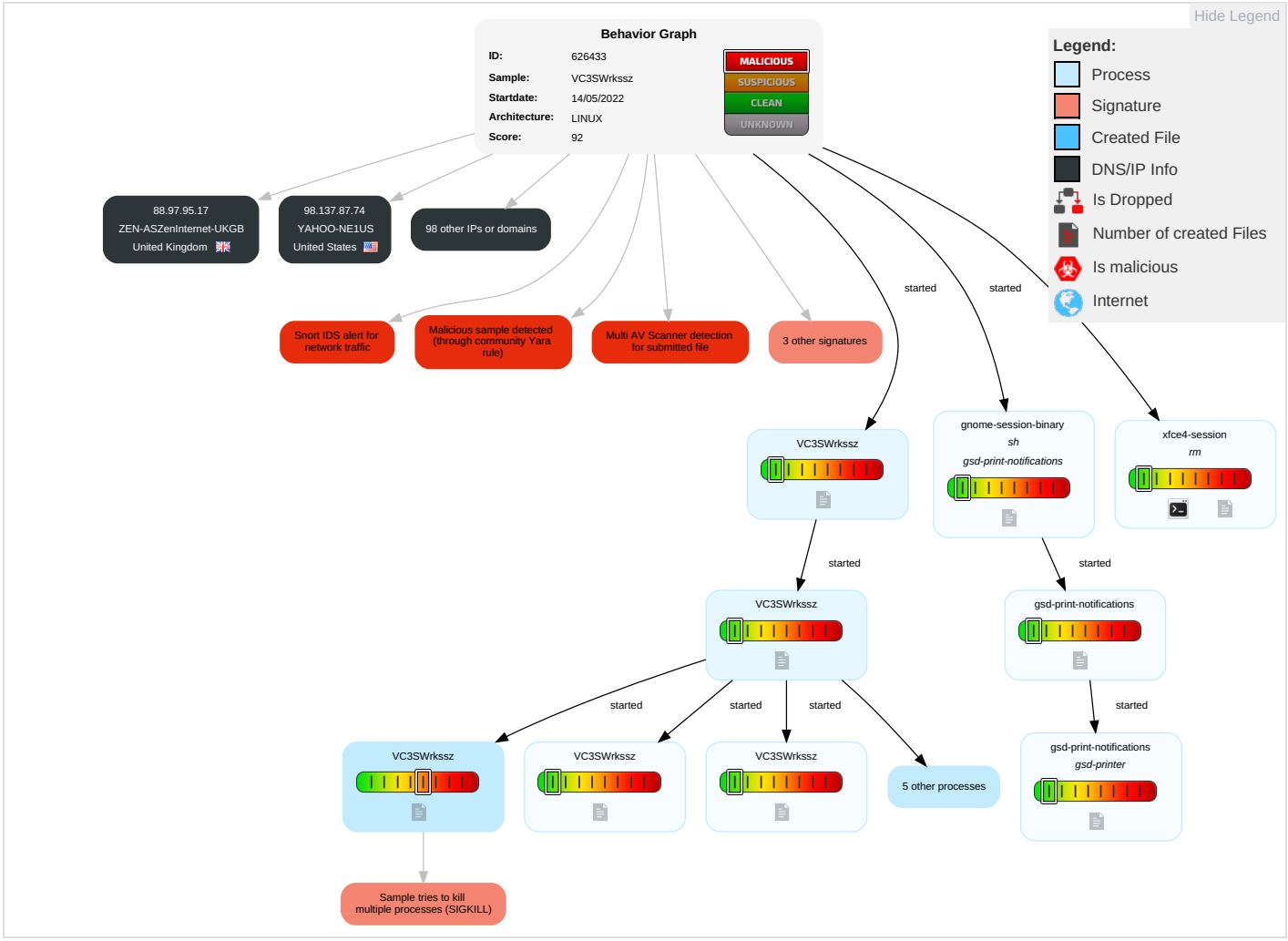
Mitre Att&ck Matrix

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	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	4 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

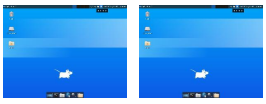
Behavior Graph

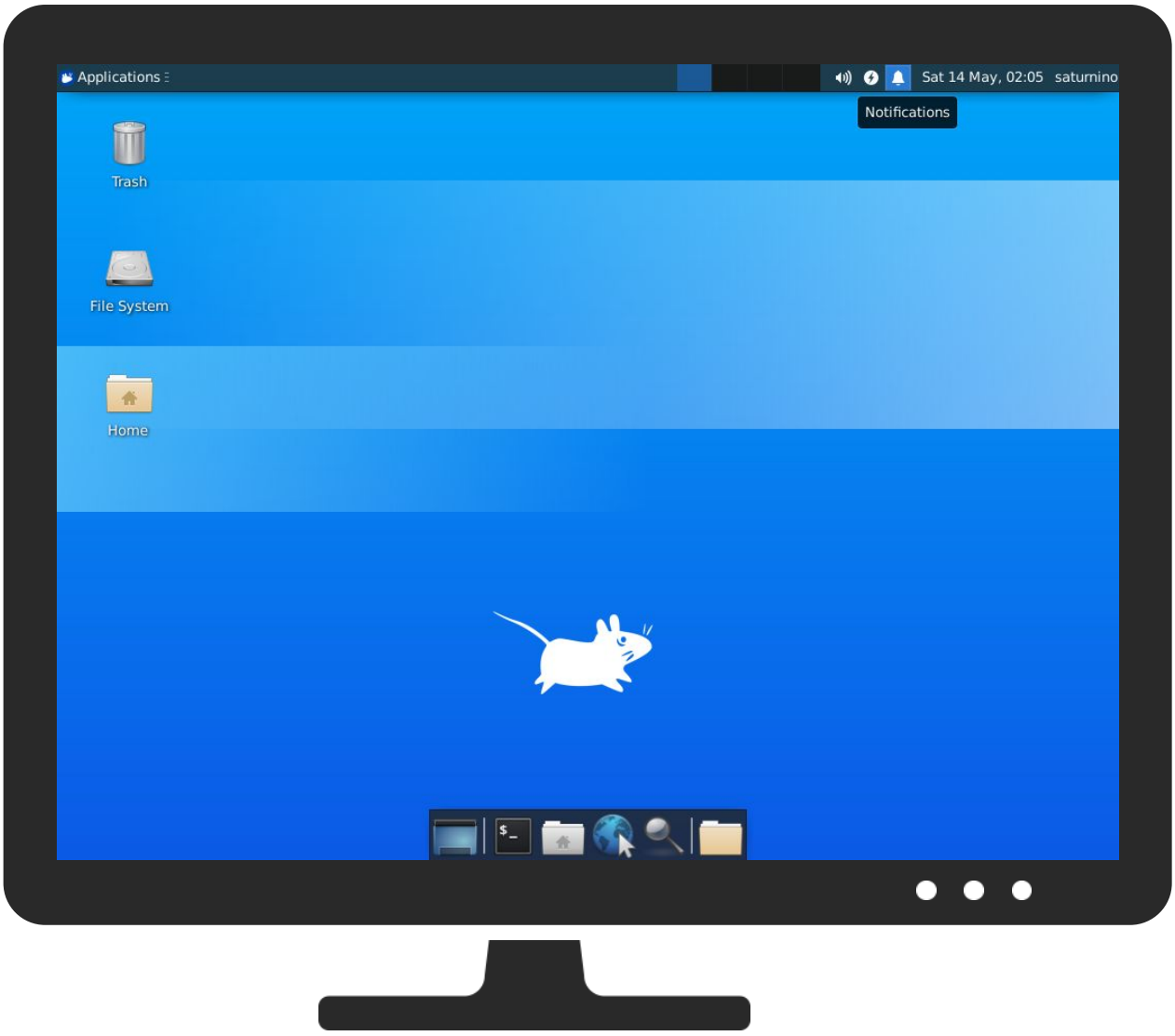


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
VC3SWrkssz	29%	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;	0%	Avira URL Cloud	safe	
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	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

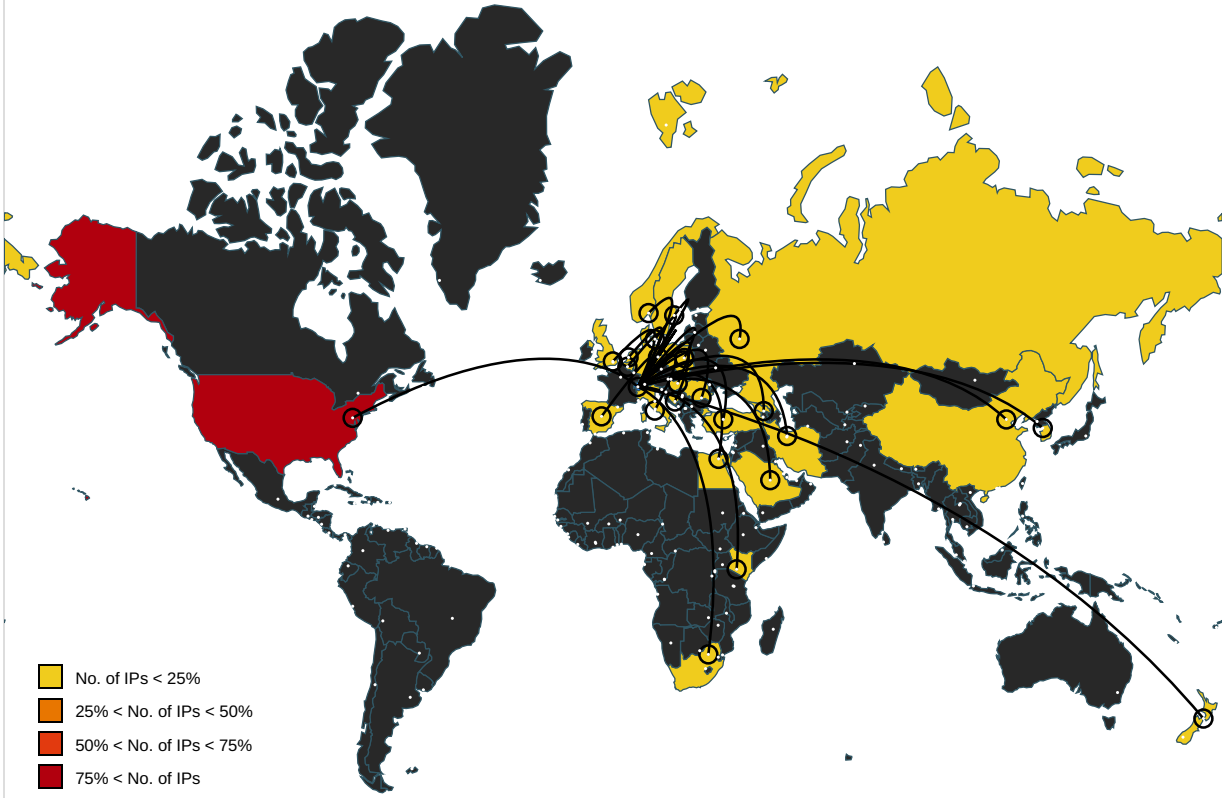
No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/tmUnblock.cgi	false	• 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
98.206.228.41	unknown	United States		7922	COMCAST-7922US	false
62.91.213.251	unknown	Germany		20686	BISPINGISPCitycarrierGermanyDE	false
172.227.134.116	unknown	United States		20940	AKAMAI-ASN1EU	false
184.223.3.26	unknown	United States		10507	SPCSUS	false
31.223.57.114	unknown	Turkey		12735	ASTURKNETTR	false
95.123.15.179	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
172.242.149.106	unknown	United States		7155	VIASAT-SP-BACKBONEUS	false
95.36.120.143	unknown	Netherlands		15670	BBNED-AS1NL	false
88.55.191.6	unknown	Italy		3269	ASN-IBSNAZIT	false
184.172.25.26	unknown	United States		36351	SOFTLAYERUS	false
94.137.178.41	unknown	Georgia		16010	MAGTICOMASCaucasus-OnlineGE	false
62.32.94.240	unknown	Russian Federation		8492	OBIT-ASOBITLtdRU	false
94.232.145.15	unknown	Poland		39893	NETSYSTEM_TP-ASNPL	false
156.69.212.10	unknown	New Zealand		297	AS297US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.151.70.233	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
157.184.0.126	unknown	United States		22192	SSHENETUS	false
62.235.224.64	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
31.238.72.60	unknown	Germany		3320	DTAGInternetserviceproviderationsDE	false
98.35.84.103	unknown	United States		7922	COMCAST-7922US	false
172.51.68.36	unknown	United States		21928	T-MOBILE-AS21928US	false
95.14.46.159	unknown	Turkey		9121	TTNETTR	false
98.176.149.131	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
94.4.72.96	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
95.142.40.188	unknown	Russian Federation		210079	EUROBYTEEurobyteLLCMoscowRussiaRU	false
172.235.101.221	unknown	United States		20940	AKAMAI-ASN1EU	false
94.37.176.228	unknown	Italy		8612	TISCALI-IT	false
95.156.176.205	unknown	Bosnia and Herzegowina		20875	HPTNET-ASBA	false
85.57.45.15	unknown	Spain		12479	UNI2-ASES	false
98.187.110.146	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
88.97.95.17	unknown	United Kingdom		13037	ZEN-ASZenInternet-UKGB	false
88.253.165.242	unknown	Turkey		9121	TTNETTR	false
41.54.12.248	unknown	South Africa		37168	CELL-CZA	false
98.15.44.76	unknown	United States		12271	TWC-12271-NYCUS	false
98.196.137.50	unknown	United States		7922	COMCAST-7922US	false
197.197.89.96	unknown	Egypt		36992	ETISALAT-MISREG	false
95.6.137.34	unknown	Turkey		9121	TTNETTR	false
88.107.143.239	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
172.71.235.2	unknown	United States		13335	CLOUDFLARENETUS	false
98.104.1.60	unknown	United States		6167	CELLCO-PARTUS	false
62.246.7.73	unknown	Germany		12312	ECOTELDE	false
5.204.164.7	unknown	Hungary		8448	PGSM-HUTorokbalintHungaryHU	false
184.49.234.41	unknown	United States		14654	WAYPORTUS	false
184.84.36.157	unknown	United States		577	BACOMCA	false
184.76.52.183	unknown	United States		16509	AMAZON-02US	false
184.216.124.80	unknown	United States		10507	SPCSUS	false
95.142.40.187	unknown	Russian Federation		210079	EUROBYTEEurobyteLLCMoscowRussiaRU	false
172.35.114.194	unknown	United States		21928	T-MOBILE-AS21928US	false
85.25.248.104	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
98.206.228.22	unknown	United States		7922	COMCAST-7922US	false
98.71.213.201	unknown	United States		7018	ATT-INTERNET4US	false
31.16.255.164	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
98.169.64.229	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
184.225.199.73	unknown	United States		10507	SPCSUS	false
85.21.177.221	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
197.76.64.251	unknown	South Africa		16637	MTNNS-ASZA	false
94.193.8.114	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
5.224.64.15	unknown	Spain		12430	VODAFONE_ESES	false
98.153.107.49	unknown	United States		20001	TWC-20001-PACWESTUS	false
98.109.42.197	unknown	United States		701	UUNETUS	false
62.245.191.250	unknown	Germany		8767	MNET-ASGermanyDE	false
79.150.100.174	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
31.94.153.240	unknown	United Kingdom		12576	EELtdGB	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.91.248.192	unknown	United Kingdom		34270	INETCInternetConnectionsLtdGB	false
98.176.149.114	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
5.238.185.239	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
95.212.118.86	unknown	Egypt		51167	CONTABODE	false
94.8.166.112	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
95.76.74.111	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
95.185.43.168	unknown	Saudi Arabia		39891	ALJAWWALSTC-ASSA	false
197.234.167.155	unknown	South Africa		37315	CipherWaveZA	false
197.237.248.159	unknown	Kenya		15399	WANANCHI-KE	false
184.34.108.21	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
94.25.52.21	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
98.117.37.49	unknown	United States		701	UUNETUS	false
172.51.68.65	unknown	United States		21928	T-MOBILE-AS21928US	false
98.39.201.80	unknown	United States		7922	COMCAST-7922US	false
88.159.204.63	unknown	Netherlands		1136	KPNKPNNationalEU	false
172.51.68.67	unknown	United States		21928	T-MOBILE-AS21928US	false
88.46.176.48	unknown	Italy		3269	ASN-IBSNAZIT	false
88.12.127.132	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
62.127.93.5	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
88.40.154.183	unknown	Italy		3269	ASN-IBSNAZIT	false
172.31.17.250	unknown	Reserved		7018	ATT-INTERNET4US	false
172.185.62.36	unknown	United States		7018	ATT-INTERNET4US	false
184.154.183.251	unknown	United States		32475	SINGLEHOP-LLCUS	false
95.112.221.217	unknown	Germany		6805	TDDE-ASN1DE	false
37.207.81.33	unknown	Italy		3269	ASN-IBSNAZIT	false
98.42.30.225	unknown	United States		7922	COMCAST-7922US	false
42.139.61.211	unknown	China		4249	LILLY-ASUS	false
98.42.30.227	unknown	United States		7922	COMCAST-7922US	false
37.191.235.161	unknown	Norway		57963	LYNET-INTERNETT-ASNO	false
118.128.12.41	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
95.145.60.70	unknown	United Kingdom		12576	EELtdGB	false
184.84.36.102	unknown	United States		577	BACOMCA	false
98.26.137.88	unknown	United States		11426	TWC-11426-CAROLINASUS	false
98.117.37.11	unknown	United States		701	UUNETUS	false
98.68.97.219	unknown	United States		7018	ATT-INTERNET4US	false
95.100.100.168	unknown	European Union		20940	AKAMAI-ASN1EU	false
184.245.8.46	unknown	United States		10507	SPCSUS	false
98.137.87.74	unknown	United States		36646	YAHOO-NE1US	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.924378908952515
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	VC3SWrkssz
File size:	36504
MD5:	981e959599e29b1d9a2968bbf6387bae
SHA1:	258686ffea44f41925fd5af6724e69b241079013
SHA256:	dc80f285f9f5077f475dbbb184dbcfbbd32f55c2a15bb80dd04bd1ebf7468978
SHA512:	450605934931ad05cfbbabc106919ac368327a3657437a7527e33d34aa81b86f342c9e8b5fd4cc67802956c7313aeadf74b765460242bd48298c46c5f5eeb520
SSDEEP:	768:uGZhmCsNe/eOd/Zz+eCp4FYnxAs6PKaxuUd/13EJgGlzDpbuR1JY:uGmNdOdgIwyDPKa6VJui
TLSH:	AEF2F13D1B511A9FC09341BD4FA047112F520BB3DAA24D9E2588FDFA9C0A481FF636E9
File Content Preview:	.ELF.....z ...4.....4. ...(.....d...d.....?T.C?T.C?T.....UPX!.h.....7D..7D.....U.....?.E.h4...@b..) ..]....E....`f..sr...Y<M.^n..E...1....Wj..4X.._...w."..u..o.....$<..v.....[

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x107a20
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Copyright Joe Security LLC 2022

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x8d64	0x8d64	4.1751	0x5	R E	0x10000		
LOAD	0x3f54	0x433f54	0x433f54	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.225.1983548655552027153 05/14/22-02:04:11.637927	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35486	55555	192.168.2.23	172.65.225.198
192.168.2.23156.245.55.1254078052869202733905/14/22-02:05:10.063522	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	40780	52869	192.168.2.23	156.245.55.125
192.168.2.2388.221.247.4656298802027121 05/14/22-02:05:16.496663	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56298	80	192.168.2.23	88.221.247.46
192.168.2.23172.65.64.984284455555202715305/14/22-02:05:20.995117	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	42844	55555	192.168.2.23	172.65.64.98
192.168.2.23172.65.48.264590655555202715305/14/22-02:05:54.037647	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	45906	55555	192.168.2.23	172.65.48.26
192.168.2.2388.218.156.21445324802027121 05/14/22-02:05:04.368184	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45324	80	192.168.2.23	88.218.156.214
192.168.2.23172.65.123.7840044555552027153 05/14/22-02:04:34.703644	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40044	55555	192.168.2.23	172.65.123.78
192.168.2.2395.209.159.21034302802027121 05/14/22-02:04:45.560206	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34302	80	192.168.2.23	95.209.159.210
192.168.2.23156.226.79.2647988528692027339 05/14/22-02:04:47.625880	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	47988	52869	192.168.2.23	156.226.79.26
192.168.2.2388.100.202.19760688802027121 05/14/22-02:04:17.306136	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60688	80	192.168.2.23	88.100.202.197
192.168.2.2395.94.67.1535236802027121 05/14/22-02:04:02.248726	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35236	80	192.168.2.23	95.94.67.15
192.168.2.2388.198.233.19751822802027121 05/14/22-02:04:21.714018	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	51822	80	192.168.2.23	88.198.233.197
192.168.2.2388.160.72.15148858802027121 05/14/22-02:04:55.282834	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48858	80	192.168.2.23	88.160.72.151
192.168.2.23172.65.175.1604493655552027153 05/14/22-02:05:43.540529	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44936	55555	192.168.2.23	172.65.175.160
192.168.2.23172.65.246.676050255552027153 05/14/22-02:05:45.978345	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60502	55555	192.168.2.23	172.65.246.67

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.245.156518725555202715305/14/22-02:04:27.970733	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51872	55555	192.168.2.23	172.65.245.156
192.168.2.2388.221.43.15360046802027121 05/14/22-02:04:49.296960	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60046	80	192.168.2.23	88.221.43.153
192.168.2.23172.65.40.184557545555202715305/14/22-02:04:34.721447	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	55754	55555	192.168.2.23	172.65.40.184
192.168.2.2395.170.142.9154540802027121 05/14/22-02:05:16.526766	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54540	80	192.168.2.23	95.170.142.91
192.168.2.23172.65.243.174560445555202715305/14/22-02:05:43.557862	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56044	55555	192.168.2.23	172.65.243.174
192.168.2.2388.83.120.5454084802027121 05/14/22-02:04:55.111233	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54084	80	192.168.2.23	88.83.120.54
192.168.2.23156.254.55.1215099852869202733905/14/22-02:04:39.323189	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	50998	52869	192.168.2.23	156.254.55.121
192.168.2.23172.65.247.445699655555202715305/14/22-02:04:27.965299	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56996	55555	192.168.2.23	172.65.247.44
192.168.2.2388.12.181.23545164802027121 05/14/22-02:05:06.625031	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45164	80	192.168.2.23	88.12.181.235
192.168.2.23172.65.66.14948008555552027153 05/14/22-02:05:09.761803	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48008	55555	192.168.2.23	172.65.66.149
192.168.2.23172.65.35.555238455555202715305/14/22-02:05:54.037779	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	52384	55555	192.168.2.23	172.65.35.55
192.168.2.23156.238.52.2334431652869202733905/14/22-02:04:03.540343	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44316	52869	192.168.2.23	156.238.52.233
192.168.2.2395.101.124.744862802027121 05/14/22-02:04:07.843399	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44862	80	192.168.2.23	95.101.124.7
192.168.2.2388.151.120.23954210802027121 05/14/22-02:04:04.413192	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54210	80	192.168.2.23	88.151.120.239
192.168.2.23197.234.59.17640198372152835222 05/14/22-02:04:48.680620	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40198	37215	192.168.2.23	197.234.59.176
192.168.2.2388.221.227.22344588802027121 05/14/22-02:04:55.265828	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44588	80	192.168.2.23	88.221.227.223
192.168.2.23172.65.176.1234920855552027153 05/14/22-02:04:01.919544	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49208	55555	192.168.2.23	172.65.176.123
192.168.2.2388.116.145.172537188020271 21 05/14/22-02:04:19.393127	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53718	80	192.168.2.23	88.116.145.172
192.168.2.2395.188.114.161597408020271 21 05/14/22-02:03:57.828010	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59740	80	192.168.2.23	95.188.114.161

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.210.80527645555520271535/14/22-02:04:07.308990	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	52764	55555	192.168.2.23	172.65.210.80
192.168.2.2395.130.227.219547248020271215/14/22-02:04:09.253114	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54724	80	192.168.2.23	95.130.227.219
192.168.2.2395.73.184.9855062802027121 05/14/22-02:05:00.755463	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55062	80	192.168.2.23	95.73.184.98
192.168.2.23156.245.46.10746162528692027339 05/14/22-02:04:51.923330	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46162	52869	192.168.2.23	156.245.46.107
192.168.2.23156.247.21.129429645286920273395/14/22-02:05:32.842628	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	42964	52869	192.168.2.23	156.247.21.129
192.168.2.2395.166.126.9450592802027121 05/14/22-02:04:25.514613	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50592	80	192.168.2.23	95.166.126.94
192.168.2.2395.217.139.18940702802027121 05/14/22-02:04:23.234556	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40702	80	192.168.2.23	95.217.139.189
192.168.2.23172.245.58.785241855555202715305/14/22-02:05:24.859914	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	52418	55555	192.168.2.23	172.245.58.78
192.168.2.23172.65.244.24633926555552027153 05/14/22-02:04:52.963336	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33926	55555	192.168.2.23	172.65.244.246
192.168.2.23172.65.167.21250504555552027153 05/14/22-02:05:46.355886	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	50504	55555	192.168.2.23	172.65.167.212
192.168.2.2395.34.6.15055186802027121 05/14/22-02:04:11.024463	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55186	80	192.168.2.23	95.34.6.150
192.168.2.2395.100.227.12641560802027121 05/14/22-02:04:19.423556	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41560	80	192.168.2.23	95.100.227.126
192.168.2.2388.150.188.18546066802027121 05/14/22-02:05:22.993162	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46066	80	192.168.2.23	88.150.188.185
192.168.2.23172.65.44.2540066555552027153 05/14/22-02:03:55.485637	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40066	55555	192.168.2.23	172.65.44.25
192.168.2.2395.216.50.13837606802027121 05/14/22-02:04:01.004807	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37606	80	192.168.2.23	95.216.50.138
192.168.2.2395.211.210.9335332802027121 05/14/22-02:04:40.769456	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35332	80	192.168.2.23	95.211.210.93
192.168.2.23172.65.41.923700855552027153 05/14/22-02:04:22.454733	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37008	55555	192.168.2.23	172.65.41.92
192.168.2.2388.221.247.2036634802027121 05/14/22-02:04:41.120142	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36634	80	192.168.2.23	88.221.247.20
192.168.2.23172.65.207.22452754555552027153 05/14/22-02:04:46.156570	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	52754	55555	192.168.2.23	172.65.207.224

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.230.24.14839870528692027339 05/14/22-02:04:37.094159	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39870	52869	192.168.2.23	156.230.24.148
192.168.2.2388.208.209.1350344802027121 05/14/22-02:04:13.122146	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50344	80	192.168.2.23	88.208.209.13
192.168.2.2395.100.228.24052510802027121 05/14/22-02:04:11.012752	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52510	80	192.168.2.23	95.100.228.240
192.168.2.2388.221.99.5954200802027121 05/14/22-02:04:04.419952	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54200	80	192.168.2.23	88.221.99.59
192.168.2.23172.65.86.6346324555552027153 05/14/22-02:03:58.555530	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	46324	55555	192.168.2.23	172.65.86.63
192.168.2.23172.65.253.1635612855552027153 05/14/22-02:04:24.881877	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56128	55555	192.168.2.23	172.65.253.163
192.168.2.2395.59.181.20043136802027121 05/14/22-02:05:19.833635	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43136	80	192.168.2.23	95.59.181.200
192.168.2.2395.100.207.12150102802027121 05/14/22-02:04:21.836564	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50102	80	192.168.2.23	95.100.207.121
192.168.2.23156.241.14.1325467252869202733 9 05/14/22-02:04:16.821957	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54672	52869	192.168.2.23	156.241.14.132
192.168.2.2395.158.153.18444468802027121 05/14/22-02:05:16.432488	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44468	80	192.168.2.23	95.158.153.184
192.168.2.23172.65.241.2365715655552027153 05/14/22-02:04:39.318465	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	57156	55555	192.168.2.23	172.65.241.236
192.168.2.23156.226.94.1894140652869202733 9 05/14/22-02:05:39.652328	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	41406	52869	192.168.2.23	156.226.94.189
192.168.2.2388.129.188.9241166802027121 05/14/22-02:04:19.399830	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41166	80	192.168.2.23	88.129.188.92
192.168.2.23172.65.166.2240758555552027153 05/14/22-02:05:46.355727	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40758	55555	192.168.2.23	172.65.166.22
192.168.2.2395.183.38.11852836802027121 05/14/22-02:04:50.334131	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52836	80	192.168.2.23	95.183.38.118
192.168.2.2388.135.148.19540620802027121 05/14/22-02:04:55.124093	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40620	80	192.168.2.23	88.135.148.195
192.168.2.23172.65.75.6257084555552027153 05/14/22-02:05:34.766951	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	57084	55555	192.168.2.23	172.65.75.62
192.168.2.23172.65.204.1013832655552027153 05/14/22-02:04:43.912984	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	38326	55555	192.168.2.23	172.65.204.101
192.168.2.2395.180.140.2447310802027121 05/14/22-02:04:36.685245	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47310	80	192.168.2.23	95.180.140.24

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.195.2.157 55260802027121 05/14/22-02:04:04.435272	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55260	80	192.168.2.23	88.195.2.157
192.168.2.2388.151.120.2 3954354802027121 05/14/22-02:04:10.940346	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54354	80	192.168.2.23	88.151.120.239
192.168.2.23172.65.67.90 56662555552027153 05/14/22-02:04:56.047288	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56662	55555	192.168.2.23	172.65.67.90
192.168.2.23172.65.102.5 144754555552027153 05/14/22-02:04:56.030167	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44754	55555	192.168.2.23	172.65.102.51
192.168.2.2395.128.74.80 46640802027121 05/14/22-02:04:17.251115	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46640	80	192.168.2.23	95.128.74.80
192.168.2.23172.65.164.1 748162555552027153 05/14/22-02:04:22.472015	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48162	55555	192.168.2.23	172.65.164.17
192.168.2.2388.83.121.22 158894802027121 05/14/22-02:04:27.640751	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58894	80	192.168.2.23	88.83.121.221
192.168.2.2395.169.219.2 5434272802027121 05/14/22-02:04:45.846183	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34272	80	192.168.2.23	95.169.219.254
192.168.2.23184.105.8.37 36406555552027153 05/14/22-02:05:18.793782	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	36406	55555	192.168.2.23	184.105.8.37
192.168.2.2395.215.97.13 935584802027121 05/14/22-02:04:25.532039	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35584	80	192.168.2.23	95.215.97.139
192.168.2.23156.224.15.1 7039200528692027339 05/14/22-02:04:39.797114	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39200	52869	192.168.2.23	156.224.15.170
192.168.2.2395.213.15.31 51808802027121 05/14/22-02:04:17.286891	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	51808	80	192.168.2.23	95.213.15.31
192.168.2.2388.218.95.11 037924802027121 05/14/22-02:05:28.503764	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37924	80	192.168.2.23	88.218.95.110
192.168.2.2395.252.227.9 960514802027121 05/14/22-02:04:57.392496	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60514	80	192.168.2.23	95.252.227.99
192.168.2.23172.65.167.1 439002555552027153 05/14/22-02:05:09.758951	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39002	55555	192.168.2.23	172.65.167.14
192.168.2.2388.209.80.20 855570802027121 05/14/22-02:03:55.571475	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	55570	80	192.168.2.23	88.209.80.208
192.168.2.23172.245.196. 21055214555552027153 05/14/22-02:05:06.317529	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	55214	55555	192.168.2.23	172.245.196.210
192.168.2.23156.244.77.1 4443746528692027339 05/14/22-02:05:07.644328	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	43746	52869	192.168.2.23	156.244.77.144
192.168.2.2395.56.137.15 542484802027121 05/14/22-02:04:07.907810	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42484	80	192.168.2.23	95.56.137.155

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.252.26.1 4258998528692027339 05/14/22- 02:04:30.267679	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58998	52869	192.168.2.23	156.252.26.142
192.168.2.23172.65.228.1 5633432555552027153 05/14/22- 02:05:45.978228	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33432	55555	192.168.2.23	172.65.228.156
192.168.2.2395.211.109.3 948768802027121 05/14/22- 02:04:57.363312	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48768	80	192.168.2.23	95.211.109.39
192.168.2.2388.215.16.24 440964802027121 05/14/22- 02:05:36.611945	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40964	80	192.168.2.23	88.215.16.244
192.168.2.2388.250.175.2 0859942802027121 05/14/22- 02:05:33.036125	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59942	80	192.168.2.23	88.250.175.208
192.168.2.2388.221.176.2 1437726802027121 05/14/22- 02:05:02.940383	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37726	80	192.168.2.23	88.221.176.214
192.168.2.23156.254.51.1 3348970528692027339 05/14/22- 02:05:53.246860	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48970	52869	192.168.2.23	156.254.51.133
192.168.2.2395.181.217.2 1542428802027121 05/14/22- 02:04:01.013042	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42428	80	192.168.2.23	95.181.217.215
192.168.2.23172.65.149.2 2744978555552027153 05/14/22- 02:03:55.468539	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44978	55555	192.168.2.23	172.65.149.227
192.168.2.2395.100.151.5 036050802027121 05/14/22- 02:05:04.113713	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36050	80	192.168.2.23	95.100.151.50
192.168.2.23156.226.51.2 659756528692027339 05/14/22- 02:03:58.608037	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	59756	52869	192.168.2.23	156.226.51.26
192.168.2.2395.44.136.16 858910802027121 05/14/22- 02:05:06.494711	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58910	80	192.168.2.23	95.44.136.168
192.168.2.23156.245.43.1 833638528692027339 05/14/22- 02:04:34.638673	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33638	52869	192.168.2.23	156.245.43.18
192.168.2.23156.250.92.8 149400528692027339 05/14/22- 02:05:30.387325	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	49400	52869	192.168.2.23	156.250.92.81
192.168.2.2395.101.122.1 2941910802027121 05/14/22- 02:03:57.733650	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41910	80	192.168.2.23	95.101.122.129
192.168.2.2388.198.82.13 638664802027121 05/14/22- 02:04:36.621117	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38664	80	192.168.2.23	88.198.82.136
192.168.2.2388.207.159.1 842422802027121 05/14/22- 02:04:04.430182	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42422	80	192.168.2.23	88.207.159.18
192.168.2.2395.56.213.80 36770802027121 05/14/22- 02:04:50.593818	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36770	80	192.168.2.23	95.56.213.80
192.168.2.2395.159.14.92 36796802027121 05/14/22- 02:04:01.047400	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36796	80	192.168.2.23	95.159.14.92

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.101.58.59 48210802027121 05/14/22-02:05:00.726341	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48210	80	192.168.2.23	95.101.58.59
192.168.2.23172.65.45.60 35894555552027153 05/14/22-02:04:31.062264	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35894	55555	192.168.2.23	172.65.45.60
192.168.2.2395.72.28.184 46380802027121 05/14/22-02:03:57.766923	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46380	80	192.168.2.23	95.72.28.184
192.168.2.23172.65.174.2 055300555552027153 05/14/22-02:03:58.555577	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	55300	55555	192.168.2.23	172.65.174.20
192.168.2.23172.65.2.221 59362555552027153 05/14/22-02:05:09.758996	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59362	55555	192.168.2.23	172.65.2.221
192.168.2.2388.151.120.2 3954256802027121 05/14/22-02:04:07.815463	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54256	80	192.168.2.23	88.151.120.239
192.168.2.2388.221.155.4 942002802027121 05/14/22-02:05:52.526130	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42002	80	192.168.2.23	88.221.155.49
192.168.2.23184.175.126. 5651794555552027153 05/14/22-02:05:04.444249	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51794	55555	192.168.2.23	184.175.126.56
192.168.2.23172.65.85.56 40568555552027153 05/14/22-02:04:07.291997	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40568	55555	192.168.2.23	172.65.85.56
192.168.2.2388.221.137.2 3833006802027121 05/14/22-02:05:25.192641	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33006	80	192.168.2.23	88.221.137.238
192.168.2.2395.101.69.25 058292802027121 05/14/22-02:04:01.004594	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58292	80	192.168.2.23	95.101.69.250
192.168.2.2395.101.188.6 034116802027121 05/14/22-02:04:04.484302	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34116	80	192.168.2.23	95.101.188.60
192.168.2.2388.166.227.1 3336224802027121 05/14/22-02:04:43.350949	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36224	80	192.168.2.23	88.166.227.133
192.168.2.2388.147.126.1 8944674802027121 05/14/22-02:04:45.457773	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44674	80	192.168.2.23	88.147.126.189
192.168.2.23172.65.33.10 843492555552027153 05/14/22-02:03:58.572506	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	43492	55555	192.168.2.23	172.65.33.108
192.168.2.2388.201.64.53 8342802027121 05/14/22-02:04:52.868346	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38342	80	192.168.2.23	88.201.64.5
192.168.2.2388.150.171.7 244640802027121 05/14/22-02:04:09.313085	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44640	80	192.168.2.23	88.150.171.72
192.168.2.2388.99.170.45 33644802027121 05/14/22-02:04:40.769297	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33644	80	192.168.2.23	88.99.170.45
192.168.2.2395.101.63.88 38726802027121 05/14/22-02:04:36.682429	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38726	80	192.168.2.23	95.101.63.88

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.226.106.22449930528692027339 05/14/22-02:03:58.604415	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	49930	52869	192.168.2.23	156.226.106.224
192.168.2.2395.216.51.24245628802027121 05/14/22-02:04:17.265531	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45628	80	192.168.2.23	95.216.51.242
192.168.2.23172.65.200.19256740555552027153 05/14/22-02:05:46.356024	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56740	55555	192.168.2.23	172.65.200.192
192.168.2.2395.87.1.2257834802027121 05/14/22-02:04:34.518726	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57834	80	192.168.2.23	95.87.1.22
192.168.2.2388.99.138.24053168802027121 05/14/22-02:04:43.357808	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53168	80	192.168.2.23	88.99.138.240
192.168.2.23172.65.97.11534182555552027153 05/14/22-02:04:19.382917	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	34182	55555	192.168.2.23	172.65.97.115
192.168.2.23172.65.167.1105902855555202715 3 05/14/22-02:04:34.685648	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59028	55555	192.168.2.23	172.65.167.110
192.168.2.2388.221.227.18053630802027121 05/14/22-02:05:50.047627	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53630	80	192.168.2.23	88.221.227.180
192.168.2.2388.10.175.4242760802027121 05/14/22-02:04:36.714857	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42760	80	192.168.2.23	88.10.175.42
192.168.2.2388.99.214.4635952802027121 05/14/22-02:04:52.770205	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35952	80	192.168.2.23	88.99.214.46
192.168.2.23172.65.211.645023655555202715 3 05/14/22-02:05:06.237219	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	50236	55555	192.168.2.23	172.65.211.64
192.168.2.2395.96.2.1854422802027121 05/14/22-02:05:45.528566	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54422	80	192.168.2.23	95.96.2.18
192.168.2.2395.216.140.24358592802027121 05/14/22-02:04:55.066889	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58592	80	192.168.2.23	95.216.140.243
192.168.2.2388.41.60.1836672802027121 05/14/22-02:04:40.877472	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36672	80	192.168.2.23	88.41.60.18
192.168.2.23156.244.102.115387025286920273 39 05/14/22-02:05:52.813667	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38702	52869	192.168.2.23	156.244.102.115
192.168.2.23172.65.95.3339672555552027153 05/14/22-02:04:04.184416	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39672	55555	192.168.2.23	172.65.95.33
192.168.2.2395.180.146.9351564802027121 05/14/22-02:04:34.515139	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	51564	80	192.168.2.23	95.180.146.93
192.168.2.23172.65.124.3056878555552027153 05/14/22-02:04:39.300441	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56878	55555	192.168.2.23	172.65.124.30
192.168.2.2395.52.241.2750394802027121 05/14/22-02:04:01.045396	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50394	80	192.168.2.23	95.52.241.27
192.168.2.23156.244.73.24855328528692027339 05/14/22-02:05:36.552777	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55328	52869	192.168.2.23	156.244.73.248

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.221.185.19260438802027121 05/14/22-02:04:43.365152	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60438	80	192.168.2.23	88.221.185.192
192.168.2.23172.65.182.9446454555552027153 05/14/22-02:05:33.583579	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	46454	55555	192.168.2.23	172.65.182.94
192.168.2.23172.65.91.11560806555552027153 05/14/22-02:05:37.001586	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60806	55555	192.168.2.23	172.65.91.115
192.168.2.23172.65.57.853936255552027153 05/14/22-02:05:41.244138	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39362	55555	192.168.2.23	172.65.57.85
192.168.2.2388.87.90.24859292802027121 05/14/22-02:04:40.936768	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59292	80	192.168.2.23	88.87.90.248
192.168.2.2398.159.33.227544985555552027153 05/14/22-02:05:24.949664	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	54498	55555	192.168.2.23	98.159.33.227
192.168.2.2388.221.190.7657518802027121 05/14/22-02:04:43.334647	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57518	80	192.168.2.23	88.221.190.76
192.168.2.23172.65.111.1046075455552027153 05/14/22-02:05:30.411524	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60754	55555	192.168.2.23	172.65.111.104
192.168.2.2395.101.251.4640078802027121 05/14/22-02:04:21.759965	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40078	80	192.168.2.23	95.101.251.46
192.168.2.2395.101.188.4252034802027121 05/14/22-02:03:55.661108	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52034	80	192.168.2.23	95.101.188.42
192.168.2.2395.46.155.18954704802027121 05/14/22-02:05:45.538592	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54704	80	192.168.2.23	95.46.155.189
192.168.2.2395.57.137.24547588802027121 05/14/22-02:05:19.828046	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47588	80	192.168.2.23	95.57.137.245
192.168.2.2388.221.127.4059250802027121 05/14/22-02:04:58.556033	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59250	80	192.168.2.23	88.221.127.40
192.168.2.2388.221.35.8157028802027121 05/14/22-02:04:32.325392	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57028	80	192.168.2.23	88.221.35.81
192.168.2.2388.231.21.15459472802027121 05/14/22-02:03:57.843382	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59472	80	192.168.2.23	88.231.21.154
192.168.2.23156.250.126.15040666528692027339 05/14/22-02:05:50.398115	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	40666	52869	192.168.2.23	156.250.126.150
192.168.2.23172.65.233.2344467055552027153 05/14/22-02:04:57.329185	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44670	55555	192.168.2.23	172.65.233.234
192.168.2.2388.99.27.2959630802027121 05/14/22-02:04:04.408250	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59630	80	192.168.2.23	88.99.27.29
192.168.2.2395.180.146.2538416802027121 05/14/22-02:04:30.926544	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38416	80	192.168.2.23	95.180.146.25

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.216.87.15359114802027121 05/14/22-02:03:53.362973	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59114	80	192.168.2.23	95.216.87.153
192.168.2.23172.65.86.641400555552027153 05/14/22-02:04:36.974233	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	41400	55555	192.168.2.23	172.65.86.6
192.168.2.2388.99.6.1533711880202712 1 05/14/22-02:04:57.386875	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37118	80	192.168.2.23	88.99.6.153
192.168.2.2388.34.183.10636654802027121 05/14/22-02:05:33.094042	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36654	80	192.168.2.23	88.34.183.106
192.168.2.2395.168.168.16852616802027121 05/14/22-02:03:57.738061	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52616	80	192.168.2.23	95.168.168.168
192.168.2.2395.183.37.14041168802027121 05/14/22-02:04:17.287353	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41168	80	192.168.2.23	95.183.37.140
192.168.2.2395.216.49.24535130802027121 05/14/22-02:04:57.381704	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35130	80	192.168.2.23	95.216.49.245
192.168.2.2388.99.32.23139366802027121 05/14/22-02:04:29.747000	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39366	80	192.168.2.23	88.99.32.231
192.168.2.2395.223.191.17654308802027121 05/14/22-02:04:00.998864	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54308	80	192.168.2.23	95.223.191.176
192.168.2.2395.142.39.19040324802027121 05/14/22-02:03:53.377984	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40324	80	192.168.2.23	95.142.39.190
192.168.2.2395.100.151.5035770802027121 05/14/22-02:04:55.171540	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35770	80	192.168.2.23	95.100.151.50
192.168.2.23172.65.199.2273499655552027153 05/14/22-02:05:37.018864	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	34996	55555	192.168.2.23	172.65.199.227
192.168.2.23172.65.86.1447446555552027153 05/14/22-02:04:11.654959	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47446	55555	192.168.2.23	172.65.86.14
192.168.2.23156.254.70.1173886052869202733 9 05/14/22-02:05:37.010525	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38860	52869	192.168.2.23	156.254.70.117
192.168.2.23172.65.246.2254933655552027153 05/14/22-02:04:31.062353	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49336	55555	192.168.2.23	172.65.246.225
192.168.2.2388.221.250.12036710802027121 05/14/22-02:04:30.978771	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36710	80	192.168.2.23	88.221.250.120
192.168.2.2388.218.158.14353512802027121 05/14/22-02:04:32.244935	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53512	80	192.168.2.23	88.218.158.143
192.168.2.23172.65.105.8740248555552027153 05/14/22-02:04:31.062442	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40248	55555	192.168.2.23	172.65.105.87
192.168.2.23172.245.113.11138934555552027153 05/14/22-02:04:07.379640	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	38934	55555	192.168.2.23	172.245.113.111

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.193.184.6838586802027121 05/14/22-02:05:47.764684	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38586	80	192.168.2.23	88.193.184.68
192.168.2.2388.151.120.23954648802027121 05/14/22-02:04:19.380599	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54648	80	192.168.2.23	88.151.120.239
192.168.2.23156.240.108.22955326528692027339 05/14/22-02:04:51.841222	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55326	52869	192.168.2.23	156.240.108.229
192.168.2.23156.226.61.773551052869202733 9 05/14/22-02:05:03.298472	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	35510	52869	192.168.2.23	156.226.61.77
192.168.2.23172.245.25.841564555552027153 05/14/22-02:05:04.432633	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	41564	55555	192.168.2.23	172.245.25.8
192.168.2.2388.99.145.7544708802027121 05/14/22-02:05:02.936838	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44708	80	192.168.2.23	88.99.145.75
192.168.2.2395.129.189.1153350802027121 05/14/22-02:04:07.881985	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53350	80	192.168.2.23	95.129.189.11
192.168.2.2388.247.119.14756892802027121 05/14/22-02:04:19.409992	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56892	80	192.168.2.23	88.247.119.147
192.168.2.23172.65.48.24341020555552027153 05/14/22-02:04:43.913081	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	41020	55555	192.168.2.23	172.65.48.243
192.168.2.2395.77.11.1836288802027121 05/14/22-02:05:08.836665	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36288	80	192.168.2.23	95.77.11.18
192.168.2.2395.214.218.12438414802027121 05/14/22-02:04:01.070491	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38414	80	192.168.2.23	95.214.218.124
192.168.2.2395.110.236.2245362802027121 05/14/22-02:04:09.284651	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45362	80	192.168.2.23	95.110.236.22
192.168.2.2395.183.15.22143498802027121 05/14/22-02:04:23.251318	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	43498	80	192.168.2.23	95.183.15.221
192.168.2.23172.65.69.150463805555520271 53 05/14/22-02:05:37.019008	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	46380	55555	192.168.2.23	172.65.69.150
192.168.2.23172.65.116.5734996555552027153 05/14/22-02:04:24.881978	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	34996	55555	192.168.2.23	172.65.116.57
192.168.2.2388.147.144.12557076802027121 05/14/22-02:04:30.883444	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	57076	80	192.168.2.23	88.147.144.125
192.168.2.23172.65.241.9347344555552027153 05/14/22-02:04:57.312233	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47344	55555	192.168.2.23	172.65.241.93
192.168.2.23172.65.132.19643310555552027153 05/14/22-02:05:06.220049	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	43310	55555	192.168.2.23	172.65.132.196
192.168.2.2395.100.182.17258936802027121 05/14/22-02:04:23.192380	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58936	80	192.168.2.23	95.100.182.172

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.201.1803649655555202715305/14/22-02:05:45.978084	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	36496	55555	192.168.2.23	172.65.201.180
192.168.2.2395.86.206.240377328020271215/14/22-02:05:28.581595	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37732	80	192.168.2.23	95.86.206.240
192.168.2.23156.245.59.2344669452869202733905/14/22-02:05:37.070954	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46694	52869	192.168.2.23	156.245.59.234
192.168.2.23172.65.230.263857855555202715305/14/22-02:05:45.960758	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	38578	55555	192.168.2.23	172.65.230.26
192.168.2.2395.142.39.190403328020271215/14/22-02:03:53.460756	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40332	80	192.168.2.23	95.142.39.190
192.168.2.2395.101.10.131455788020271215/14/22-02:04:34.509938	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	45578	80	192.168.2.23	95.101.10.131
192.168.2.2395.111.227.220499748020271215/14/22-02:04:25.535524	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	49974	80	192.168.2.23	95.111.227.220
192.168.2.23172.65.79.233450345555202715305/14/22-02:05:54.037713	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	45034	55555	192.168.2.23	172.65.79.233
192.168.2.23197.44.95.233397925286920273395/14/22-02:05:48.080780	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39792	52869	192.168.2.23	197.44.95.233
192.168.2.2395.101.179.218408348020271215/14/22-02:04:21.731177	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40834	80	192.168.2.23	95.101.179.218
192.168.2.2395.84.209.124441788020271215/14/22-02:04:34.530155	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44178	80	192.168.2.23	95.84.209.124
192.168.2.2388.221.241.166464768020271215/14/22-02:04:45.587757	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46476	80	192.168.2.23	88.221.241.166
192.168.2.23172.65.43.964876255555202715305/14/22-02:04:04.201524	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48762	55555	192.168.2.23	172.65.43.96
192.168.2.23172.65.147.2144500555552027153 05/14/22-02:05:24.831840	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44500	55555	192.168.2.23	172.65.147.21
192.168.2.2388.53.121.22358244802027121 05/14/22-02:05:36.550041	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58244	80	192.168.2.23	88.53.121.223
192.168.2.23172.65.244.1833758055555202715305/14/22-02:05:21.335692	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37580	55555	192.168.2.23	172.65.244.183
192.168.2.2395.217.234.23742976802027121 05/14/22-02:04:45.496386	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42976	80	192.168.2.23	95.217.234.237
192.168.2.2388.22.77.1933586802027121 05/14/22-02:05:16.374618	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33586	80	192.168.2.23	88.22.77.19
192.168.2.23172.245.103.9646626555552027153 05/14/22-02:05:21.142244	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	46626	55555	192.168.2.23	172.245.103.96

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.217.177.21652404802027121 05/14/22-02:04:01.012402	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	52404	80	192.168.2.23	95.217.177.216
192.168.2.2388.217.172.16433898802027121 05/14/22-02:04:32.232576	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	33898	80	192.168.2.23	88.217.172.164
192.168.2.2388.247.4.1542394802027121 05/14/22-02:03:57.818353	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42394	80	192.168.2.23	88.247.4.15
192.168.2.23172.65.190.19056196555552027153 05/14/22-02:05:09.759089	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56196	55555	192.168.2.23	172.65.190.190
192.168.2.2388.99.106.22060562802027121 05/14/22-02:04:21.715165	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60562	80	192.168.2.23	88.99.106.220
192.168.2.2388.221.156.3548314802027121 05/14/22-02:04:58.613996	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48314	80	192.168.2.23	88.221.156.35
192.168.2.2388.255.170.1759020802027121 05/14/22-02:04:37.610970	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59020	80	192.168.2.23	88.255.170.17
192.168.2.23172.65.46.159140555552027153 05/14/22-02:05:16.317135	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	59140	55555	192.168.2.23	172.65.46.1
192.168.2.2395.90.100.25360968802027121 05/14/22-02:04:45.495189	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60968	80	192.168.2.23	95.90.100.253
192.168.2.2395.100.10.2758494802027121 05/14/22-02:05:23.036314	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58494	80	192.168.2.23	95.100.10.27
192.168.2.2388.151.120.23954218802027121 05/14/22-02:04:04.436112	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54218	80	192.168.2.23	88.151.120.239
192.168.2.2395.217.74.2949830802027121 05/14/22-02:04:48.048276	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	49830	80	192.168.2.23	95.217.74.29
192.168.2.23172.65.41.23933628555552027153 05/14/22-02:05:09.761720	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33628	55555	192.168.2.23	172.65.41.239
192.168.2.23172.65.91.6249884555552027153 05/14/22-02:03:52.401161	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	49884	55555	192.168.2.23	172.65.91.62
192.168.2.2395.217.171.18950806802027121 05/14/22-02:05:03.000835	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50806	80	192.168.2.23	95.217.171.189
192.168.2.23172.245.107.23640466555552027153 05/14/22-02:05:04.432766	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40466	55555	192.168.2.23	172.245.107.236
192.168.2.2395.211.48.23437548802027121 05/14/22-02:04:29.723243	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37548	80	192.168.2.23	95.211.48.234
192.168.2.2395.143.49.23841548802027121 05/14/22-02:04:09.265829	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	41548	80	192.168.2.23	95.143.49.238
192.168.2.2395.216.113.23540052802027121 05/14/22-02:04:19.433599	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40052	80	192.168.2.23	95.216.113.235

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.99.250.96 38340802027121 05/14/22-02:03:57.760926	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38340	80	192.168.2.23	88.99.250.96
192.168.2.2395.110.188.5 850186802027121 05/14/22-02:04:21.767738	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50186	80	192.168.2.23	95.110.188.58
192.168.2.23172.65.147.2 4056508555552027153 05/14/22-02:04:15.724140	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	56508	55555	192.168.2.23	172.65.147.240
192.168.2.23172.65.7.173 517178555552027153 05/14/22-02:04:34.703705	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51778	55555	192.168.2.23	172.65.7.173
192.168.2.23172.65.227.1 3246070555552027153 05/14/22-02:05:09.758844	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	46070	55555	192.168.2.23	172.65.227.132
192.168.2.23172.65.94.14 451176555552027153 05/14/22-02:04:19.383126	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51176	55555	192.168.2.23	172.65.94.144
192.168.2.2388.99.0.5634 224802027121 05/14/22-02:04:40.793936	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	34224	80	192.168.2.23	88.99.0.56
192.168.2.23156.245.35.2 0639160528692027339 05/14/22-02:04:01.120042	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39160	52869	192.168.2.23	156.245.35.206
192.168.2.23172.65.203.1 5944186555552027153 05/14/22-02:03:58.555655	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	44186	55555	192.168.2.23	172.65.203.159
192.168.2.23172.65.205.1 6052354555552027153 05/14/22-02:04:49.789360	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	52354	55555	192.168.2.23	172.65.205.160
192.168.2.23156.226.100. 4157032528692027339 05/14/22-02:05:04.864593	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57032	52869	192.168.2.23	156.226.100.41
192.168.2.2395.216.241.2 1038106802027121 05/14/22-02:04:50.438289	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	38106	80	192.168.2.23	95.216.241.210
192.168.2.2388.151.115.2 648772802027121 05/14/22-02:04:09.698765	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48772	80	192.168.2.23	88.151.115.26
192.168.2.2388.248.100.2 1059808802027121 05/14/22-02:04:45.455125	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59808	80	192.168.2.23	88.248.100.210
192.168.2.23172.65.170.2 0642126555552027153 05/14/22-02:05:04.147038	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	42126	55555	192.168.2.23	172.65.170.206
192.168.2.2388.221.247.4 656332802027121 05/14/22-02:05:16.728469	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56332	80	192.168.2.23	88.221.247.46
192.168.2.2395.65.48.224 4716802027121 05/14/22-02:04:23.241574	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	44716	80	192.168.2.23	95.65.48.22
192.168.2.23156.254.86.1 0347550528692027339 05/14/22-02:05:02.793230	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	47550	52869	192.168.2.23	156.254.86.103
192.168.2.23172.65.116.2 4337208555552027153 05/14/22-02:03:58.555471	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	37208	55555	192.168.2.23	172.65.116.243

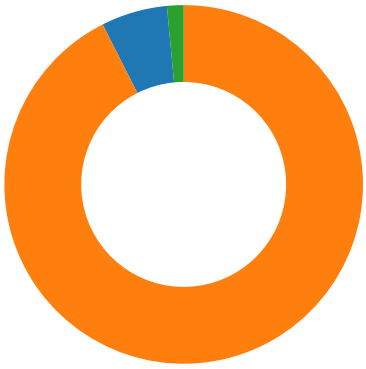
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23172.65.196.122418005555520271535/14/22-02:05:37.001489	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	41800	55555	192.168.2.23	172.65.196.122
192.168.2.2388.151.50.2139518802027121 05/14/22-02:05:23.027466	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39518	80	192.168.2.23	88.151.50.21
192.168.2.2395.245.176.100474588020271215/14/22-02:04:02.312326	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	47458	80	192.168.2.23	95.245.176.100
192.168.2.23156.254.85.2345610528692027339 05/14/22-02:05:12.491233	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	45610	52869	192.168.2.23	156.254.85.23
192.168.2.2388.198.176.12760206802027121 05/14/22-02:04:13.144517	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60206	80	192.168.2.23	88.198.176.127
192.168.2.2388.221.10.20254556802027121 05/14/22-02:04:52.747584	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54556	80	192.168.2.23	88.221.10.202
192.168.2.23172.65.36.175484865555520271535/14/22-02:04:57.312175	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48486	55555	192.168.2.23	172.65.36.175
192.168.2.2388.247.120.10250276802027121 05/14/22-02:05:50.075434	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50276	80	192.168.2.23	88.247.120.102
192.168.2.2388.221.18.13558280802027121 05/14/22-02:04:32.272004	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58280	80	192.168.2.23	88.221.18.135
192.168.2.2395.101.189.5648426802027121 05/14/22-02:03:55.661040	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48426	80	192.168.2.23	95.101.189.56
192.168.2.23172.65.214.1560194555552027153 05/14/22-02:05:20.978194	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60194	55555	192.168.2.23	172.65.214.15
192.168.2.2395.100.77.4953544802027121 05/14/22-02:05:23.001580	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53544	80	192.168.2.23	95.100.77.49
192.168.2.2395.91.29.21342706802027121 05/14/22-02:05:19.755389	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42706	80	192.168.2.23	95.91.29.213
192.168.2.23172.65.97.200516025555520271535/14/22-02:04:34.685570	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51602	55555	192.168.2.23	172.65.97.200
192.168.2.2395.65.25.2359674802027121 05/14/22-02:04:09.303014	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59674	80	192.168.2.23	95.65.25.23
192.168.2.2398.159.33.130422025555520271535/14/22-02:04:46.257949	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	42202	55555	192.168.2.23	98.159.33.130
192.168.2.2388.221.136.7740648802027121 05/14/22-02:04:43.322465	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	40648	80	192.168.2.23	88.221.136.77
192.168.2.2395.101.241.19859824802027121 05/14/22-02:04:43.339295	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59824	80	192.168.2.23	95.101.241.198
192.168.2.2395.216.236.17850606802027121 05/14/22-02:05:45.541757	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	50606	80	192.168.2.23	95.216.236.178

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.148.137.22246540802027121 05/14/22-02:04:40.840279	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	46540	80	192.168.2.23	88.148.137.222
192.168.2.2388.221.138.14732984802027121 05/14/22-02:05:27.261197	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	32984	80	192.168.2.23	88.221.138.147
192.168.2.2395.211.221.12139408802027121 05/14/22-02:04:21.756854	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	39408	80	192.168.2.23	95.211.221.121
192.168.2.2388.226.220.15637282802027121 05/14/22-02:05:04.229140	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	37282	80	192.168.2.23	88.226.220.156
192.168.2.2395.148.139.3154776802027121 05/14/22-02:04:50.437562	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54776	80	192.168.2.23	95.148.139.31
192.168.2.2388.31.6.1135942802027121 05/14/22-02:04:58.535677	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59422	80	192.168.2.23	88.31.6.113
192.168.2.2388.148.49.4251404802027121 05/14/22-02:04:48.007218	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	51404	80	192.168.2.23	88.148.49.42
192.168.2.2388.99.101.20254734802027121 05/14/22-02:04:01.022090	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	54734	80	192.168.2.23	88.99.101.202
192.168.2.23172.65.50.23143836555552027153 05/14/22-02:05:41.244057	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	43836	55555	192.168.2.23	172.65.50.231
192.168.2.2388.202.226.21658762802027121 05/14/22-02:04:32.259524	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58762	80	192.168.2.23	88.202.226.216
192.168.2.23172.65.98.13860678555552027153 05/14/22-02:04:50.716191	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60678	55555	192.168.2.23	172.65.98.138
192.168.2.23172.65.50.684850655555552027153 05/14/22-02:04:13.394170	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	48506	55555	192.168.2.23	172.65.50.68
192.168.2.23172.65.203.9147194555552027153 05/14/22-02:05:18.632714	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	47194	55555	192.168.2.23	172.65.203.91
192.168.2.23172.65.225.2225102855552027153 05/14/22-02:04:31.045044	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	51082	55555	192.168.2.23	172.65.225.222
192.168.2.2395.100.119.3360388802027121 05/14/22-02:04:55.076014	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60388	80	192.168.2.23	95.100.119.33
192.168.2.2388.31.225.15836930802027121 05/14/22-02:04:58.537628	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	36930	80	192.168.2.23	88.31.225.158
192.168.2.2395.219.212.2959618802027121 05/14/22-02:05:00.802432	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	59618	80	192.168.2.23	95.219.212.29
192.168.2.23172.65.20.20039984555552027153 05/14/22-02:05:04.335191	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	39984	55555	192.168.2.23	172.65.20.200
192.168.2.23172.65.105.2004010055555552027153 05/14/22-02:04:46.275094	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	40100	55555	192.168.2.23	172.65.105.200

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.244.78.2 0139706528692027339 05/14/22- 02:05:33.351834	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39706	52869	192.168.2.23	156.244.78.201
192.168.2.23172.65.187.2 835410555552027153 05/14/22- 02:05:43.557994	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	35410	55555	192.168.2.23	172.65.187.28
192.168.2.2362.75.251.60 1461880802404338 05/14/22- 02:04:37.171076	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	14618	8080	192.168.2.23	62.75.251.60
192.168.2.23172.65.190.1 8233602555552027153 05/14/22- 02:05:24.831916	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	33602	55555	192.168.2.23	172.65.190.182
192.168.2.2388.147.251.7 849714802027121 05/14/22- 02:05:52.722920	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	49714	80	192.168.2.23	88.147.251.78
192.168.2.2395.216.247.2 4048722802027121 05/14/22- 02:03:53.362682	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48722	80	192.168.2.23	95.216.247.240
192.168.2.2388.249.57.15 956710802027121 05/14/22- 02:04:55.177371	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	56710	80	192.168.2.23	88.249.57.159
192.168.2.2395.100.222.3 448534802027121 05/14/22- 02:04:57.385948	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	48534	80	192.168.2.23	95.100.222.34
192.168.2.23172.65.1.109 54966555552027153 05/14/22- 02:05:45.960834	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	54966	55555	192.168.2.23	172.65.1.109
192.168.2.2388.79.138.16 058010802027121 05/14/22- 02:04:19.377128	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	58010	80	192.168.2.23	88.79.138.160
192.168.2.2395.100.151.5 035616802027121 05/14/22- 02:04:48.074101	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35616	80	192.168.2.23	95.100.151.50
192.168.2.2395.181.22.15 853724802027121 05/14/22- 02:04:19.574675	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	53724	80	192.168.2.23	95.181.22.158
192.168.2.23172.65.118.4 260148555552027153 05/14/22- 02:04:27.953786	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	60148	55555	192.168.2.23	172.65.118.42
192.168.2.23172.65.103.4 058388555552027153 05/14/22- 02:04:42.995871	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	58388	55555	192.168.2.23	172.65.103.40
192.168.2.23156.226.14.2 4139102528692027339 05/14/22- 02:04:47.287454	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39102	52869	192.168.2.23	156.226.14.241
192.168.2.23172.65.76.18 357028555552027153 05/14/22- 02:05:09.775735	TCP	2027153	ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound	57028	55555	192.168.2.23	172.65.76.183
192.168.2.23156.250.83.8 654350528692027339 05/14/22- 02:05:12.575619	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54350	52869	192.168.2.23	156.250.83.86
192.168.2.2395.100.151.5 035638802027121 05/14/22- 02:04:49.195229	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	35638	80	192.168.2.23	95.100.151.50
192.168.2.2395.56.213.15 642384802027121 05/14/22- 02:04:04.659452	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	42384	80	192.168.2.23	95.56.213.156

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.216.27.10660464802027121 05/14/22-02:04:45.496679	TCP	2027121	ET TROJAN ELF/Mirai Variant UA Outbound (Tsunami)	60464	80	192.168.2.23	95.216.27.106
192.168.2.23156.226.83.13349816528692027339 05/14/22-02:05:07.440596	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	49816	52869	192.168.2.23	156.226.83.133

Network Port Distribution



Total Packets: 67

- 52869 undefined
- 443 (HTTPS)
- 37215 undefined

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:80
- 192.168.0.14:80

System Behavior

Analysis Process: VC3SWrkssz PID: **6223**, Parent PID: **6121**

General

Start time:	02:03:49
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz
Arguments:	/tmp/VC3SWrkssz
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: VC3SWrkssz PID: **6226**, Parent PID: **6223**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz

Copyright Joe Security LLC 2022

Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: VC3SWrkssz PID: **6228**, Parent PID: **6226**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: VC3SWrkssz PID: **6229**, Parent PID: **6226**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: VC3SWrkssz PID: **6231**, Parent PID: **6226**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: VC3SWrkssz PID: **6232**, Parent PID: **6226**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: VC3SWrkssz PID: **6235**, Parent PID: **6226**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: VC3SWrkssz PID: **6236**, Parent PID: **6226**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz

Copyright Joe Security LLC 2022

Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: VC3SWrkssz PID: **6239**, Parent PID: **6226**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: VC3SWrkssz PID: **6241**, Parent PID: **6226**

General

Start time:	02:03:50
Start date:	14/05/2022
Path:	/tmp/VC3SWrkssz
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-binary PID: **6281**, Parent PID: **1477**

General

Start time:	02:05:08
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: **6281**, Parent PID: **1477**

General

Start time:	02:05:08
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: **6281**, Parent PID: **1477**

General

Start time:	02:05:08
Start date:	14/05/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	/usr/libexec/gsd-print-notifications
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Copyright Joe Security LLC 2022

File Activities

File Read

Analysis Process: gsd-print-notifications PID: **6287**, Parent PID: **6281**

General

Start time:	02:05:09
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: **6288**, Parent PID: **6287**

General

Start time:	02:05:09
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: **6288**, Parent PID: **1**

General

Start time:	02:05:09
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: **6311**, Parent PID: **1900**

General

Start time:	02:05:41
Start date:	14/05/2022
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: rm PID: **6311**, Parent PID: **1900**

General

Start time:	02:05:41
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

Copyright Joe Security LLC 2022

File Activities

File Deleted

File Read