

ID: 634910
Sample Name: N0hjaP1acV
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:11:47
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report N0hjaP1acV 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
PCAP (Network Traffic) 5
Memory Dumps 5
Snort Signatures 5
Joe Sandbox Signatures 45
AV Detection 45
Networking 45
Data Obfuscation 46
Hooking and other Techniques for Hiding and Protection 46
Stealing of Sensitive Information 46
Remote Access Functionality 46
Mitre Att&ck Matrix 46
Malware Configuration 46
Behavior Graph 46
Antivirus, Machine Learning and Genetic Malware Detection 47
Initial Sample 47
Dropped Files 47
Domains 47
URLs 47
Domains and IPs 47
Contacted Domains 48
URLs from Memory and Binaries 48
World Map of Contacted IPs 48
Public IPs 48
Joe Sandbox View / Context 50
IPs 50
Domains 51
ASNs 51
JA3 Fingerprints 51
Dropped Files 51
Created / dropped Files 51
Static File Info 51
General 51
Static ELF Info 51
ELF header 51
Program Segments 52
Network Behavior 52
Snort IDS Alerts 52
TCP Packets 68
System Behavior 68
Analysis Process: N0hjaP1acV PID: 6229, Parent PID: 6122 68
General 68
File Activities 68
File Read 68
Analysis Process: N0hjaP1acV PID: 6231, Parent PID: 6229 68
General 68
Analysis Process: N0hjaP1acV PID: 6232, Parent PID: 6229 68
General 68
Analysis Process: N0hjaP1acV PID: 6233, Parent PID: 6229 68
General 68
Analysis Process: N0hjaP1acV PID: 6235, Parent PID: 6229 68
General 69
Analysis Process: N0hjaP1acV PID: 6237, Parent PID: 6229 69
General 69
Analysis Process: N0hjaP1acV PID: 6241, Parent PID: 6229 69
General 69
Analysis Process: N0hjaP1acV PID: 6245, Parent PID: 6241 69
General 69
File Activities 69
File Read 69
Analysis Process: N0hjaP1acV PID: 6256, Parent PID: 6245 69
General 69
Analysis Process: N0hjaP1acV PID: 6258, Parent PID: 6256 69

Copyright Joe Security LLC 2022

General 69
Analysis Process: N0hjaP1acV PID: 6248, Parent PID: 6241 70
General 70
Analysis Process: N0hjaP1acV PID: 6250, Parent PID: 6248 70
General 70

Linux Analysis Report

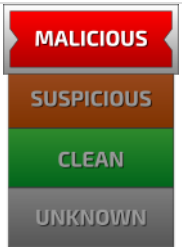
N0hjaP1acV

Overview

General Information

Sample Name:	N0hjaP1acV
Analysis ID:	634910
MD5:	ee14dc420ebe8f..
SHA1:	8b3d7ca9d831a9..
SHA256:	30f9ae9beb37d5..
Tags:	32 elf mips mirai
Infos:	

Detection



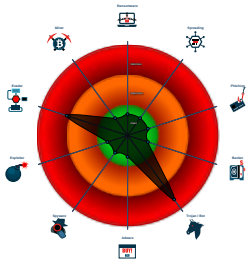
Mirai

Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Sample is packed with UPX
- Uses known network protocols on n…
- Connects to many ports of the same…
- Sample contains only a LOAD segm…
- Yara signature match
- HTTP GET or POST without a user …
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…

Classification



Analysis Advice

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

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

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:	634910
Start date and time: 27/05/202202:11:47	2022-05-27 02:11:47 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	N0hjaP1acV
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:	mal84.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/N0hjaP1acV
PID:	6229
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected

Copyright Joe Security LLC 2022

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- N0hjaP1acV (PID: 6229, Parent: 6122, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/N0hjaP1acV
  - N0hjaP1acV New Fork (PID: 6231, Parent: 6229)
  - N0hjaP1acV New Fork (PID: 6232, Parent: 6229)
  - N0hjaP1acV New Fork (PID: 6233, Parent: 6229)
  - N0hjaP1acV New Fork (PID: 6235, Parent: 6229)
  - N0hjaP1acV New Fork (PID: 6237, Parent: 6229)
  - N0hjaP1acV New Fork (PID: 6241, Parent: 6229)
    - N0hjaP1acV New Fork (PID: 6245, Parent: 6241)
      - N0hjaP1acV New Fork (PID: 6256, Parent: 6245)
        - N0hjaP1acV New Fork (PID: 6258, Parent: 6256)
    - N0hjaP1acV New Fork (PID: 6248, Parent: 6241)
      - N0hjaP1acV New Fork (PID: 6250, Parent: 6248)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
N0hjaP1acV	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0xad78:$s1: PROT_EXEC\|PROT_WRITE failed. • 0xade7:$s2: $Id: UPX • 0xad98:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
6256.1.0000000046947e86.000000002687ffb5.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6248.1.0000000046947e86.000000002687ffb5.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6241.1.0000000046947e86.000000002687ffb5.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6229.1.0000000046947e86.000000002687ffb5.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6245.1.0000000046947e86.000000002687ffb5.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Snort Signatures

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.224.14.79

Timestamp:	192.168.2.23156.224.14.7950618528692027339 05/27/22-02:13:58.105252
SID:	2027339
Source Port:	50618
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: 156.226.61.65

Timestamp:	192.168.2.23156.226.61.6557204528692027339 05/27/22-02:16:04.924108
SID:	2027339

Copyright Joe Security LLC 2022

Source Port:	57204
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: 156.235.98.202

Timestamp:	192.168.2.23156.235.98.20249046528692027339 05/27/22-02:14:35.444891
SID:	2027339
Source Port:	49046
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: 156.241.74.220

Timestamp:	192.168.2.23156.241.74.22046262528692027339 05/27/22-02:14:36.677860
SID:	2027339
Source Port:	46262
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: 156.241.84.115

Timestamp:	192.168.2.23156.241.84.11541430528692027339 05/27/22-02:13:56.668282
SID:	2027339
Source Port:	41430
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: 156.227.240.97

Timestamp:	192.168.2.23156.227.240.9754036528692027339 05/27/22-02:13:49.289658
SID:	2027339
Source Port:	54036
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: 156.224.22.38

Timestamp:	192.168.2.23156.224.22.3855960528692027339 05/27/22-02:14:36.626878
SID:	2027339
Source Port:	55960
Destination Port:	52869
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: 156.225.138.90

Timestamp:	192.168.2.23156.225.138.9042848372152835222 05/27/22-02:15:11.674046
SID:	2835222
Source Port:	42848
Destination Port:	37215
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: 156.244.71.10

Timestamp:	192.168.2.23156.244.71.1035844528692027339 05/27/22-02:12:54.856801
SID:	2027339
Source Port:	35844
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.250.14.21	
Timestamp:	192.168.2.23156.250.14.2143682528692027339 05/27/22-02:15:25.586143
SID:	2027339
Source Port:	43682
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: 156.224.9.163	
Timestamp:	192.168.2.23156.224.9.16347384528692027339 05/27/22-02:14:57.144519
SID:	2027339
Source Port:	47384
Destination Port:	52869
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: 156.238.48.26	
Timestamp:	192.168.2.23156.238.48.2654720372152835222 05/27/22-02:13:39.144497
SID:	2835222
Source Port:	54720
Destination Port:	37215
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: 156.238.46.158	
Timestamp:	192.168.2.23156.238.46.15837544528692027339 05/27/22-02:15:35.761225
SID:	2027339
Source Port:	37544
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: 156.245.60.155	
Timestamp:	192.168.2.23156.245.60.15545062528692027339 05/27/22-02:14:40.059383
SID:	2027339
Source Port:	45062
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: 156.238.49.159	
Timestamp:	192.168.2.23156.238.49.15951956528692027339 05/27/22-02:14:00.916205
SID:	2027339
Source Port:	51956
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: 156.225.143.185	
Timestamp:	192.168.2.23156.225.143.18546852528692027339 05/27/22-02:15:44.829670
SID:	2027339
Source Port:	46852
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: 156.241.116.80	
Timestamp:	192.168.2.23156.241.116.8035674528692027339 05/27/22-02:14:37.094245
SID:	2027339
Source Port:	35674

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: 156.226.82.142

Timestamp:	192.168.2.23156.226.82.14242758528692027339 05/27/22-02:12:55.926001
SID:	2027339
Source Port:	42758
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: 156.226.96.226

Timestamp:	192.168.2.23156.226.96.22646198528692027339 05/27/22-02:13:10.956619
SID:	2027339
Source Port:	46198
Destination Port:	52869
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: 156.244.71.36

Timestamp:	192.168.2.23156.244.71.36470223372152835222 05/27/22-02:13:23.331351
SID:	2835222
Source Port:	47022
Destination Port:	37215
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: 156.244.123.9

Timestamp:	192.168.2.23156.244.123.935674528692027339 05/27/22-02:14:50.971307
SID:	2027339
Source Port:	35674
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: 156.244.105.89

Timestamp:	192.168.2.23156.244.105.8957578528692027339 05/27/22-02:15:32.707694
SID:	2027339
Source Port:	57578
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: 156.254.59.97

Timestamp:	192.168.2.23156.254.59.9749196528692027339 05/27/22-02:12:56.166673
SID:	2027339
Source Port:	49196
Destination Port:	52869
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: 156.240.106.147

Timestamp:	192.168.2.23156.240.106.14755106372152835222 05/27/22-02:14:29.271383
SID:	2835222
Source Port:	55106
Destination Port:	37215
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: 156.244.87.226	
Timestamp:	192.168.2.23156.244.87.22641980528692027339 05/27/22-02:14:29.289410
SID:	2027339
Source Port:	41980
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: 156.225.159.90	
Timestamp:	192.168.2.23156.225.159.9053200528692027339 05/27/22-02:15:26.120158
SID:	2027339
Source Port:	53200
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: 156.247.27.253	
Timestamp:	192.168.2.23156.247.27.25357938528692027339 05/27/22-02:13:53.102906
SID:	2027339
Source Port:	57938
Destination Port:	52869
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: 156.245.61.25	
Timestamp:	192.168.2.23156.245.61.2542128372152835222 05/27/22-02:14:49.510258
SID:	2835222
Source Port:	42128
Destination Port:	37215
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: 156.254.91.28	
Timestamp:	192.168.2.23156.254.91.2855614528692027339 05/27/22-02:14:18.676105
SID:	2027339
Source Port:	55614
Destination Port:	52869
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: 156.224.10.82	
Timestamp:	192.168.2.23156.224.10.82427463721528352222 05/27/22-02:13:33.105779
SID:	2835222
Source Port:	42746
Destination Port:	37215
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: 156.254.84.162	
Timestamp:	192.168.2.23156.254.84.162602583721528352222 05/27/22-02:15:47.741844
SID:	2835222
Source Port:	60258
Destination Port:	37215
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: 41.78.123.1	
Timestamp:	192.168.2.2341.78.123.148548528692027339 05/27/22-02:13:21.096567
SID:	2027339
Source Port:	48548

Destination Port:	52869
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: 156.239.155.158	
Timestamp:	192.168.2.23156.239.155.15857160372152835222 05/27/22-02:14:46.840933
SID:	2835222
Source Port:	57160
Destination Port:	37215
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: 156.226.77.187	
Timestamp:	192.168.2.23156.226.77.18754816372152835222 05/27/22-02:15:44.742124
SID:	2835222
Source Port:	54816
Destination Port:	37215
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: 156.226.108.99	
Timestamp:	192.168.2.23156.226.108.99437185286920273339 05/27/22-02:12:43.189218
SID:	2027339
Source Port:	43718
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: 156.254.52.190	
Timestamp:	192.168.2.23156.254.52.19033086528692027339 05/27/22-02:13:35.255592
SID:	2027339
Source Port:	33086
Destination Port:	52869
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: 156.250.86.121	
Timestamp:	192.168.2.23156.250.86.12138606372152835222 05/27/22-02:14:39.009848
SID:	2835222
Source Port:	38606
Destination Port:	37215
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: 156.250.126.238	
Timestamp:	192.168.2.23156.250.126.23844746528692027339 05/27/22-02:15:02.150467
SID:	2027339
Source Port:	44746
Destination Port:	52869
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: 156.244.81.63	
Timestamp:	192.168.2.23156.244.81.6340236372152835222 05/27/22-02:15:19.372629
SID:	2835222
Source Port:	40236
Destination Port:	37215
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: 156.226.56.10	
Timestamp:	192.168.2.23156.226.56.1052602372152835222 05/27/22-02:12:54.824351
SID:	2835222
Source Port:	52602
Destination Port:	37215
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: 197.234.54.143	
Timestamp:	192.168.2.23197.234.54.14351348372152835222 05/27/22-02:16:02.763420
SID:	2835222
Source Port:	51348
Destination Port:	37215
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: 156.238.46.42	
Timestamp:	192.168.2.23156.238.46.4234500528692027339 05/27/22-02:15:27.951216
SID:	2027339
Source Port:	34500
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: 156.226.91.153	
Timestamp:	192.168.2.23156.226.91.15335422528692027339 05/27/22-02:12:57.071160
SID:	2027339
Source Port:	35422
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: 156.244.112.81	
Timestamp:	192.168.2.23156.244.112.8149114528692027339 05/27/22-02:14:02.928791
SID:	2027339
Source Port:	49114
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: 156.254.78.100	
Timestamp:	192.168.2.23156.254.78.10032836528692027339 05/27/22-02:14:14.336004
SID:	2027339
Source Port:	32836
Destination Port:	52869
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: 156.254.97.108	
Timestamp:	192.168.2.23156.254.97.10846336372152835222 05/27/22-02:15:58.248205
SID:	2835222
Source Port:	46336
Destination Port:	37215
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: 156.230.29.64	
Timestamp:	192.168.2.23156.230.29.64451743721528352222 05/27/22-02:13:57.768233
SID:	2835222
Source Port:	45174

Destination Port:	37215
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: 156.241.110.12

Timestamp:	192.168.2.23156.241.110.1256560528692027339 05/27/22-02:15:46.756882
SID:	2027339
Source Port:	56560
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: 156.241.75.0

Timestamp:	192.168.2.23156.241.75.035466528692027339 05/27/22-02:13:10.915908
SID:	2027339
Source Port:	35466
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: 156.226.92.229

Timestamp:	192.168.2.23156.226.92.22957968528692027339 05/27/22-02:14:25.235370
SID:	2027339
Source Port:	57968
Destination Port:	52869
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: 156.241.74.111

Timestamp:	192.168.2.23156.241.74.11139380372152835222 05/27/22-02:14:17.492006
SID:	2835222
Source Port:	39380
Destination Port:	37215
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: 156.241.79.46

Timestamp:	192.168.2.23156.241.79.4638264528692027339 05/27/22-02:12:53.354886
SID:	2027339
Source Port:	38264
Destination Port:	52869
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: 156.244.115.139

Timestamp:	192.168.2.23156.244.115.13956778372152835222 05/27/22-02:13:45.586935
SID:	2835222
Source Port:	56778
Destination Port:	37215
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: 156.247.27.77

Timestamp:	192.168.2.23156.247.27.7743950528692027339 05/27/22-02:14:48.265097
SID:	2027339
Source Port:	43950
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: 156.254.53.4	
Timestamp:	192.168.2.23156.254.53.439590528692027339 05/27/22-02:14:50.766924
SID:	2027339
Source Port:	39590
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: 156.225.133.35	
Timestamp:	192.168.2.23156.225.133.3557720528692027339 05/27/22-02:15:41.275652
SID:	2027339
Source Port:	57720
Destination Port:	52869
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: 156.241.76.131	
Timestamp:	192.168.2.23156.241.76.13138880372152835222 05/27/22-02:13:29.292236
SID:	2835222
Source Port:	38880
Destination Port:	37215
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: 156.226.80.57	
Timestamp:	192.168.2.23156.226.80.5734018528692027339 05/27/22-02:13:52.173426
SID:	2027339
Source Port:	34018
Destination Port:	52869
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: 156.232.94.195	
Timestamp:	192.168.2.23156.232.94.19548476372152835222 05/27/22-02:15:58.177549
SID:	2835222
Source Port:	48476
Destination Port:	37215
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: 156.238.54.156	
Timestamp:	192.168.2.23156.238.54.15656814528692027339 05/27/22-02:13:52.850974
SID:	2027339
Source Port:	56814
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: 156.239.152.119	
Timestamp:	192.168.2.23156.239.152.11950524528692027339 05/27/22-02:15:30.191969
SID:	2027339
Source Port:	50524
Destination Port:	52869
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: 156.241.66.209	
Timestamp:	192.168.2.23156.241.66.20950904372152835222 05/27/22-02:15:47.269657
SID:	2835222
Source Port:	50904

Destination Port:	37215
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: 156.235.111.139

Timestamp:	192.168.2.23156.235.111.13948572372152835222 05/27/22-02:15:58.658252
SID:	2835222
Source Port:	48572
Destination Port:	37215
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: 156.227.240.129

Timestamp:	192.168.2.23156.227.240.12943716528692027339 05/27/22-02:13:38.769973
SID:	2027339
Source Port:	43716
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: 156.225.139.63

Timestamp:	192.168.2.23156.225.139.63453705286920273339 05/27/22-02:13:01.828686
SID:	2027339
Source Port:	45370
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: 156.241.115.176

Timestamp:	192.168.2.23156.241.115.176586285286920273339 05/27/22-02:15:29.598619
SID:	2027339
Source Port:	58628
Destination Port:	52869
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: 156.245.60.153

Timestamp:	192.168.2.23156.245.60.15346750372152835222 05/27/22-02:13:24.130514
SID:	2835222
Source Port:	46750
Destination Port:	37215
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: 156.239.152.241

Timestamp:	192.168.2.23156.239.152.24145346528692027339 05/27/22-02:13:27.364885
SID:	2027339
Source Port:	45346
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: 156.241.82.219

Timestamp:	192.168.2.23156.241.82.21942842528692027339 05/27/22-02:13:59.432040
SID:	2027339
Source Port:	42842
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.225.159.75	
Timestamp:	192.168.2.23156.225.159.7533144528692027339 05/27/22-02:16:02.376255
SID:	2027339
Source Port:	33144
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: 156.254.49.101	
Timestamp:	192.168.2.23156.254.49.10155184528692027339 05/27/22-02:13:23.358713
SID:	2027339
Source Port:	55184
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: 156.226.103.99	
Timestamp:	192.168.2.23156.226.103.9948840528692027339 05/27/22-02:13:52.855377
SID:	2027339
Source Port:	48840
Destination Port:	52869
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: 156.241.79.239	
Timestamp:	192.168.2.23156.241.79.23948044372152835222 05/27/22-02:14:15.506746
SID:	2835222
Source Port:	48044
Destination Port:	37215
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: 156.225.155.216	
Timestamp:	192.168.2.23156.225.155.21634766528692027339 05/27/22-02:14:09.609403
SID:	2027339
Source Port:	34766
Destination Port:	52869
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: 156.235.98.157	
Timestamp:	192.168.2.23156.235.98.15754100372152835222 05/27/22-02:14:50.692622
SID:	2835222
Source Port:	54100
Destination Port:	37215
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: 156.235.102.82	
Timestamp:	192.168.2.23156.235.102.8256764372152835222 05/27/22-02:12:48.708918
SID:	2835222
Source Port:	56764
Destination Port:	37215
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: 156.244.75.37	
Timestamp:	192.168.2.23156.244.75.37600123721528352222 05/27/22-02:13:33.140390
SID:	2835222
Source Port:	60012

Destination Port:	37215
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: 156.226.108.16

Timestamp:	192.168.2.23156.226.108.1634146528692027339 05/27/22-02:15:33.429510
SID:	2027339
Source Port:	34146
Destination Port:	52869
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: 156.241.99.112

Timestamp:	192.168.2.23156.241.99.11246524372152835222 05/27/22-02:14:22.250710
SID:	2835222
Source Port:	46524
Destination Port:	37215
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: 156.250.113.213

Timestamp:	192.168.2.23156.250.113.21339116528692027339 05/27/22-02:13:04.328886
SID:	2027339
Source Port:	39116
Destination Port:	52869
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: 156.226.78.146

Timestamp:	192.168.2.23156.226.78.14639698372152835222 05/27/22-02:13:36.843203
SID:	2835222
Source Port:	39698
Destination Port:	37215
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: 156.227.245.168

Timestamp:	192.168.2.23156.227.245.16853588528692027339 05/27/22-02:15:23.400250
SID:	2027339
Source Port:	53588
Destination Port:	52869
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: 156.241.89.156

Timestamp:	192.168.2.23156.241.89.15641022372152835222 05/27/22-02:13:15.717127
SID:	2835222
Source Port:	41022
Destination Port:	37215
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: 156.226.63.85

Timestamp:	192.168.2.23156.226.63.8542466528692027339 05/27/22-02:13:38.710756
SID:	2027339
Source Port:	42466
Destination Port:	52869
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 156.226.102.113	
Timestamp:	192.168.2.23156.226.102.11344524372152835222 05/27/22-02:15:36.796853
SID:	2835222
Source Port:	44524
Destination Port:	37215
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: 156.254.60.168	
Timestamp:	192.168.2.23156.254.60.16839394528692027339 05/27/22-02:13:19.454012
SID:	2027339
Source Port:	39394
Destination Port:	52869
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: 156.245.60.34	
Timestamp:	192.168.2.23156.245.60.3440268372152835222 05/27/22-02:13:22.309987
SID:	2835222
Source Port:	40268
Destination Port:	37215
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: 156.238.61.110	
Timestamp:	192.168.2.23156.238.61.11047844528692027339 05/27/22-02:13:31.890200
SID:	2027339
Source Port:	47844
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: 156.230.26.230	
Timestamp:	192.168.2.23156.230.26.23059828528692027339 05/27/22-02:15:29.650636
SID:	2027339
Source Port:	59828
Destination Port:	52869
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: 156.250.95.135	
Timestamp:	192.168.2.23156.250.95.13541928372152835222 05/27/22-02:15:55.855853
SID:	2835222
Source Port:	41928
Destination Port:	37215
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: 156.244.103.201	
Timestamp:	192.168.2.23156.244.103.20155744372152835222 05/27/22-02:13:30.822378
SID:	2835222
Source Port:	55744
Destination Port:	37215
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: 156.232.89.112	
Timestamp:	192.168.2.23156.232.89.11239742528692027339 05/27/22-02:16:03.547915
SID:	2027339
Source Port:	39742

Destination Port:	52869
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: 156.245.52.216	
Timestamp:	192.168.2.23156.245.52.21637384372152835222 05/27/22-02:13:57.603579
SID:	2835222
Source Port:	37384
Destination Port:	37215
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: 156.250.124.111	
Timestamp:	192.168.2.23156.250.124.111331523721528352222 05/27/22-02:14:34.749820
SID:	2835222
Source Port:	33152
Destination Port:	37215
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: 156.254.34.170	
Timestamp:	192.168.2.23156.254.34.17034528528692027339 05/27/22-02:14:56.885248
SID:	2027339
Source Port:	34528
Destination Port:	52869
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: 156.245.54.140	
Timestamp:	192.168.2.23156.245.54.14049164372152835222 05/27/22-02:13:24.836193
SID:	2835222
Source Port:	49164
Destination Port:	37215
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: 156.238.32.38	
Timestamp:	192.168.2.23156.238.32.38458863721528352222 05/27/22-02:14:00.364163
SID:	2835222
Source Port:	45886
Destination Port:	37215
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: 156.241.95.87	
Timestamp:	192.168.2.23156.241.95.8757264372152835222 05/27/22-02:15:19.224623
SID:	2835222
Source Port:	57264
Destination Port:	37215
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: 156.244.107.95	
Timestamp:	192.168.2.23156.244.107.9559450528692027339 05/27/22-02:12:46.370080
SID:	2027339
Source Port:	59450
Destination Port:	52869
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: 156.230.24.131	
Timestamp:	192.168.2.23156.230.24.13137042372152835222 05/27/22-02:16:06.079051
SID:	2835222
Source Port:	37042
Destination Port:	37215
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: 156.235.104.141	
Timestamp:	192.168.2.23156.235.104.14141364372152835222 05/27/22-02:14:07.440368
SID:	2835222
Source Port:	41364
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.246.193.41	
Timestamp:	192.168.2.23197.246.193.4154768372152835222 05/27/22-02:14:18.135266
SID:	2835222
Source Port:	54768
Destination Port:	37215
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: 156.230.30.193	
Timestamp:	192.168.2.23156.230.30.19348628372152835222 05/27/22-02:13:14.410059
SID:	2835222
Source Port:	48628
Destination Port:	37215
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: 156.241.91.74	
Timestamp:	192.168.2.23156.241.91.7440776372152835222 05/27/22-02:12:44.206867
SID:	2835222
Source Port:	40776
Destination Port:	37215
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: 156.226.60.8	
Timestamp:	192.168.2.23156.226.60.858916372152835222 05/27/22-02:13:06.892359
SID:	2835222
Source Port:	58916
Destination Port:	37215
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: 156.241.74.235	
Timestamp:	192.168.2.23156.241.74.23548190528692027339 05/27/22-02:13:26.081860
SID:	2027339
Source Port:	48190
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: 156.244.99.232	
Timestamp:	192.168.2.23156.244.99.23254506528692027339 05/27/22-02:14:08.659215
SID:	2027339
Source Port:	54506

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: 156.245.48.141	
Timestamp:	192.168.2.23156.245.48.14135426528692027339 05/27/22-02:12:50.304313
SID:	2027339
Source Port:	35426
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: 156.235.97.34	
Timestamp:	192.168.2.23156.235.97.3437308528692027339 05/27/22-02:12:59.940810
SID:	2027339
Source Port:	37308
Destination Port:	52869
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: 156.244.88.176	
Timestamp:	192.168.2.23156.244.88.17641590372152835222 05/27/22-02:15:56.186019
SID:	2835222
Source Port:	41590
Destination Port:	37215
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: 156.250.15.25	
Timestamp:	192.168.2.23156.250.15.2547450528692027339 05/27/22-02:13:49.655052
SID:	2027339
Source Port:	47450
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: 156.224.29.180	
Timestamp:	192.168.2.23156.224.29.18044182528692027339 05/27/22-02:14:53.146841
SID:	2027339
Source Port:	44182
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: 156.226.85.26	
Timestamp:	192.168.2.23156.226.85.2660200528692027339 05/27/22-02:12:57.635007
SID:	2027339
Source Port:	60200
Destination Port:	52869
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: 156.225.132.194	
Timestamp:	192.168.2.23156.225.132.19453538372152835222 05/27/22-02:14:15.265038
SID:	2835222
Source Port:	53538
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 156.250.88.124	
Timestamp:	192.168.2.23156.250.88.12440016372152835222 05/27/22-02:12:51.593923
SID:	2835222
Source Port:	40016
Destination Port:	37215
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: 156.244.97.231	
Timestamp:	192.168.2.23156.244.97.23148260372152835222 05/27/22-02:14:22.025068
SID:	2835222
Source Port:	48260
Destination Port:	37215
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: 156.226.14.12	
Timestamp:	192.168.2.23156.226.14.1233270528692027339 05/27/22-02:14:00.689986
SID:	2027339
Source Port:	33270
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: 41.0.84.77	
Timestamp:	192.168.2.2341.0.84.7736524528692027339 05/27/22-02:14:50.212272
SID:	2027339
Source Port:	36524
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: 156.238.61.225	
Timestamp:	192.168.2.23156.238.61.22551084528692027339 05/27/22-02:14:54.636072
SID:	2027339
Source Port:	51084
Destination Port:	52869
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: 156.241.106.95	
Timestamp:	192.168.2.23156.241.106.9537216372152835222 05/27/22-02:13:44.364053
SID:	2835222
Source Port:	37216
Destination Port:	37215
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: 156.225.132.208	
Timestamp:	192.168.2.23156.225.132.20852444528692027339 05/27/22-02:14:02.725896
SID:	2027339
Source Port:	52444
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: 156.245.51.40	
Timestamp:	192.168.2.23156.245.51.4044368528692027339 05/27/22-02:15:28.190347
SID:	2027339
Source Port:	44368

Destination Port:	52869
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: 156.241.73.26

Timestamp:	192.168.2.23156.241.73.2647476372152835222 05/27/22-02:15:29.455772
SID:	2835222
Source Port:	47476
Destination Port:	37215
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: 156.226.70.214

Timestamp:	192.168.2.23156.226.70.21457858528692027339 05/27/22-02:15:25.590511
SID:	2027339
Source Port:	57858
Destination Port:	52869
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: 156.241.10.40

Timestamp:	192.168.2.23156.241.10.40505783721528352222 05/27/22-02:13:29.590300
SID:	2835222
Source Port:	50578
Destination Port:	37215
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: 156.224.29.173

Timestamp:	192.168.2.23156.224.29.17353380372152835222 05/27/22-02:13:45.539483
SID:	2835222
Source Port:	53380
Destination Port:	37215
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: 156.224.23.92

Timestamp:	192.168.2.23156.224.23.9258526372152835222 05/27/22-02:13:24.790368
SID:	2835222
Source Port:	58526
Destination Port:	37215
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: 156.226.94.87

Timestamp:	192.168.2.23156.226.94.8759650372152835222 05/27/22-02:14:18.028243
SID:	2835222
Source Port:	59650
Destination Port:	37215
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: 156.225.136.124

Timestamp:	192.168.2.23156.225.136.12443902372152835222 05/27/22-02:15:26.194360
SID:	2835222
Source Port:	43902
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 156.238.54.168	
Timestamp:	192.168.2.23156.238.54.16845118372152835222 05/27/22-02:14:18.028002
SID:	2835222
Source Port:	45118
Destination Port:	37215
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: 156.226.69.46	
Timestamp:	192.168.2.23156.226.69.4648562372152835222 05/27/22-02:13:04.054928
SID:	2835222
Source Port:	48562
Destination Port:	37215
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: 156.241.68.40	
Timestamp:	192.168.2.23156.241.68.4039378372152835222 05/27/22-02:13:23.904907
SID:	2835222
Source Port:	39378
Destination Port:	37215
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: 156.244.123.215	
Timestamp:	192.168.2.23156.244.123.21541922528692027339 05/27/22-02:13:00.537684
SID:	2027339
Source Port:	41922
Destination Port:	52869
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: 156.238.51.75	
Timestamp:	192.168.2.23156.238.51.7551070372152835222 05/27/22-02:13:49.473187
SID:	2835222
Source Port:	51070
Destination Port:	37215
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: 156.244.71.251	
Timestamp:	192.168.2.23156.244.71.25145106372152835222 05/27/22-02:15:24.727191
SID:	2835222
Source Port:	45106
Destination Port:	37215
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: 156.232.90.70	
Timestamp:	192.168.2.23156.232.90.7048948528692027339 05/27/22-02:16:03.715684
SID:	2027339
Source Port:	48948
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: 156.235.98.63	
Timestamp:	192.168.2.23156.235.98.6352232528692027339 05/27/22-02:14:31.680197
SID:	2027339
Source Port:	52232

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: 156.226.71.88

Timestamp:	192.168.2.23156.226.71.8852088528692027339 05/27/22-02:15:08.130201
SID:	2027339
Source Port:	52088
Destination Port:	52869
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: 156.254.54.197

Timestamp:	192.168.2.23156.254.54.19744280372152835222 05/27/22-02:14:52.946969
SID:	2835222
Source Port:	44280
Destination Port:	37215
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: 156.250.12.0

Timestamp:	192.168.2.23156.250.12.0366323723152835222 05/27/22-02:13:03.624342
SID:	2835222
Source Port:	36632
Destination Port:	37215
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: 156.250.8.55

Timestamp:	192.168.2.23156.250.8.5546794528692027339 05/27/22-02:16:01.823422
SID:	2027339
Source Port:	46794
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: 156.244.70.59

Timestamp:	192.168.2.23156.244.70.5951892528692027339 05/27/22-02:12:43.767721
SID:	2027339
Source Port:	51892
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: 156.241.125.55

Timestamp:	192.168.2.23156.241.125.5538080528692027339 05/27/22-02:13:56.593665
SID:	2027339
Source Port:	38080
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: 156.235.96.85

Timestamp:	192.168.2.23156.235.96.8544686528692027339 05/27/22-02:14:39.577991
SID:	2027339
Source Port:	44686
Destination Port:	52869
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: 156.241.79.200	
Timestamp:	192.168.2.23156.241.79.20055110372152835222 05/27/22-02:13:33.332911
SID:	2835222
Source Port:	55110
Destination Port:	37215
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: 156.227.247.30	
Timestamp:	192.168.2.23156.227.247.3046224528692027339 05/27/22-02:15:17.885570
SID:	2027339
Source Port:	46224
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: 156.250.116.49	
Timestamp:	192.168.2.23156.250.116.4956468528692027339 05/27/22-02:15:59.528866
SID:	2027339
Source Port:	56468
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: 156.226.67.60	
Timestamp:	192.168.2.23156.226.67.6038562528692027339 05/27/22-02:15:49.696382
SID:	2027339
Source Port:	38562
Destination Port:	52869
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: 156.240.109.206	
Timestamp:	192.168.2.23156.240.109.20643920372152835222 05/27/22-02:12:42.296506
SID:	2835222
Source Port:	43920
Destination Port:	37215
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: 156.241.125.225	
Timestamp:	192.168.2.23156.241.125.22534114528692027339 05/27/22-02:13:00.075937
SID:	2027339
Source Port:	34114
Destination Port:	52869
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: 156.244.111.223	
Timestamp:	192.168.2.23156.244.111.22336972372152835222 05/27/22-02:14:51.973133
SID:	2835222
Source Port:	36972
Destination Port:	37215
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: 156.227.244.163	
Timestamp:	192.168.2.23156.227.244.16356848372152835222 05/27/22-02:14:51.959326
SID:	2835222
Source Port:	56848

Destination Port:	37215
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: 156.254.91.206	
Timestamp:	192.168.2.23156.254.91.20635914372152835222 05/27/22-02:14:39.039040
SID:	2835222
Source Port:	35914
Destination Port:	37215
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: 156.244.109.199	
Timestamp:	192.168.2.23156.244.109.19948556372152835222 05/27/22-02:14:22.555051
SID:	2835222
Source Port:	48556
Destination Port:	37215
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: 156.241.100.156	
Timestamp:	192.168.2.23156.241.100.15653238528692027339 05/27/22-02:14:06.366393
SID:	2027339
Source Port:	53238
Destination Port:	52869
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: 156.226.49.163	
Timestamp:	192.168.2.23156.226.49.16350578372152835222 05/27/22-02:15:29.431320
SID:	2835222
Source Port:	50578
Destination Port:	37215
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: 156.254.97.171	
Timestamp:	192.168.2.23156.254.97.17148168372152835222 05/27/22-02:15:39.488038
SID:	2835222
Source Port:	48168
Destination Port:	37215
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: 156.226.106.167	
Timestamp:	192.168.2.23156.226.106.16754500528692027339 05/27/22-02:15:20.331149
SID:	2027339
Source Port:	54500
Destination Port:	52869
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: 156.241.79.134	
Timestamp:	192.168.2.23156.241.79.13455592372152835222 05/27/22-02:13:17.995176
SID:	2835222
Source Port:	55592
Destination Port:	37215
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: 156.226.75.46	
Timestamp:	192.168.2.23156.226.75.4648516528692027339 05/27/22-02:14:01.198799
SID:	2027339
Source Port:	48516
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: 156.225.141.199	
Timestamp:	192.168.2.23156.225.141.19958162528692027339 05/27/22-02:13:05.395964
SID:	2027339
Source Port:	58162
Destination Port:	52869
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: 156.254.58.237	
Timestamp:	192.168.2.23156.254.58.23755430372152835222 05/27/22-02:14:57.299845
SID:	2835222
Source Port:	55430
Destination Port:	37215
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: 156.244.85.128	
Timestamp:	192.168.2.23156.244.85.12849114528692027339 05/27/22-02:14:32.261733
SID:	2027339
Source Port:	49114
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: 156.230.16.4	
Timestamp:	192.168.2.23156.230.16.454496528692027339 05/27/22-02:15:51.760200
SID:	2027339
Source Port:	54496
Destination Port:	52869
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: 156.225.138.112	
Timestamp:	192.168.2.23156.225.138.11251752372152835222 05/27/22-02:13:57.830736
SID:	2835222
Source Port:	51752
Destination Port:	37215
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: 156.226.106.71	
Timestamp:	192.168.2.23156.226.106.7147258372152835222 05/27/22-02:15:03.890871
SID:	2835222
Source Port:	47258
Destination Port:	37215
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: 156.250.15.239	
Timestamp:	192.168.2.23156.250.15.23946968528692027339 05/27/22-02:15:47.192692
SID:	2027339
Source Port:	46968

Destination Port:	52869
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: 156.245.58.44	
Timestamp:	192.168.2.23156.245.58.44486103721528352222 05/27/22-02:13:46.898085
SID:	2835222
Source Port:	48610
Destination Port:	37215
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: 156.247.25.156	
Timestamp:	192.168.2.23156.247.25.156485365286920273 39 05/27/22-02:12:46.612785
SID:	2027339
Source Port:	48536
Destination Port:	52869
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: 156.241.133.240	
Timestamp:	192.168.2.23156.241.133.240562863721528352222 05/27/22-02:13:39.348628
SID:	2835222
Source Port:	56286
Destination Port:	37215
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: 156.230.28.73	
Timestamp:	192.168.2.23156.230.28.7345884528692027339 05/27/22-02:15:39.186764
SID:	2027339
Source Port:	45884
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: 156.226.56.241	
Timestamp:	192.168.2.23156.226.56.24144482528692027339 05/27/22-02:14:31.741771
SID:	2027339
Source Port:	44482
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: 156.235.97.166	
Timestamp:	192.168.2.23156.235.97.16654848528692027339 05/27/22-02:13:34.854493
SID:	2027339
Source Port:	54848
Destination Port:	52869
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: 156.225.132.207	
Timestamp:	192.168.2.23156.225.132.207364343721528352222 05/27/22-02:12:42.088150
SID:	2835222
Source Port:	36434
Destination Port:	37215
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: 156.247.20.102	
Timestamp:	192.168.2.23156.247.20.10237006528692027339 05/27/22-02:12:57.512512
SID:	2027339
Source Port:	37006
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: 156.241.127.197	
Timestamp:	192.168.2.23156.241.127.19738718528692027339 05/27/22-02:12:53.360210
SID:	2027339
Source Port:	38718
Destination Port:	52869
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: 156.224.31.58	
Timestamp:	192.168.2.23156.224.31.5834264372152835222 05/27/22-02:14:00.300631
SID:	2835222
Source Port:	34264
Destination Port:	37215
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: 156.238.62.61	
Timestamp:	192.168.2.23156.238.62.6141094528692027339 05/27/22-02:15:44.833472
SID:	2027339
Source Port:	41094
Destination Port:	52869
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: 156.238.61.198	
Timestamp:	192.168.2.23156.238.61.19838604372152835222 05/27/22-02:12:42.098117
SID:	2835222
Source Port:	38604
Destination Port:	37215
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: 156.225.137.129	
Timestamp:	192.168.2.23156.225.137.12950458528692027339 05/27/22-02:15:07.743958
SID:	2027339
Source Port:	50458
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: 156.254.97.195	
Timestamp:	192.168.2.23156.254.97.19555994528692027339 05/27/22-02:16:00.365402
SID:	2027339
Source Port:	55994
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: 156.254.107.16	
Timestamp:	192.168.2.23156.254.107.1652176528692027339 05/27/22-02:16:02.078691
SID:	2027339
Source Port:	52176

Destination Port:	52869
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: 156.241.104.159	
Timestamp:	192.168.2.23156.241.104.15951580372152835222 05/27/22-02:14:33.327999
SID:	2835222
Source Port:	51580
Destination Port:	37215
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: 156.254.39.235	
Timestamp:	192.168.2.23156.254.39.23552566528692027339 05/27/22-02:15:32.125041
SID:	2027339
Source Port:	52566
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: 156.247.21.73	
Timestamp:	192.168.2.23156.247.21.7352968528692027339 05/27/22-02:15:49.939246
SID:	2027339
Source Port:	52968
Destination Port:	52869
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: 156.241.13.19	
Timestamp:	192.168.2.23156.241.13.1957972372152835222 05/27/22-02:15:29.464566
SID:	2835222
Source Port:	57972
Destination Port:	37215
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: 156.226.15.21	
Timestamp:	192.168.2.23156.226.15.2155130528692027339 05/27/22-02:13:27.026150
SID:	2027339
Source Port:	55130
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: 156.245.49.37	
Timestamp:	192.168.2.23156.245.49.3753600528692027339 05/27/22-02:14:26.799092
SID:	2027339
Source Port:	53600
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: 156.240.105.159	
Timestamp:	192.168.2.23156.240.105.15933672528692027339 05/27/22-02:13:00.042953
SID:	2027339
Source Port:	33672
Destination Port:	52869
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: 197.0.78.138	
Timestamp:	192.168.2.23197.0.78.13843770372152835222 05/27/22-02:15:44.616626
SID:	2835222
Source Port:	43770
Destination Port:	37215
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: 156.244.91.164	
Timestamp:	192.168.2.23156.244.91.16451552372152835222 05/27/22-02:15:48.271631
SID:	2835222
Source Port:	51552
Destination Port:	37215
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: 156.245.50.72	
Timestamp:	192.168.2.23156.245.50.7248118372152835222 05/27/22-02:14:06.437344
SID:	2835222
Source Port:	48118
Destination Port:	37215
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: 156.245.56.173	
Timestamp:	192.168.2.23156.245.56.17355964372152835222 05/27/22-02:14:01.873343
SID:	2835222
Source Port:	55964
Destination Port:	37215
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: 156.245.58.22	
Timestamp:	192.168.2.23156.245.58.2256504528692027339 05/27/22-02:14:37.543936
SID:	2027339
Source Port:	56504
Destination Port:	52869
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: 156.224.23.160	
Timestamp:	192.168.2.23156.224.23.16048230372152835222 05/27/22-02:14:38.368764
SID:	2835222
Source Port:	48230
Destination Port:	37215
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: 156.227.245.226	
Timestamp:	192.168.2.23156.227.245.226327863721528352222 05/27/22-02:15:19.170164
SID:	2835222
Source Port:	32786
Destination Port:	37215
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: 156.241.133.99	
Timestamp:	192.168.2.23156.241.133.9933550528692027339 05/27/22-02:13:38.944703
SID:	2027339
Source Port:	33550

Destination Port:	52869
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: 156.224.30.169

Timestamp:	192.168.2.23156.224.30.16944296372152835222 05/27/22-02:14:00.475775
SID:	2835222
Source Port:	44296
Destination Port:	37215
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: 156.250.91.142

Timestamp:	192.168.2.23156.250.91.14250058372152835222 05/27/22-02:13:35.537847
SID:	2835222
Source Port:	50058
Destination Port:	37215
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: 156.226.25.220

Timestamp:	192.168.2.23156.226.25.22033464528692027339 05/27/22-02:13:45.425689
SID:	2027339
Source Port:	33464
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: 156.247.17.8

Timestamp:	192.168.2.23156.247.17.854470528692027339 05/27/22-02:13:13.162457
SID:	2027339
Source Port:	54470
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: 156.238.59.115

Timestamp:	192.168.2.23156.238.59.11555876528692027339 05/27/22-02:13:57.702025
SID:	2027339
Source Port:	55876
Destination Port:	52869
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: 156.225.140.6

Timestamp:	192.168.2.23156.225.140.660912372152835222 05/27/22-02:15:40.316659
SID:	2835222
Source Port:	60912
Destination Port:	37215
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: 156.241.98.77

Timestamp:	192.168.2.23156.241.98.7758232528692027339 05/27/22-02:12:53.648941
SID:	2027339
Source Port:	58232
Destination Port:	52869
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: 156.254.54.155	
Timestamp:	192.168.2.23156.254.54.15546512372152835222 05/27/22-02:14:38.804612
SID:	2835222
Source Port:	46512
Destination Port:	37215
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: 156.237.4.33	
Timestamp:	192.168.2.23156.237.4.3337864528692027339 05/27/22-02:15:46.120268
SID:	2027339
Source Port:	37864
Destination Port:	52869
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: 156.241.102.130	
Timestamp:	192.168.2.23156.241.102.13036626372152835222 05/27/22-02:13:15.647863
SID:	2835222
Source Port:	36626
Destination Port:	37215
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: 156.224.12.38	
Timestamp:	192.168.2.23156.224.12.3833492372152835222 05/27/22-02:15:58.248459
SID:	2835222
Source Port:	33492
Destination Port:	37215
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: 156.240.108.157	
Timestamp:	192.168.2.23156.240.108.15747280528692027339 05/27/22-02:13:57.669807
SID:	2027339
Source Port:	47280
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: 156.241.95.104	
Timestamp:	192.168.2.23156.241.95.10457164528692027339 05/27/22-02:13:04.404090
SID:	2027339
Source Port:	57164
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: 156.245.51.84	
Timestamp:	192.168.2.23156.245.51.8442484528692027339 05/27/22-02:15:11.333358
SID:	2027339
Source Port:	42484
Destination Port:	52869
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: 156.254.92.26	
Timestamp:	192.168.2.23156.254.92.2643852372152835222 05/27/22-02:14:35.952032
SID:	2835222
Source Port:	43852

Destination Port:	37215
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: 156.241.74.71	
Timestamp:	192.168.2.23156.241.74.7157752528692027339 05/27/22-02:14:36.906433
SID:	2027339
Source Port:	57752
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: 156.244.114.186	
Timestamp:	192.168.2.23156.244.114.18634296528692027339 05/27/22-02:14:00.653295
SID:	2027339
Source Port:	34296
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: 156.224.20.170	
Timestamp:	192.168.2.23156.224.20.17034504528692027339 05/27/22-02:13:34.854326
SID:	2027339
Source Port:	34504
Destination Port:	52869
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: 156.245.57.168	
Timestamp:	192.168.2.23156.245.57.16858512372152835222 05/27/22-02:12:59.620616
SID:	2835222
Source Port:	58512
Destination Port:	37215
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: 156.238.52.111	
Timestamp:	192.168.2.23156.238.52.11151128372152835222 05/27/22-02:13:41.136266
SID:	2835222
Source Port:	51128
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.140.12.139	
Timestamp:	192.168.2.2341.140.12.13953634372152835222 05/27/22-02:14:56.565566
SID:	2835222
Source Port:	53634
Destination Port:	37215
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: 156.226.87.229	
Timestamp:	192.168.2.23156.226.87.22947502372152835222 05/27/22-02:14:13.155214
SID:	2835222
Source Port:	47502
Destination Port:	37215
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: 156.224.22.154	
Timestamp:	192.168.2.23156.224.22.15445932528692027339 05/27/22-02:12:52.902558
SID:	2027339
Source Port:	45932
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: 156.225.137.22	
Timestamp:	192.168.2.23156.225.137.2246960528692027339 05/27/22-02:14:37.082380
SID:	2027339
Source Port:	46960
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: 156.235.100.77	
Timestamp:	192.168.2.23156.235.100.7760114528692027339 05/27/22-02:13:38.665239
SID:	2027339
Source Port:	60114
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: 156.241.80.8	
Timestamp:	192.168.2.23156.241.80.852088528692027339 05/27/22-02:13:40.714340
SID:	2027339
Source Port:	52088
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: 156.254.78.144	
Timestamp:	192.168.2.23156.254.78.14439760528692027339 05/27/22-02:15:10.377160
SID:	2027339
Source Port:	39760
Destination Port:	52869
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: 156.241.75.54	
Timestamp:	192.168.2.23156.241.75.5453238372152835222 05/27/22-02:15:24.966301
SID:	2835222
Source Port:	53238
Destination Port:	37215
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: 156.226.73.139	
Timestamp:	192.168.2.23156.226.73.13932928372152835222 05/27/22-02:16:02.988563
SID:	2835222
Source Port:	32928
Destination Port:	37215
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: 156.254.56.201	
Timestamp:	192.168.2.23156.254.56.20143398372152835222 05/27/22-02:13:57.860088
SID:	2835222
Source Port:	43398

Destination Port:	37215
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: 156.225.132.151	
Timestamp:	192.168.2.23156.225.132.151587265286920273339 05/27/22-02:14:53.211027
SID:	2027339
Source Port:	58726
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: 156.254.49.84	
Timestamp:	192.168.2.23156.254.49.8437180528692027339 05/27/22-02:15:29.068878
SID:	2027339
Source Port:	37180
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: 156.254.57.19	
Timestamp:	192.168.2.23156.254.57.1952420528692027339 05/27/22-02:12:41.170166
SID:	2027339
Source Port:	52420
Destination Port:	52869
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: 156.241.71.140	
Timestamp:	192.168.2.23156.241.71.14049818372152835222 05/27/22-02:13:17.716844
SID:	2835222
Source Port:	49818
Destination Port:	37215
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: 156.226.76.208	
Timestamp:	192.168.2.23156.226.76.20839132372152835222 05/27/22-02:12:36.342235
SID:	2835222
Source Port:	39132
Destination Port:	37215
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: 156.254.80.21	
Timestamp:	192.168.2.23156.254.80.2158070372152835222 05/27/22-02:13:06.666292
SID:	2835222
Source Port:	58070
Destination Port:	37215
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: 156.224.15.80	
Timestamp:	192.168.2.23156.224.15.8033284372152835222 05/27/22-02:13:11.149360
SID:	2835222
Source Port:	33284
Destination Port:	37215
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: 156.250.94.192	
Timestamp:	192.168.2.23156.250.94.19250570372152835222 05/27/22-02:15:59.700334
SID:	2835222
Source Port:	50570
Destination Port:	37215
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: 156.254.54.28	
Timestamp:	192.168.2.23156.254.54.2847544528692027339 05/27/22-02:13:35.459409
SID:	2027339
Source Port:	47544
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: 156.238.62.74	
Timestamp:	192.168.2.23156.238.62.7445152528692027339 05/27/22-02:13:56.811726
SID:	2027339
Source Port:	45152
Destination Port:	52869
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: 156.226.62.167	
Timestamp:	192.168.2.23156.226.62.16735340372152835222 05/27/22-02:14:12.939722
SID:	2835222
Source Port:	35340
Destination Port:	37215
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: 156.245.63.194	
Timestamp:	192.168.2.23156.245.63.19455388372152835222 05/27/22-02:12:59.125522
SID:	2835222
Source Port:	55388
Destination Port:	37215
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: 156.235.100.95	
Timestamp:	192.168.2.23156.235.100.9560966372152835222 05/27/22-02:14:10.940139
SID:	2835222
Source Port:	60966
Destination Port:	37215
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: 156.254.104.34	
Timestamp:	192.168.2.23156.254.104.3457648528692027339 05/27/22-02:16:02.071437
SID:	2027339
Source Port:	57648
Destination Port:	52869
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: 156.241.78.149	
Timestamp:	192.168.2.23156.241.78.14950422372152835222 05/27/22-02:14:26.066500
SID:	2835222
Source Port:	50422

Destination Port:	37215
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: 156.254.47.22

Timestamp:	192.168.2.23156.254.47.2243716372152835222 05/27/22-02:15:59.755311
SID:	2835222
Source Port:	43716
Destination Port:	37215
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: 156.241.103.18

Timestamp:	192.168.2.23156.241.103.1856104528692027339 05/27/22-02:13:20.893383
SID:	2027339
Source Port:	56104
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: 197.234.59.46

Timestamp:	192.168.2.23197.234.59.4655500528692027339 05/27/22-02:15:10.654032
SID:	2027339
Source Port:	55500
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: 156.230.27.70

Timestamp:	192.168.2.23156.230.27.7046850528692027339 05/27/22-02:15:23.381190
SID:	2027339
Source Port:	46850
Destination Port:	52869
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: 156.238.19.86

Timestamp:	192.168.2.23156.238.19.8649444372152835222 05/27/22-02:13:01.184283
SID:	2835222
Source Port:	49444
Destination Port:	37215
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: 156.241.112.224

Timestamp:	192.168.2.23156.241.112.22458220528692027339 05/27/22-02:13:33.393126
SID:	2027339
Source Port:	58220
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: 156.250.118.96

Timestamp:	192.168.2.23156.250.118.9651618528692027339 05/27/22-02:13:39.114643
SID:	2027339
Source Port:	51618
Destination Port:	52869
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: 156.226.72.130	
Timestamp:	192.168.2.23156.226.72.13056680372152835222 05/27/22-02:15:30.266729
SID:	2835222
Source Port:	56680
Destination Port:	37215
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: 156.238.62.139	
Timestamp:	192.168.2.23156.238.62.13953164528692027339 05/27/22-02:15:44.702643
SID:	2027339
Source Port:	53164
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: 156.241.98.171	
Timestamp:	192.168.2.23156.241.98.17159740528692027339 05/27/22-02:13:40.694540
SID:	2027339
Source Port:	59740
Destination Port:	52869
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: 156.250.13.247	
Timestamp:	192.168.2.23156.250.13.24753126372152835222 05/27/22-02:13:53.272848
SID:	2835222
Source Port:	53126
Destination Port:	37215
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: 197.232.16.122	
Timestamp:	192.168.2.23197.232.16.12238206528692027339 05/27/22-02:14:46.558798
SID:	2027339
Source Port:	38206
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: 156.250.122.218	
Timestamp:	192.168.2.23156.250.122.21842844528692027339 05/27/22-02:13:23.578725
SID:	2027339
Source Port:	42844
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: 156.245.54.168	
Timestamp:	192.168.2.23156.245.54.16858244528692027339 05/27/22-02:14:56.952383
SID:	2027339
Source Port:	58244
Destination Port:	52869
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: 156.254.47.219	
Timestamp:	192.168.2.23156.254.47.21960866372152835222 05/27/22-02:15:22.673219
SID:	2835222
Source Port:	60866

Destination Port:	37215
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: 156.224.21.214	
Timestamp:	192.168.2.23156.224.21.21458956528692027339 05/27/22-02:12:49.830344
SID:	2027339
Source Port:	58956
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: 156.244.65.29	
Timestamp:	192.168.2.23156.244.65.2942292528692027339 05/27/22-02:13:38.739294
SID:	2027339
Source Port:	42292
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: 156.250.120.191	
Timestamp:	192.168.2.23156.250.120.19144668528692027339 05/27/22-02:15:04.565007
SID:	2027339
Source Port:	44668
Destination Port:	52869
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: 156.254.83.35	
Timestamp:	192.168.2.23156.254.83.3549398372152835222 05/27/22-02:14:56.478107
SID:	2835222
Source Port:	49398
Destination Port:	37215
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: 156.250.89.168	
Timestamp:	192.168.2.23156.250.89.16847430372152835222 05/27/22-02:14:33.492223
SID:	2835222
Source Port:	47430
Destination Port:	37215
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: 156.241.8.181	
Timestamp:	192.168.2.23156.241.8.18160434372152835222 05/27/22-02:14:17.531747
SID:	2835222
Source Port:	60434
Destination Port:	37215
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: 156.245.56.175	
Timestamp:	192.168.2.23156.245.56.17547336372152835222 05/27/22-02:13:30.930123
SID:	2835222
Source Port:	47336
Destination Port:	37215
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: 156.244.96.229	
Timestamp:	192.168.2.23156.244.96.22958766528692027339 05/27/22-02:14:59.658492
SID:	2027339
Source Port:	58766
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: 156.245.60.206	
Timestamp:	192.168.2.23156.245.60.20657106528692027339 05/27/22-02:15:57.085948
SID:	2027339
Source Port:	57106
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: 156.225.142.222	
Timestamp:	192.168.2.23156.225.142.22242424528692027339 05/27/22-02:14:34.289205
SID:	2027339
Source Port:	42424
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: 156.224.22.230	
Timestamp:	192.168.2.23156.224.22.23044286528692027339 05/27/22-02:15:39.353713
SID:	2027339
Source Port:	44286
Destination Port:	52869
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: 156.227.240.228	
Timestamp:	192.168.2.23156.227.240.228445123721528352222 05/27/22-02:12:36.138433
SID:	2835222
Source Port:	44512
Destination Port:	37215
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: 156.254.111.230	
Timestamp:	192.168.2.23156.254.111.23043658528692027339 05/27/22-02:13:56.928093
SID:	2027339
Source Port:	43658
Destination Port:	52869
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: 156.241.122.29	
Timestamp:	192.168.2.23156.241.122.2954938372152835222 05/27/22-02:16:05.477682
SID:	2835222
Source Port:	54938
Destination Port:	37215
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: 156.241.102.202	
Timestamp:	192.168.2.23156.241.102.20257920528692027339 05/27/22-02:13:49.854598
SID:	2027339
Source Port:	57920

Destination Port:	52869
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: 156.232.95.55	
Timestamp:	192.168.2.23156.232.95.5536332372152835222 05/27/22-02:14:42.534896
SID:	2835222
Source Port:	36332
Destination Port:	37215
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: 156.254.66.139	
Timestamp:	192.168.2.23156.254.66.13938366372152835222 05/27/22-02:13:08.640227
SID:	2835222
Source Port:	38366
Destination Port:	37215
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: 156.250.121.73	
Timestamp:	192.168.2.23156.250.121.7352058372152835222 05/27/22-02:15:27.222565
SID:	2835222
Source Port:	52058
Destination Port:	37215
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: 156.250.94.91	
Timestamp:	192.168.2.23156.250.94.9154174372152835222 05/27/22-02:13:40.148680
SID:	2835222
Source Port:	54174
Destination Port:	37215
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: 156.244.117.128	
Timestamp:	192.168.2.23156.244.117.12852300372152835222 05/27/22-02:14:01.942691
SID:	2835222
Source Port:	52300
Destination Port:	37215
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: 156.241.112.159	
Timestamp:	192.168.2.23156.241.112.15944218372152835222 05/27/22-02:15:38.230922
SID:	2835222
Source Port:	44218
Destination Port:	37215
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: 156.240.104.21	
Timestamp:	192.168.2.23156.240.104.2144700372152835222 05/27/22-02:14:10.957392
SID:	2835222
Source Port:	44700
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound - Source IP: 192.168.2.23 - Destination IP: 156.250.91.48	
Timestamp:	192.168.2.23156.250.91.4841964528692027339 05/27/22-02:14:37.762120
SID:	2027339
Source Port:	41964
Destination Port:	52869
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: 156.254.39.187	
Timestamp:	192.168.2.23156.254.39.18756308372152835222 05/27/22-02:15:19.193274
SID:	2835222
Source Port:	56308
Destination Port:	37215
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: 156.241.121.148	
Timestamp:	192.168.2.23156.241.121.14844116528692027339 05/27/22-02:15:11.303838
SID:	2027339
Source Port:	44116
Destination Port:	52869
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: 156.226.49.180	
Timestamp:	192.168.2.23156.226.49.18046232372152835222 05/27/22-02:13:29.334888
SID:	2835222
Source Port:	46232
Destination Port:	37215
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: 156.238.55.79	
Timestamp:	192.168.2.23156.238.55.7957326372152835222 05/27/22-02:13:52.055223
SID:	2835222
Source Port:	57326
Destination Port:	37215
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: 156.238.48.101	
Timestamp:	192.168.2.23156.238.48.10159654372152835222 05/27/22-02:14:41.192161
SID:	2835222
Source Port:	59654
Destination Port:	37215
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: 156.238.55.23	
Timestamp:	192.168.2.23156.238.55.2340874372152835222 05/27/22-02:14:26.852111
SID:	2835222
Source Port:	40874
Destination Port:	37215
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: 156.238.58.248	
Timestamp:	192.168.2.23156.238.58.24843112528692027339 05/27/22-02:14:07.437398
SID:	2027339
Source Port:	43112

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: 156.226.74.55	
Timestamp:	192.168.2.23156.226.74.5539048528692027339 05/27/22-02:13:35.207018
SID:	2027339
Source Port:	39048
Destination Port:	52869
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: 156.241.106.241	
Timestamp:	192.168.2.23156.241.106.241562823721528352222 05/27/22-02:15:11.455257
SID:	2835222
Source Port:	56282
Destination Port:	37215
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: 156.250.122.181	
Timestamp:	192.168.2.23156.250.122.181541443721528352222 05/27/22-02:12:51.092716
SID:	2835222
Source Port:	54144
Destination Port:	37215
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: 156.241.94.117	
Timestamp:	192.168.2.23156.241.94.11739036528692027339 05/27/22-02:14:09.966616
SID:	2027339
Source Port:	39036
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: 156.224.20.197	
Timestamp:	192.168.2.23156.224.20.19748634528692027339 05/27/22-02:14:19.780807
SID:	2027339
Source Port:	48634
Destination Port:	52869
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: 156.240.105.92	
Timestamp:	192.168.2.23156.240.105.9251254372152835222 05/27/22-02:15:03.950087
SID:	2835222
Source Port:	51254
Destination Port:	37215
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: 156.239.155.141	
Timestamp:	192.168.2.23156.239.155.141455043721528352222 05/27/22-02:14:38.834279
SID:	2835222
Source Port:	45504
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 156.235.108.40	
Timestamp:	192.168.2.23156.235.108.4034412372152835222 05/27/22-02:14:52.871348
SID:	2835222
Source Port:	34412
Destination Port:	37215
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: 156.241.89.153	
Timestamp:	192.168.2.23156.241.89.15352104528692027339 05/27/22-02:13:27.225645
SID:	2027339
Source Port:	52104
Destination Port:	52869
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: 156.235.103.207	
Timestamp:	192.168.2.23156.235.103.20747134372152835222 05/27/22-02:15:58.666213
SID:	2835222
Source Port:	47134
Destination Port:	37215
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: 156.244.88.74	
Timestamp:	192.168.2.23156.244.88.7459642372152835222 05/27/22-02:12:37.779404
SID:	2835222
Source Port:	59642
Destination Port:	37215
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: 156.241.78.17	
Timestamp:	192.168.2.23156.241.78.1734970372152835222 05/27/22-02:15:55.887379
SID:	2835222
Source Port:	34970
Destination Port:	37215
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: 156.254.58.28	
Timestamp:	192.168.2.23156.254.58.2849626528692027339 05/27/22-02:14:03.905575
SID:	2027339
Source Port:	49626
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

Connects to many ports of the same IP (likely port scanning)

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

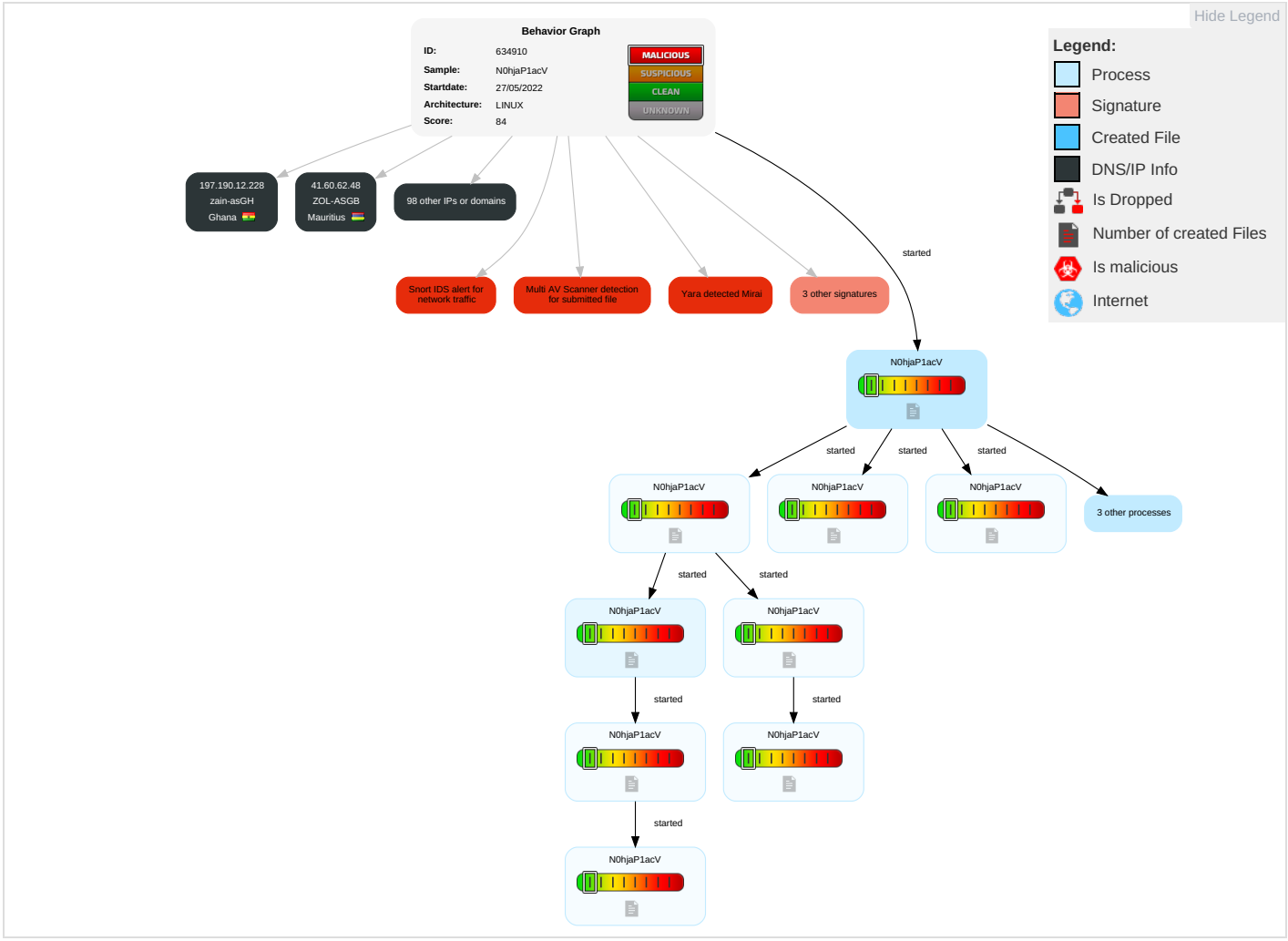
Mitre Att&ck Matrix

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	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	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
N0hjaP1acV	30%	Virustotal		Browse
N0hjaP1acV	39%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.billybobbot.com/crawler/)	0%	URL Reputation	safe	
http://fast.no/support/crawler.asp)	0%	URL Reputation	safe	
http://185.44.81.114/bins/mips;	100%	Avira URL Cloud	malware	
http://feedback.redkolibri.com/	0%	URL Reputation	safe	

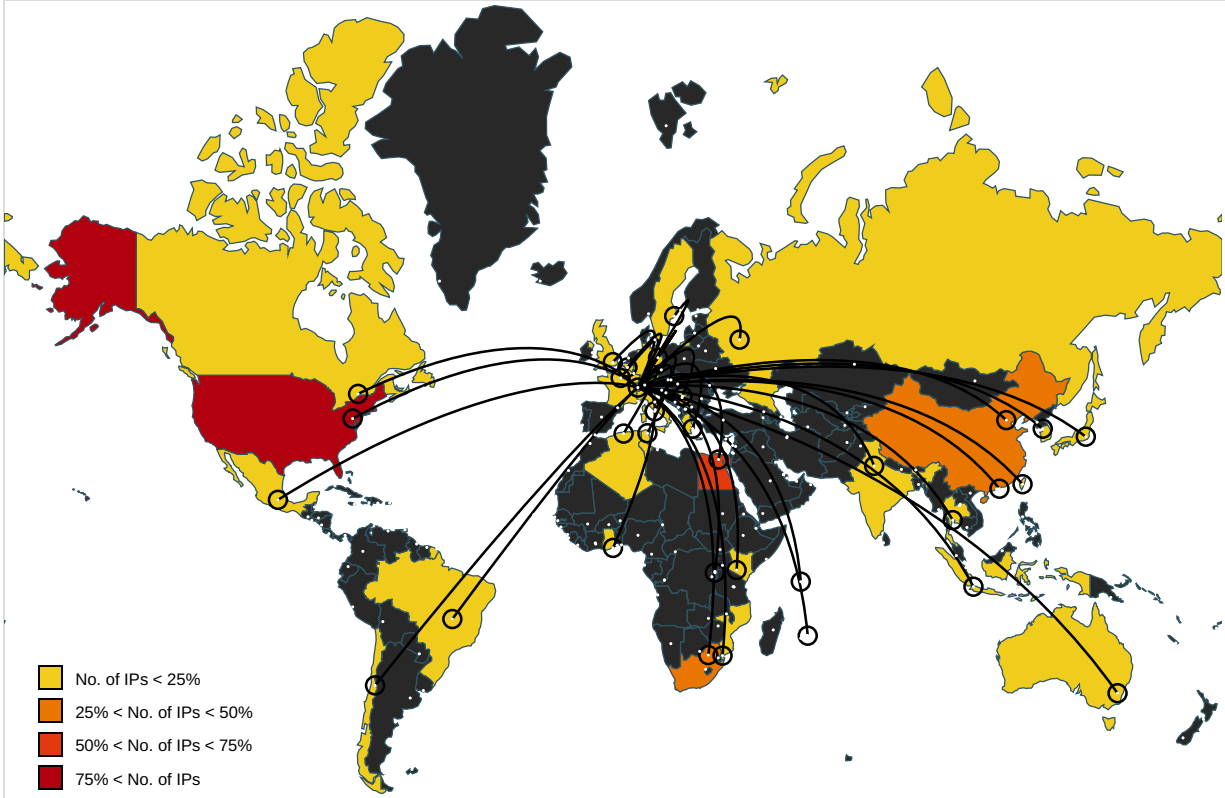
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.13.57.228	unknown	Tunisia		37504	MeninxTN	false
191.232.45.248	unknown	Brazil		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
41.114.147.144	unknown	South Africa		16637	MTNNS-ASZA	false
18.240.63.162	unknown	United States		16509	AMAZON-02US	false
16.113.51.109	unknown	United States		unknown	unknown	false
148.237.59.96	unknown	Mexico		7325	UniversidadAutonomaDeTamaulipasMX	false
8.35.85.236	unknown	United States		36614	VIZADA-INC-AS1US	false
174.79.178.137	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
41.2.68.194	unknown	South Africa		29975	VODACOM-ZA	false
116.6.240.232	unknown	China		134774	CHINANET-GUANGDONG-SHENZHEN-MANCHINANETGuangdong province	false
41.196.116.145	unknown	Egypt		24863	LINKdotNET-ASEG	false
38.217.51.203	unknown	United States		174	COGENT-174US	false
41.60.62.48	unknown	Mauritius		30969	ZOL-ASGB	false
202.196.143.73	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
81.113.185.44	unknown	Italy		20959	TELECOM-ITALIA-DATA-COMIT	false
156.176.96.210	unknown	Egypt		36992	ETISALAT-MISREG	false
53.188.22.70	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
154.247.55.140	unknown	Algeria		36947	ALGTEL-ASDZ	false
92.124.86.80	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.140.100.214	unknown	United States		16509	AMAZON-02US	false
39.208.21.149	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
152.12.194.225	unknown	United States		81	NCRENUS	false
76.124.251.209	unknown	United States		7922	COMCAST-7922US	false
12.89.103.161	unknown	United States		7018	ATT-INTERNET4US	false
74.214.134.160	unknown	Canada		36817	MCSNETCA	false
93.202.30.191	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
67.50.208.97	unknown	United States		7385	ALLSTREAMUS	false
114.47.3.87	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
101.186.227.228	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
185.199.120.219	unknown	Serbia		42603	PARKING-SERVIS-ASRS	false
163.125.252.73	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
171.101.102.224	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	false
41.187.200.110	unknown	Egypt		20928	NOOR-ASEG	false
148.35.90.214	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
31.121.22.168	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
197.60.107.68	unknown	Egypt		8452	TE-ASTE-ASEG	false
37.32.128.243	unknown	Greece		5408	GR-NEThttpwwwgrnetgrGR	false
182.228.224.31	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
197.235.33.27	unknown	Mozambique		37223	VODACOM-MZ	false
197.4.29.28	unknown	Tunisia		5438	ATI-TN	false
156.49.135.64	unknown	Sweden		29975	VODACOM-ZA	false
156.175.120.20	unknown	Egypt		36992	ETISALAT-MISREG	false
197.202.110.207	unknown	Algeria		36947	ALGTEL-ASDZ	false
162.111.217.205	unknown	United States		4196	WELLSFARGO-4196US	false
156.246.150.172	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
41.17.0.125	unknown	South Africa		29975	VODACOM-ZA	false
70.171.93.169	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
156.255.211.8	unknown	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	false
197.202.209.190	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.79.92.19	unknown	United States		11363	FUJITSU-USAUS	false
41.35.57.90	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.171.231.149	unknown	South Africa		36937	Neotel-ASZA	false
66.193.178.23	unknown	United States		27537	ACCAASUS	false
98.72.203.159	unknown	United States		7018	ATT-INTERNET4US	false
78.69.183.161	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
197.132.199.93	unknown	Egypt		24835	RAYA-ASEG	false
171.2.219.217	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
54.126.191.38	unknown	United States		16509	AMAZON-02US	false
156.196.122.203	unknown	Egypt		8452	TE-ASTE-ASEG	false
206.198.52.93	unknown	United States		26844	PACTIVUS	false
156.249.107.53	unknown	Seychelles		139086	ONL-HKOCEANNETWORKLIMITEDHK	false
197.58.204.237	unknown	Egypt		8452	TE-ASTE-ASEG	false
66.171.26.158	unknown	United States		33339	NEMONT-CELLULARUS	false
163.222.171.169	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.18.227.180	unknown	France		1945	FR-LYRESLyonRechercheetEnseignementSuperieurLyRESE	false
197.12.31.229	unknown	Tunisia		37703	ATLAXTN	false
156.183.30.16	unknown	Egypt		36992	ETISALAT-MISREG	false
103.133.37.115	unknown	India		135851	PARTHIV-ASExcogitateTechnologiesPvtLtdIN	false
156.197.112.189	unknown	Egypt		8452	TE-ASTE-ASEG	false
42.156.20.11	unknown	China		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
89.233.66.101	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
57.170.159.134	unknown	Belgium		2686	ATGS-MMD-ASUS	false
156.235.189.193	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	false
183.177.82.231	unknown	Hong Kong		10310	YAHOO-1US	false
41.139.156.190	unknown	Kenya		37061	SafaricomKE	false
53.206.242.155	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
43.41.137.199	unknown	Japan		4249	LILLY-ASUS	false
105.237.52.53	unknown	South Africa		16637	MTNNS-ASZA	false
61.42.187.104	unknown	Korea Republic of		4668	LGNET-AS-KRLGCNSKR	false
143.170.67.138	unknown	United States		16504	GRANITEUS	false
19.211.216.137	unknown	United States		3	MIT-GATEWAYSUS	false
197.190.12.228	unknown	Ghana		37140	zain-asGH	false
42.54.144.183	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
41.186.210.247	unknown	Rwanda		36890	MTNRW-ASNRW	false
156.111.211.31	unknown	United States		395139	NYP-INTERNETUS	false
89.92.79.92	unknown	France		5410	BOUYGTEL-ISPFR	false
124.31.194.13	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
191.214.237.15	unknown	Brazil		7738	TelemarNorteLesteSABR	false
197.49.247.251	unknown	Egypt		8452	TE-ASTE-ASEG	false
193.54.61.173	unknown	France		2471	FR-DOM-GUADELOUPEIlesdelaGuadeloupeEU	false
193.205.119.153	unknown	Italy		137	ASGARRConsortiumGARREU	false
156.147.203.61	unknown	Korea Republic of		4668	LGNET-AS-KRLGCNSKR	false
195.32.24.62	unknown	Italy		202870	AS_DIMENSIONEIT	false
190.47.23.48	unknown	Chile		22047	VTRBANDAANCHASACL	false
114.188.75.138	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
156.241.24.117	unknown	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	false
197.76.213.163	unknown	South Africa		16637	MTNNS-ASZA	false
92.24.1.91	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
156.249.231.127	unknown	Seychelles		26484	IKGUL-26484US	false
156.108.54.3	unknown	United States		36081	STATE-OF-COLORADO-MNT-NETWORKUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.948815950081947
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	N0hjaP1acV
File size:	46660
MD5:	ee14dc420ebe8fe314e596360fc6e382
SHA1:	8b3d7ca9d831a9ecd543ea5d344b30b525c267c2
SHA256:	30f9ae9beb37d5a8f1858b947be85c8fbcbd4c094f3c8cd5b8e6d2886d6e08b9
SHA512:	3f6e8186e2ca52c4ae6c16bd8f3a998e03df89733ebd350ccfa8c9b232a2a1478478abadbd28da72ef6614ac142c6d03ae1da15b393fd4e7922436525b375594
SSDEEP:	768:DKXFkWQeA8P3WTS75z772f+8sDvzzEcraKI6a/GCMGWJ:D41PG4Sm8qb+KI6aI
TLSH:	CB23E17ED1D03CC7FFA9A8BE608C4DD02C55F682229D5749E316C8C983B5AADB289034
File Content Preview:	.ELF.....4.....4. ...(.....O...OF..OF.....:.jcUPX!d.....l...l.....U.....?.E.h;....#.....b.L#3:....sO..v.... [.x..5.43.B.....}...L.....ol.....6I.p,...Q.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little 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:	0x10a1c8
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2

Copyright Joe Security LLC 2022

ELF header	
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0xb505	0xb505	4.1369	0x5	R E	0x10000		
LOAD	0x4f9c	0x464f9c	0x464f9c	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.224.14.795061852869202733905/27/22-02:13:58.105252	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	50618	52869	192.168.2.23	156.224.14.79
192.168.2.23156.226.61.655720452869202733905/27/22-02:16:04.924108	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57204	52869	192.168.2.23	156.226.61.65
192.168.2.23156.235.98.202490465286920273905/27/22-02:14:35.444891	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	49046	52869	192.168.2.23	156.235.98.202
192.168.2.23156.241.74.2204626528692027339905/27/22-02:14:36.677860	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46262	52869	192.168.2.23	156.241.74.220
192.168.2.23156.241.84.1154143052869202733905/27/22-02:13:56.668282	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	41430	52869	192.168.2.23	156.241.84.115
192.168.2.23156.227.240.97540365286920273905/27/22-02:13:49.289658	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54036	52869	192.168.2.23	156.227.240.97
192.168.2.23156.224.22.385590528692027339905/27/22-02:14:36.626878	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55960	52869	192.168.2.23	156.224.22.38
192.168.2.23156.225.138.90428483721528352225/27/22-02:15:11.674046	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42848	37215	192.168.2.23	156.225.138.90
192.168.2.23156.244.71.103584452869202733905/27/22-02:12:54.856801	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	35844	52869	192.168.2.23	156.244.71.10
192.168.2.23156.250.14.2143682528692027339905/27/22-02:15:25.586143	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	43682	52869	192.168.2.23	156.250.14.21
192.168.2.23156.224.9.163473845286920273905/27/22-02:14:57.144519	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	47384	52869	192.168.2.23	156.224.9.163
192.168.2.23156.238.48.2654720372152835225/27/22-02:13:39.144497	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54720	37215	192.168.2.23	156.238.48.26
192.168.2.23156.238.46.1583754452869202733905/27/22-02:15:35.761225	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	37544	52869	192.168.2.23	156.238.46.158

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.245.60.1 5545062528692027339 05/27/22- 02:14:40.059383	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	45062	52869	192.168.2.23	156.245.60.155
192.168.2.23156.238.49.1 5951956528692027339 05/27/22- 02:14:00.916205	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	51956	52869	192.168.2.23	156.238.49.159
192.168.2.23156.225.143. 18546852528692027339 05/27/22- 02:15:44.829670	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46852	52869	192.168.2.23	156.225.143.185
192.168.2.23156.241.116. 8035674528692027339 05/27/22- 02:14:37.094245	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	35674	52869	192.168.2.23	156.241.116.80
192.168.2.23156.226.82.1 4242758528692027339 05/27/22- 02:12:55.926001	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	42758	52869	192.168.2.23	156.226.82.142
192.168.2.23156.226.96.2 2646198528692027339 05/27/22- 02:13:10.956619	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46198	52869	192.168.2.23	156.226.96.226
192.168.2.23156.244.71.3 647022372152835222 05/27/22- 02:13:23.331351	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47022	37215	192.168.2.23	156.244.71.36
192.168.2.23156.244.123. 935674528692027339 05/27/22- 02:14:50.971307	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	35674	52869	192.168.2.23	156.244.123.9
192.168.2.23156.244.105. 8957578528692027339 05/27/22- 02:15:32.707694	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57578	52869	192.168.2.23	156.244.105.89
192.168.2.23156.254.59.9 749196528692027339 05/27/22- 02:12:56.166673	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	49196	52869	192.168.2.23	156.254.59.97
192.168.2.23156.240.106. 14755106372152835222 05/27/22- 02:14:29.271383	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55106	37215	192.168.2.23	156.240.106.147
192.168.2.23156.244.87.2 2641980528692027339 05/27/22- 02:14:29.289410	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	41980	52869	192.168.2.23	156.244.87.226
192.168.2.23156.225.159. 9053200528692027339 05/27/22- 02:15:26.120158	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	53200	52869	192.168.2.23	156.225.159.90
192.168.2.23156.247.27.2 5357938528692027339 05/27/22- 02:13:53.102906	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57938	52869	192.168.2.23	156.247.27.253
192.168.2.23156.245.61.2 542128372152835222 05/27/22- 02:14:49.510258	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42128	37215	192.168.2.23	156.245.61.25
192.168.2.23156.254.91.2 855614528692027339 05/27/22- 02:14:18.676105	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55614	52869	192.168.2.23	156.254.91.28
192.168.2.23156.224.10.8 242746372152835222 05/27/22- 02:13:33.105779	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42746	37215	192.168.2.23	156.224.10.82
192.168.2.23156.254.84.1 6260258372152835222 05/27/22- 02:15:47.741844	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60258	37215	192.168.2.23	156.254.84.162
192.168.2.2341.78.123.14 8548528692027339 05/27/22- 02:13:21.096567	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48548	52869	192.168.2.23	41.78.123.1

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.239.155.15857160372152835222 05/27/22-02:14:46.840933	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57160	37215	192.168.2.23	156.239.155.158
192.168.2.23156.226.77.187548163721528352222 05/27/22-02:15:44.742124	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54816	37215	192.168.2.23	156.226.77.187
192.168.2.23156.226.108.9943718528692027339 05/27/22-02:12:43.189218	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	43718	52869	192.168.2.23	156.226.108.99
192.168.2.23156.254.52.1903308528692027339 05/27/22-02:13:35.255592	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33086	52869	192.168.2.23	156.254.52.190
192.168.2.23156.250.86.1213860637215283522 05/27/22-02:14:39.009848	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38606	37215	192.168.2.23	156.250.86.121
192.168.2.23156.250.126.23844746528692027339 05/27/22-02:15:02.150467	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44746	52869	192.168.2.23	156.250.126.238
192.168.2.23156.244.81.634023637215283522 05/27/22-02:15:19.372629	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40236	37215	192.168.2.23	156.244.81.63
192.168.2.23156.226.56.1052602372152835222 05/27/22-02:12:54.824351	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52602	37215	192.168.2.23	156.226.56.10
192.168.2.23197.234.54.1435134837215283522 05/27/22-02:16:02.763420	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51348	37215	192.168.2.23	197.234.54.143
192.168.2.23156.238.46.4234500528692027339 05/27/22-02:15:27.951216	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34500	52869	192.168.2.23	156.238.46.42
192.168.2.23156.226.91.1533542252869202733 9 05/27/22-02:12:57.071160	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	35422	52869	192.168.2.23	156.226.91.153
192.168.2.23156.244.112.8149114528692027339 05/27/22-02:14:02.928791	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	49114	52869	192.168.2.23	156.244.112.81
192.168.2.23156.254.78.1003283652869202733 9 05/27/22-02:14:14.336004	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	32836	52869	192.168.2.23	156.254.78.100
192.168.2.23156.254.97.1084633637215283522 05/27/22-02:15:58.248205	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46336	37215	192.168.2.23	156.254.97.108
192.168.2.23156.230.29.6445174372152835222 05/27/22-02:13:57.768233	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45174	37215	192.168.2.23	156.230.29.64
192.168.2.23156.241.110.1256560528692027339 05/27/22-02:15:46.756882	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	56560	52869	192.168.2.23	156.241.110.12
192.168.2.23156.241.75.035466528692027339 05/27/22-02:13:10.915908	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	35466	52869	192.168.2.23	156.241.75.0
192.168.2.23156.226.92.2295796852869202733 9 05/27/22-02:14:25.235370	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57968	52869	192.168.2.23	156.226.92.229
192.168.2.23156.241.74.1113938037215283522 05/27/22-02:14:17.492006	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39380	37215	192.168.2.23	156.241.74.111

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.241.79.4 638264528692027339 05/27/22- 02:12:53.354886	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38264	52869	192.168.2.23	156.241.79.46
192.168.2.23156.244.115. 13956778372152835222 05/27/22- 02:13:45.586935	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56778	37215	192.168.2.23	156.244.115.139
192.168.2.23156.247.27.7 743950528692027339 05/27/22- 02:14:48.265097	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	43950	52869	192.168.2.23	156.247.27.77
192.168.2.23156.254.53.4 39590528692027339 05/27/22- 02:14:50.766924	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39590	52869	192.168.2.23	156.254.53.4
192.168.2.23156.225.133. 3557720528692027339 05/27/22- 02:15:41.275652	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57720	52869	192.168.2.23	156.225.133.35
192.168.2.23156.241.76.1 3138880372152835222 05/27/22- 02:13:29.292236	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38880	37215	192.168.2.23	156.241.76.131
192.168.2.23156.226.80.5 734018528692027339 05/27/22- 02:13:52.173426	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34018	52869	192.168.2.23	156.226.80.57
192.168.2.23156.232.94.1 9548476372152835222 05/27/22- 02:15:58.177549	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48476	37215	192.168.2.23	156.232.94.195
192.168.2.23156.238.54.1 5656814528692027339 05/27/22- 02:13:52.850974	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	56814	52869	192.168.2.23	156.238.54.156
192.168.2.23156.239.152. 11950524528692027339 05/27/22- 02:15:30.191969	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	50524	52869	192.168.2.23	156.239.152.119
192.168.2.23156.241.66.2 0950904372152835222 05/27/22- 02:15:47.269657	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50904	37215	192.168.2.23	156.241.66.209
192.168.2.23156.235.111. 13948572372152835222 05/27/22- 02:15:58.658252	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48572	37215	192.168.2.23	156.235.111.139
192.168.2.23156.227.240. 12943716528692027339 05/27/22- 02:13:38.769973	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	43716	52869	192.168.2.23	156.227.240.129
192.168.2.23156.225.139. 6345370528692027339 05/27/22- 02:13:01.828686	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	45370	52869	192.168.2.23	156.225.139.63
192.168.2.23156.241.115. 17658628528692027339 05/27/22- 02:15:29.598619	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58628	52869	192.168.2.23	156.241.115.176
192.168.2.23156.245.60.1 5346750372152835222 05/27/22- 02:13:24.130514	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46750	37215	192.168.2.23	156.245.60.153
192.168.2.23156.239.152. 24145346528692027339 05/27/22- 02:13:27.364885	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	45346	52869	192.168.2.23	156.239.152.241
192.168.2.23156.241.82.2 1942842528692027339 05/27/22- 02:13:59.432040	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	42842	52869	192.168.2.23	156.241.82.219
192.168.2.23156.225.159. 7533144528692027339 05/27/22- 02:16:02.376255	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33144	52869	192.168.2.23	156.225.159.75

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.254.49.1 0155184528692027339 05/27/22- 02:13:23.358713	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55184	52869	192.168.2.23	156.254.49.101
192.168.2.23156.226.103. 9948840528692027339 05/27/22- 02:13:52.855377	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48840	52869	192.168.2.23	156.226.103.99
192.168.2.23156.241.79.2 3948044372152835222 05/27/22- 02:14:15.506746	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48044	37215	192.168.2.23	156.241.79.239
192.168.2.23156.225.155. 21634766528692027339 05/27/22- 02:14:09.609403	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34766	52869	192.168.2.23	156.225.155.216
192.168.2.23156.235.98.1 5754100372152835222 05/27/22- 02:14:50.692622	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54100	37215	192.168.2.23	156.235.98.157
192.168.2.23156.235.102. 8256764372152835222 05/27/22- 02:12:48.708918	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56764	37215	192.168.2.23	156.235.102.82
192.168.2.23156.244.75.3 760012372152835222 05/27/22- 02:13:33.140390	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60012	37215	192.168.2.23	156.244.75.37
192.168.2.23156.226.108. 1634146528692027339 05/27/22- 02:15:33.429510	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34146	52869	192.168.2.23	156.226.108.16
192.168.2.23156.241.99.1 1246524372152835222 05/27/22- 02:14:22.250710	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46524	37215	192.168.2.23	156.241.99.112
192.168.2.23156.250.113. 21339116528692027339 05/27/22- 02:13:04.328886	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39116	52869	192.168.2.23	156.250.113.213
192.168.2.23156.226.78.1 4639698372152835222 05/27/22- 02:13:36.843203	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39698	37215	192.168.2.23	156.226.78.146
192.168.2.23156.227.245. 16853588528692027339 05/27/22- 02:15:23.400250	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	53588	52869	192.168.2.23	156.227.245.168
192.168.2.23156.241.89.1 5641022372152835222 05/27/22- 02:13:15.717127	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41022	37215	192.168.2.23	156.241.89.156
192.168.2.23156.226.63.8 542466528692027339 05/27/22- 02:13:38.710756	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	42466	52869	192.168.2.23	156.226.63.85
192.168.2.23156.226.102. 11344524372152835222 05/27/22- 02:15:36.796853	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44524	37215	192.168.2.23	156.226.102.113
192.168.2.23156.254.60.1 6839394528692027339 05/27/22- 02:13:19.454012	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39394	52869	192.168.2.23	156.254.60.168
192.168.2.23156.245.60.3 440268372152835222 05/27/22- 02:13:22.309987	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40268	37215	192.168.2.23	156.245.60.34
192.168.2.23156.238.61.1 1047844528692027339 05/27/22- 02:13:31.890200	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	47844	52869	192.168.2.23	156.238.61.110
192.168.2.23156.230.26.2 3059828528692027339 05/27/22- 02:15:29.650636	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	59828	52869	192.168.2.23	156.230.26.230

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.250.95.1 3541928372152835222 05/27/22- 02:15:55.855853	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41928	37215	192.168.2.23	156.250.95.135
192.168.2.23156.244.103. 20155744372152835222 05/27/22- 02:13:30.822378	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55744	37215	192.168.2.23	156.244.103.201
192.168.2.23156.232.89.1 1239742528692027339 05/27/22- 02:16:03.547915	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39742	52869	192.168.2.23	156.232.89.112
192.168.2.23156.245.52.2 1637384372152835222 05/27/22- 02:13:57.603579	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37384	37215	192.168.2.23	156.245.52.216
192.168.2.23156.250.124. 11133152372152835222 05/27/22- 02:14:34.749820	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33152	37215	192.168.2.23	156.250.124.111
192.168.2.23156.254.34.1 7034528528692027339 05/27/22- 02:14:56.885248	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34528	52869	192.168.2.23	156.254.34.170
192.168.2.23156.245.54.1 4049164372152835222 05/27/22- 02:13:24.836193	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49164	37215	192.168.2.23	156.245.54.140
192.168.2.23156.238.32.3 845886372152835222 05/27/22- 02:14:00.364163	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45886	37215	192.168.2.23	156.238.32.38
192.168.2.23156.241.95.8 757264372152835222 05/27/22- 02:15:19.224623	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57264	37215	192.168.2.23	156.241.95.87
192.168.2.23156.244.107. 9559450528692027339 05/27/22- 02:12:46.370080	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	59450	52869	192.168.2.23	156.244.107.95
192.168.2.23156.230.24.1 3137042372152835222 05/27/22- 02:16:06.079051	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37042	37215	192.168.2.23	156.230.24.131
192.168.2.23156.235.104. 14141364372152835222 05/27/22- 02:14:07.440368	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41364	37215	192.168.2.23	156.235.104.141
192.168.2.23197.246.193. 4154768372152835222 05/27/22- 02:14:18.135266	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54768	37215	192.168.2.23	197.246.193.41
192.168.2.23156.230.30.1 9348628372152835222 05/27/22- 02:13:14.410059	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48628	37215	192.168.2.23	156.230.30.193
192.168.2.23156.241.91.7 440776372152835222 05/27/22- 02:12:44.206867	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40776	37215	192.168.2.23	156.241.91.74
192.168.2.23156.226.60.8 58916372152835222 05/27/22- 02:13:06.892359	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58916	37215	192.168.2.23	156.226.60.8
192.168.2.23156.241.74.2 3548190528692027339 05/27/22- 02:13:26.081860	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48190	52869	192.168.2.23	156.241.74.235
192.168.2.23156.244.99.2 3254506528692027339 05/27/22- 02:14:08.659215	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54506	52869	192.168.2.23	156.244.99.232
192.168.2.23156.245.48.1 4135426528692027339 05/27/22- 02:12:50.304313	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	35426	52869	192.168.2.23	156.245.48.141

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.235.97.343730852869202733905/27/22-02:12:59.940810	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	37308	52869	192.168.2.23	156.235.97.34
192.168.2.23156.244.88.176415903721528352205/27/22-02:15:56.186019	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41590	37215	192.168.2.23	156.244.88.176
192.168.2.23156.250.15.254745052869202733905/27/22-02:13:49.655052	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	47450	52869	192.168.2.23	156.250.15.25
192.168.2.23156.224.29.180441825286920273390505/27/22-02:14:53.146841	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44182	52869	192.168.2.23	156.224.29.180
192.168.2.23156.226.85.266020052869202733905/27/22-02:12:57.635007	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	60200	52869	192.168.2.23	156.226.85.26
192.168.2.23156.225.132.194535383721528352205/27/22-02:14:15.265038	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53538	37215	192.168.2.23	156.225.132.194
192.168.2.23156.250.88.124400163721528352205/27/22-02:12:51.593923	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40016	37215	192.168.2.23	156.250.88.124
192.168.2.23156.244.97.231482603721528352205/27/22-02:14:22.025068	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48260	37215	192.168.2.23	156.244.97.231
192.168.2.23156.226.14.123327052869202733905/27/22-02:14:00.689986	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33270	52869	192.168.2.23	156.226.14.12
192.168.2.2341.0.84.773652452869202733905/27/22-02:14:50.212272	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	36524	52869	192.168.2.23	41.0.84.77
192.168.2.23156.238.61.225510845286920273390505/27/22-02:14:54.636072	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	51084	52869	192.168.2.23	156.238.61.225
192.168.2.23156.241.106.95372163721528352205/27/22-02:13:44.364053	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37216	37215	192.168.2.23	156.241.106.95
192.168.2.23156.225.132.208524445286920273390505/27/22-02:14:02.725896	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52444	52869	192.168.2.23	156.225.132.208
192.168.2.23156.245.51.404436852869202733905/27/22-02:15:28.190347	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44368	52869	192.168.2.23	156.245.51.40
192.168.2.23156.241.73.264747637215283522205/27/22-02:15:29.455772	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47476	37215	192.168.2.23	156.241.73.26
192.168.2.23156.226.70.214578585286920273390505/27/22-02:15:25.590511	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57858	52869	192.168.2.23	156.226.70.214
192.168.2.23156.241.10.405057837215283522205/27/22-02:13:29.590300	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50578	37215	192.168.2.23	156.241.10.40
192.168.2.23156.224.29.173533803721528352205/27/22-02:13:45.539483	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53380	37215	192.168.2.23	156.224.29.173
192.168.2.23156.224.23.925852637215283522205/27/22-02:13:24.790368	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58526	37215	192.168.2.23	156.224.23.92

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.226.94.875965037215283522205/27/22-02:14:18.028243	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59650	37215	192.168.2.23	156.226.94.87
192.168.2.23156.225.136.124439023721528352222205/27/22-02:15:26.194360	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43902	37215	192.168.2.23	156.225.136.124
192.168.2.23156.238.54.1684511837215283522205/27/22-02:14:18.028002	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45118	37215	192.168.2.23	156.238.54.168
192.168.2.23156.226.69.4648562372152835222205/27/22-02:13:04.054928	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48562	37215	192.168.2.23	156.226.69.46
192.168.2.23156.241.68.4039378372152835222205/27/22-02:13:23.904907	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39378	37215	192.168.2.23	156.241.68.40
192.168.2.23156.244.123.215419225286920273395/27/22-02:13:00.537684	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	41922	52869	192.168.2.23	156.244.123.215
192.168.2.23156.238.51.755107037215283522205/27/22-02:13:49.473187	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51070	37215	192.168.2.23	156.238.51.75
192.168.2.23156.244.71.2514510637215283522205/27/22-02:15:24.727191	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45106	37215	192.168.2.23	156.244.71.251
192.168.2.23156.232.90.704894852869202733905/27/22-02:16:03.715684	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48948	52869	192.168.2.23	156.232.90.70
192.168.2.23156.235.98.635223252869202733905/27/22-02:14:31.680197	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52232	52869	192.168.2.23	156.235.98.63
192.168.2.23156.226.71.885208852869202733905/27/22-02:15:08.130201	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52088	52869	192.168.2.23	156.226.71.88
192.168.2.23156.254.54.197442803721528352222205/27/22-02:14:52.946969	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44280	37215	192.168.2.23	156.254.54.197
192.168.2.23156.250.12.036632372152835222205/27/22-02:13:03.624342	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36632	37215	192.168.2.23	156.250.12.0
192.168.2.23156.250.8.554679452869202733905/27/22-02:16:01.823422	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46794	52869	192.168.2.23	156.250.8.55
192.168.2.23156.244.70.595189252869202733905/27/22-02:12:43.767721	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	51892	52869	192.168.2.23	156.244.70.59
192.168.2.23156.241.125.5538080528692027339205/27/22-02:13:56.593665	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38080	52869	192.168.2.23	156.241.125.55
192.168.2.23156.235.96.854468652869202733905/27/22-02:14:39.577991	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44686	52869	192.168.2.23	156.235.96.85
192.168.2.23156.241.79.200551103721528352222205/27/22-02:13:33.332911	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55110	37215	192.168.2.23	156.241.79.200
192.168.2.23156.227.247.3046224528692027339205/27/22-02:15:17.885570	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46224	52869	192.168.2.23	156.227.247.30

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.250.116.4956468528692027339 05/27/22-02:15:59.528866	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	56468	52869	192.168.2.23	156.250.116.49
192.168.2.23156.226.67.6038562528692027339 05/27/22-02:15:49.696382	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38562	52869	192.168.2.23	156.226.67.60
192.168.2.23156.240.109.20643920372152835222 05/27/22-02:12:42.296506	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43920	37215	192.168.2.23	156.240.109.206
192.168.2.23156.241.125.22534114528692027339 05/27/22-02:13:00.075937	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34114	52869	192.168.2.23	156.241.125.225
192.168.2.23156.244.111.22336972372152835222 05/27/22-02:14:51.973133	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36972	37215	192.168.2.23	156.244.111.223
192.168.2.23156.227.244.16356848372152835222 05/27/22-02:14:51.959326	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56848	37215	192.168.2.23	156.227.244.163
192.168.2.23156.254.91.2063591437215283522 05/27/22-02:14:39.039040	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35914	37215	192.168.2.23	156.254.91.206
192.168.2.23156.244.109.19948556372152835222 05/27/22-02:14:22.555051	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48556	37215	192.168.2.23	156.244.109.199
192.168.2.23156.241.100.15653238528692027339 05/27/22-02:14:06.366393	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	53238	52869	192.168.2.23	156.241.100.156
192.168.2.23156.226.49.1635057837215283522 05/27/22-02:15:29.431320	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50578	37215	192.168.2.23	156.226.49.163
192.168.2.23156.254.97.1714816837215283522 05/27/22-02:15:39.488038	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48168	37215	192.168.2.23	156.254.97.171
192.168.2.23156.226.106.16754500528692027339 05/27/22-02:15:20.331149	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54500	52869	192.168.2.23	156.226.106.167
192.168.2.23156.241.79.1345559237215283522 05/27/22-02:13:17.995176	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55592	37215	192.168.2.23	156.241.79.134
192.168.2.23156.226.75.464851652869202733 9 05/27/22-02:14:01.198799	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48516	52869	192.168.2.23	156.226.75.46
192.168.2.23156.225.141.19958162528692027339 05/27/22-02:13:05.395964	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58162	52869	192.168.2.23	156.225.141.199
192.168.2.23156.254.58.2375543037215283522 05/27/22-02:14:57.299845	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55430	37215	192.168.2.23	156.254.58.237
192.168.2.23156.244.85.1284911452869202733 9 05/27/22-02:14:32.261733	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	49114	52869	192.168.2.23	156.244.85.128
192.168.2.23156.230.16.4544966528692027339 05/27/22-02:15:51.760200	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54496	52869	192.168.2.23	156.230.16.4
192.168.2.23156.225.138.11251752372152835222 05/27/22-02:13:57.830736	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51752	37215	192.168.2.23	156.225.138.112

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.226.106.71472583721528352225/27/22-02:15:03.890871	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47258	37215	192.168.2.23	156.226.106.71
192.168.2.23156.250.15.23946968528692027339 05/27/22-02:15:47.192692	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46968	52869	192.168.2.23	156.250.15.239
192.168.2.23156.245.58.4448610372152835222 05/27/22-02:13:46.898085	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48610	37215	192.168.2.23	156.245.58.44
192.168.2.23156.247.25.15648536528692027339 05/27/22-02:12:46.612785	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48536	52869	192.168.2.23	156.247.25.156
192.168.2.23156.241.133.24056286372152835222 05/27/22-02:13:39.348628	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56286	37215	192.168.2.23	156.241.133.240
192.168.2.23156.230.28.7345884528692027339 05/27/22-02:15:39.186764	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	45884	52869	192.168.2.23	156.230.28.73
192.168.2.23156.226.56.2414448528692027339 05/27/22-02:14:31.741771	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44482	52869	192.168.2.23	156.226.56.241
192.168.2.23156.235.97.1665848528692027339 05/27/22-02:13:34.854493	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54848	52869	192.168.2.23	156.235.97.166
192.168.2.23156.225.132.20736434372152835222 05/27/22-02:12:42.088150	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36434	37215	192.168.2.23	156.225.132.207
192.168.2.23156.247.20.1023700652869202733905/27/22-02:12:57.512512	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	37006	52869	192.168.2.23	156.247.20.102
192.168.2.23156.241.127.19738718528692027339 05/27/22-02:12:53.360210	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38718	52869	192.168.2.23	156.241.127.197
192.168.2.23156.224.31.5834264372152835222 05/27/22-02:14:00.300631	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34264	37215	192.168.2.23	156.224.31.58
192.168.2.23156.238.62.614109452869202733905/27/22-02:15:44.833472	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	41094	52869	192.168.2.23	156.238.62.61
192.168.2.23156.238.61.1983860437215283522205/27/22-02:12:42.098117	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38604	37215	192.168.2.23	156.238.61.198
192.168.2.23156.225.137.12950458528692027339 05/27/22-02:15:07.743958	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	50458	52869	192.168.2.23	156.225.137.129
192.168.2.23156.254.97.1955599452869202733905/27/22-02:16:00.365402	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55994	52869	192.168.2.23	156.254.97.195
192.168.2.23156.254.107.1652176528692027339 05/27/22-02:16:02.078691	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52176	52869	192.168.2.23	156.254.107.16
192.168.2.23156.241.104.15951580372152835222 05/27/22-02:14:33.327999	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51580	37215	192.168.2.23	156.241.104.159
192.168.2.23156.254.39.2355256652869202733905/27/22-02:15:32.125041	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52566	52869	192.168.2.23	156.254.39.235

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.247.21.7 352968528692027339 05/27/22-02:15:49.939246	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52968	52869	192.168.2.23	156.247.21.73
192.168.2.23156.241.13.1 957972372152835222 05/27/22-02:15:29.464566	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57972	37215	192.168.2.23	156.241.13.19
192.168.2.23156.226.15.2 155130528692027339 05/27/22-02:13:27.026150	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55130	52869	192.168.2.23	156.226.15.21
192.168.2.23156.245.49.3 753600528692027339 05/27/22-02:14:26.799092	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	53600	52869	192.168.2.23	156.245.49.37
192.168.2.23156.240.105. 15933672528692027339 05/27/22-02:13:00.042953	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33672	52869	192.168.2.23	156.240.105.159
192.168.2.23197.0.78.138 43770372152835222 05/27/22-02:15:44.616626	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43770	37215	192.168.2.23	197.0.78.138
192.168.2.23156.244.91.1 645155237215283522 2 05/27/22-02:15:48.271631	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51552	37215	192.168.2.23	156.244.91.164
192.168.2.23156.245.50.7 248118372152835222 05/27/22-02:14:06.437344	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48118	37215	192.168.2.23	156.245.50.72
192.168.2.23156.245.56.1 735596437215283522 2 05/27/22-02:14:01.873343	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55964	37215	192.168.2.23	156.245.56.173
192.168.2.23156.245.58.2 256504528692027339 05/27/22-02:14:37.543936	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	56504	52869	192.168.2.23	156.245.58.22
192.168.2.23156.224.23.1 6048230372152835222 05/27/22-02:14:38.368764	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48230	37215	192.168.2.23	156.224.23.160
192.168.2.23156.227.245. 22632786372152835222 05/27/22-02:15:19.170164	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	32786	37215	192.168.2.23	156.227.245.226
192.168.2.23156.241.133. 9933550528692027339 05/27/22-02:13:38.944703	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33550	52869	192.168.2.23	156.241.133.99
192.168.2.23156.224.30.1 6944296372152835222 05/27/22-02:14:00.475775	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44296	37215	192.168.2.23	156.224.30.169
192.168.2.23156.250.91.1 4250058372152835222 05/27/22-02:13:35.537847	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50058	37215	192.168.2.23	156.250.91.142
192.168.2.23156.226.25.2 2033464528692027339 05/27/22-02:13:45.425689	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	33464	52869	192.168.2.23	156.226.25.220
192.168.2.23156.247.17.8 54470528692027339 05/27/22-02:13:13.162457	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	54470	52869	192.168.2.23	156.247.17.8
192.168.2.23156.238.59.1 1555876528692027339 05/27/22-02:13:57.702025	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55876	52869	192.168.2.23	156.238.59.115
192.168.2.23156.225.140. 660912372152835222 05/27/22-02:15:40.316659	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60912	37215	192.168.2.23	156.225.140.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.241.98.775823528692027339 05/27/22-02:12:53.648941	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58232	52869	192.168.2.23	156.241.98.77
192.168.2.23156.254.54.155465123721528352225 05/27/22-02:14:38.804612	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46512	37215	192.168.2.23	156.254.54.155
192.168.2.23156.237.4.3337864528692027339 05/27/22-02:15:46.120268	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	37864	52869	192.168.2.23	156.237.4.33
192.168.2.23156.241.102.13036626372152835222 05/27/22-02:13:15.647863	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36626	37215	192.168.2.23	156.241.102.130
192.168.2.23156.224.12.383349237215283522 05/27/22-02:15:58.248459	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33492	37215	192.168.2.23	156.224.12.38
192.168.2.23156.240.108.15747280528692027339 05/27/22-02:13:57.669807	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	47280	52869	192.168.2.23	156.240.108.157
192.168.2.23156.241.95.1045716452869202733 9 05/27/22-02:13:04.404090	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57164	52869	192.168.2.23	156.241.95.104
192.168.2.23156.245.51.844248452869202733 9 05/27/22-02:15:11.333358	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	42484	52869	192.168.2.23	156.245.51.84
192.168.2.23156.254.92.264385237215283522 05/27/22-02:14:35.952032	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43852	37215	192.168.2.23	156.254.92.26
192.168.2.23156.241.74.715775528692027339 05/27/22-02:14:36.906433	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57752	52869	192.168.2.23	156.241.74.71
192.168.2.23156.244.114.18634296528692027339 05/27/22-02:14:00.653295	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34296	52869	192.168.2.23	156.244.114.186
192.168.2.23156.224.20.170345045286920273 39 05/27/22-02:13:34.854326	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	34504	52869	192.168.2.23	156.224.20.170
192.168.2.23156.245.57.168585123721528352225 05/27/22-02:12:59.620616	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58512	37215	192.168.2.23	156.245.57.168
192.168.2.23156.238.52.111511283721528352225 05/27/22-02:13:41.136266	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51128	37215	192.168.2.23	156.238.52.111
192.168.2.2341.140.12.139536343721528352225 05/27/22-02:14:56.565566	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53634	37215	192.168.2.23	41.140.12.139
192.168.2.23156.226.87.229475023721528352225 05/27/22-02:14:13.155214	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47502	37215	192.168.2.23	156.226.87.229
192.168.2.23156.224.22.154459325286920273 39 05/27/22-02:12:52.902558	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	45932	52869	192.168.2.23	156.224.22.154
192.168.2.23156.225.137.22469605286920273 39 05/27/22-02:14:37.082380	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46960	52869	192.168.2.23	156.225.137.22
192.168.2.23156.235.100.77601145286920273 39 05/27/22-02:13:38.665239	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	60114	52869	192.168.2.23	156.235.100.77

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.241.80.852088528692027339 05/27/22-02:13:40.714340	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52088	52869	192.168.2.23	156.241.80.8
192.168.2.23156.254.78.144397605286920273390 5/27/22-02:15:10.377160	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39760	52869	192.168.2.23	156.254.78.144
192.168.2.23156.241.75.545323837215283522205/27/22-02:15:24.966301	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53238	37215	192.168.2.23	156.241.75.54
192.168.2.23156.226.73.139329283721528352220 5/27/22-02:16:02.988563	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	32928	37215	192.168.2.23	156.226.73.139
192.168.2.23156.254.56.201433983721528352220 5/27/22-02:13:57.860088	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43398	37215	192.168.2.23	156.254.56.201
192.168.2.23156.225.132.151587265286920273390 5/27/22-02:14:53.211027	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58726	52869	192.168.2.23	156.225.132.151
192.168.2.23156.254.49.843718052869202733905/27/22-02:15:29.068878	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	37180	52869	192.168.2.23	156.254.49.84
192.168.2.23156.254.57.195242052869202733905/27/22-02:12:41.170166	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52420	52869	192.168.2.23	156.254.57.19
192.168.2.23156.241.71.140498183721528352220 5/27/22-02:13:17.716844	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49818	37215	192.168.2.23	156.241.71.140
192.168.2.23156.226.76.208391323721528352220 5/27/22-02:12:36.342235	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39132	37215	192.168.2.23	156.226.76.208
192.168.2.23156.254.80.215807037215283522205/27/22-02:13:06.666292	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58070	37215	192.168.2.23	156.254.80.21
192.168.2.23156.224.15.803328437215283522205/27/22-02:13:11.149360	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33284	37215	192.168.2.23	156.224.15.80
192.168.2.23156.250.94.192505703721528352220 5/27/22-02:15:59.700334	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50570	37215	192.168.2.23	156.250.94.192
192.168.2.23156.254.54.284754452869202733905/27/22-02:13:35.459409	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	47544	52869	192.168.2.23	156.254.54.28
192.168.2.23156.238.62.744515528692027339 05/27/22-02:13:56.811726	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	45152	52869	192.168.2.23	156.238.62.74
192.168.2.23156.226.62.167353403721528352220 5/27/22-02:14:12.939722	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35340	37215	192.168.2.23	156.226.62.167
192.168.2.23156.245.63.194553883721528352220 5/27/22-02:12:59.125522	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55388	37215	192.168.2.23	156.245.63.194
192.168.2.23156.235.100.95609663721528352220 5/27/22-02:14:10.940139	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60966	37215	192.168.2.23	156.235.100.95
192.168.2.23156.254.104.345764852869202733905/27/22-02:16:02.071437	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57648	52869	192.168.2.23	156.254.104.34

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.241.78.1495042372152835222 05/27/22-02:14:26.066500	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50422	37215	192.168.2.23	156.241.78.149
192.168.2.23156.254.47.2243716372152835222 05/27/22-02:15:59.755311	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43716	37215	192.168.2.23	156.254.47.22
192.168.2.23156.241.103.1856104528692027339 05/27/22-02:13:20.893383	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	56104	52869	192.168.2.23	156.241.103.18
192.168.2.23197.234.59.4655500528692027339 05/27/22-02:15:10.654032	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	55500	52869	192.168.2.23	197.234.59.46
192.168.2.23156.230.27.7046850528692027339 05/27/22-02:15:23.381190	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	46850	52869	192.168.2.23	156.230.27.70
192.168.2.23156.238.19.8649444372152835222 05/27/22-02:13:01.184283	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49444	37215	192.168.2.23	156.238.19.86
192.168.2.23156.241.112.22458220528692027339 05/27/22-02:13:33.393126	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58220	52869	192.168.2.23	156.241.112.224
192.168.2.23156.250.118.9651618528692027339 05/27/22-02:13:39.114643	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	51618	52869	192.168.2.23	156.250.118.96
192.168.2.23156.226.72.1305668037215283522 05/27/22-02:15:30.266729	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56680	37215	192.168.2.23	156.226.72.130
192.168.2.23156.238.62.1395316452869202733 9 05/27/22-02:15:44.702643	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	53164	52869	192.168.2.23	156.238.62.139
192.168.2.23156.241.98.1715974052869202733 9 05/27/22-02:13:40.694540	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	59740	52869	192.168.2.23	156.241.98.171
192.168.2.23156.250.13.2475312637215283522 05/27/22-02:13:53.272848	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53126	37215	192.168.2.23	156.250.13.247
192.168.2.23197.232.16.1223820652869202733 9 05/27/22-02:14:46.558798	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	38206	52869	192.168.2.23	197.232.16.122
192.168.2.23156.250.122.21842844528692027339 05/27/22-02:13:23.578725	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	42844	52869	192.168.2.23	156.250.122.218
192.168.2.23156.245.54.1685824452869202733 9 05/27/22-02:14:56.952383	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58244	52869	192.168.2.23	156.245.54.168
192.168.2.23156.254.47.2196086637215283522 05/27/22-02:15:22.673219	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60866	37215	192.168.2.23	156.254.47.219
192.168.2.23156.224.21.2145895652869202733 9 05/27/22-02:12:49.830344	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58956	52869	192.168.2.23	156.224.21.214
192.168.2.23156.244.65.2942292528692027339 05/27/22-02:13:38.739294	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	42292	52869	192.168.2.23	156.244.65.29
192.168.2.23156.250.120.1914466852869202733 9 05/27/22-02:15:04.565007	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44668	52869	192.168.2.23	156.250.120.191

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.254.83.3 549398372152835222 05/27/22-02:14:56.478107	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49398	37215	192.168.2.23	156.254.83.35
192.168.2.23156.250.89.1 684743037215283522 2 05/27/22-02:14:33.492223	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47430	37215	192.168.2.23	156.250.89.168
192.168.2.23156.241.8.18 160434372152835222 05/27/22-02:14:17.531747	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60434	37215	192.168.2.23	156.241.8.181
192.168.2.23156.245.56.1 7547336372152835222 05/27/22-02:13:30.930123	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47336	37215	192.168.2.23	156.245.56.175
192.168.2.23156.244.96.2 2958766528692027339 05/27/22-02:14:59.658492	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	58766	52869	192.168.2.23	156.244.96.229
192.168.2.23156.245.60.2 0657106528692027339 05/27/22-02:15:57.085948	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57106	52869	192.168.2.23	156.245.60.206
192.168.2.23156.225.142. 22242424528692027339 05/27/22-02:14:34.289205	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	42424	52869	192.168.2.23	156.225.142.222
192.168.2.23156.224.22.2 3044286528692027339 05/27/22-02:15:39.353713	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44286	52869	192.168.2.23	156.224.22.230
192.168.2.23156.227.240. 22844512372152835222 05/27/22-02:12:36.138433	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44512	37215	192.168.2.23	156.227.240.228
192.168.2.23156.254.111. 23043658528692027339 05/27/22-02:13:56.928093	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	43658	52869	192.168.2.23	156.254.111.230
192.168.2.23156.241.122. 2954938372152835222 05/27/22-02:16:05.477682	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54938	37215	192.168.2.23	156.241.122.29
192.168.2.23156.241.102. 20257920528692027339 05/27/22-02:13:49.854598	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	57920	52869	192.168.2.23	156.241.102.202
192.168.2.23156.232.95.5 536332372152835222 05/27/22-02:14:42.534896	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36332	37215	192.168.2.23	156.232.95.55
192.168.2.23156.254.66.1 3938366372152835222 05/27/22-02:13:08.640227	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38366	37215	192.168.2.23	156.254.66.139
192.168.2.23156.250.121. 7352058372152835222 05/27/22-02:15:27.222565	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52058	37215	192.168.2.23	156.250.121.73
192.168.2.23156.250.94.9 154174372152835222 05/27/22-02:13:40.148680	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54174	37215	192.168.2.23	156.250.94.91
192.168.2.23156.244.117. 12852300372152835222 05/27/22-02:14:01.942691	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52300	37215	192.168.2.23	156.244.117.128
192.168.2.23156.241.112. 15944218372152835222 05/27/22-02:15:38.230922	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44218	37215	192.168.2.23	156.241.112.159
192.168.2.23156.240.104. 2144700372152835222 05/27/22-02:14:10.957392	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44700	37215	192.168.2.23	156.240.104.21

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.250.91.4 841964528692027339 05/27/22- 02:14:37.762120	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	41964	52869	192.168.2.23	156.250.91.48
192.168.2.23156.254.39.1 8756308372152835222 05/27/22- 02:15:19.193274	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56308	37215	192.168.2.23	156.254.39.187
192.168.2.23156.241.121. 14844116528692027339 05/27/22- 02:15:11.303838	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	44116	52869	192.168.2.23	156.241.121.148
192.168.2.23156.226.49.1 8046232372152835222 05/27/22- 02:13:29.334888	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46232	37215	192.168.2.23	156.226.49.180
192.168.2.23156.238.55.7 957326372152835222 05/27/22- 02:13:52.055223	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57326	37215	192.168.2.23	156.238.55.79
192.168.2.23156.238.48.1 0159654372152835222 05/27/22- 02:14:41.192161	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59654	37215	192.168.2.23	156.238.48.101
192.168.2.23156.238.55.2 340874372152835222 05/27/22- 02:14:26.852111	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40874	37215	192.168.2.23	156.238.55.23
192.168.2.23156.238.58.2 4843112528692027339 05/27/22- 02:14:07.437398	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	43112	52869	192.168.2.23	156.238.58.248
192.168.2.23156.226.74.5 539048528692027339 05/27/22- 02:13:35.207018	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39048	52869	192.168.2.23	156.226.74.55
192.168.2.23156.241.106. 24156282372152835222 05/27/22- 02:15:11.455257	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56282	37215	192.168.2.23	156.241.106.241
192.168.2.23156.250.122. 18154144372152835222 05/27/22- 02:12:51.092716	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54144	37215	192.168.2.23	156.250.122.181
192.168.2.23156.241.94.1 1739036528692027339 05/27/22- 02:14:09.966616	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	39036	52869	192.168.2.23	156.241.94.117
192.168.2.23156.224.20.1 9748634528692027339 05/27/22- 02:14:19.780807	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	48634	52869	192.168.2.23	156.224.20.197
192.168.2.23156.240.105. 9251254372152835222 05/27/22- 02:15:03.950087	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51254	37215	192.168.2.23	156.240.105.92
192.168.2.23156.239.155. 14145504372152835222 05/27/22- 02:14:38.834279	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45504	37215	192.168.2.23	156.239.155.141
192.168.2.23156.235.108. 4034412372152835222 05/27/22- 02:14:52.871348	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34412	37215	192.168.2.23	156.235.108.40
192.168.2.23156.241.89.1 5352104528692027339 05/27/22- 02:13:27.225645	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	52104	52869	192.168.2.23	156.241.89.153
192.168.2.23156.235.103. 20747134372152835222 05/27/22- 02:15:58.666213	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47134	37215	192.168.2.23	156.235.103.207
192.168.2.23156.244.88.7 459642372152835222 05/27/22- 02:12:37.779404	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59642	37215	192.168.2.23	156.244.88.74

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.241.78.17349703721528352220 5/27/22-02:15:55.887379	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34970	37215	192.168.2.23	156.241.78.17
192.168.2.23156.254.58.28496265286920273390 5/27/22-02:14:03.905575	TCP	2027339	ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound	49626	52869	192.168.2.23	156.254.58.28

TCP Packets

System Behavior

Analysis Process: N0hjaP1acV PID: 6229, Parent PID: 6122

General

Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	/tmp/N0hjaP1acV
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: N0hjaP1acV PID: 6231, Parent PID: 6229

General

Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: N0hjaP1acV PID: 6232, Parent PID: 6229

General

Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: N0hjaP1acV PID: 6233, Parent PID: 6229

General

Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: N0hjaP1acV PID: 6235, Parent PID: 6229

Copyright Joe Security LLC 2022

General	
Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: N0hjaP1acV PID: **6237**, Parent PID: **6229**

General	
Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: N0hjaP1acV PID: **6241**, Parent PID: **6229**

General	
Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: N0hjaP1acV PID: **6245**, Parent PID: **6241**

General	
Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: N0hjaP1acV PID: **6256**, Parent PID: **6245**

General	
Start time:	02:12:38
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: N0hjaP1acV PID: **6258**, Parent PID: **6256**

General	
Start time:	02:12:38
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Copyright Joe Security LLC 2022

Analysis Process: N0hjaP1acV PID: **6248**, Parent PID: **6241**

General

Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: N0hjaP1acV PID: **6250**, Parent PID: **6248**

General

Start time:	02:12:31
Start date:	27/05/2022
Path:	/tmp/N0hjaP1acV
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Copyright Joe Security LLC 2022