ID: 679628
Sample Name: notabotnet.arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:18:31
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

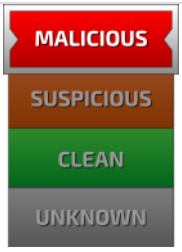
notabotnet.arm

Overview

General Information

Sample Name:	notabotnet.arm
Analysis ID:	679628
MD5:	d8edb88e8280e2.
SHA1:	d9262e6ab9d9a9.
SHA256:	4d365f4c4e3f946..
Tags:	Mirai
Infos:	

Detection



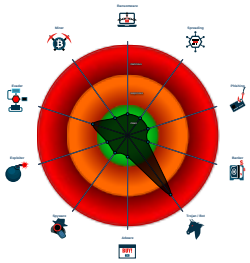
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Connects to many ports of the same…
- Uses known network protocols on n…
- Yara signature match
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Detected TCP or UDP traffic on non…
- Sample listens on a socket

Classification



Analysis Advice

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

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

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

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679628
Start date and time: 06/08/202207:18:31	2022-08-06 07:18:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	notabotnet.arm
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:	mal80.troj.linARM@0/0@1/0

Warnings

Runtime Messages

Command:	/tmp/notabotnet.arm
PID:	6236
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	xXxSlicexXxxVEGA.

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- notabotnet.arm (PID: 6236, Parent: 6127, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/notabotnet.arm
  - notabotnet.arm New Fork (PID: 6238, Parent: 6236)
  - notabotnet.arm New Fork (PID: 6239, Parent: 6236)
    - notabotnet.arm New Fork (PID: 6241, Parent: 6239)
    - notabotnet.arm New Fork (PID: 6243, Parent: 6239)
    - notabotnet.arm New Fork (PID: 6246, Parent: 6239)
    - notabotnet.arm New Fork (PID: 6248, Parent: 6239)
    - notabotnet.arm New Fork (PID: 6251, Parent: 6239)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
notabotnet.arm	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x12fa8:$xo1: Dfs`eeh&<'9 • 0x13020:$xo1: Dfs`eeh&<'9 • 0x13094:$xo1: Dfs`eeh&<'9 • 0x13104:$xo1: Dfs`eeh&<'9 • 0x13150:$xo1: Dfs`eeh&<'9
notabotnet.arm	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6238.1.00007f5fa8033000.00007f5fa8034000.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x528:$xo1: Dfs`eeh&<'9 • 0x5a4:$xo1: Dfs`eeh&<'9 • 0x61c:$xo1: Dfs`eeh&<'9 • 0x690:$xo1: Dfs`eeh&<'9 • 0x6e0:$xo1: Dfs`eeh&<'9
6241.1.00007f5fa8032000.00007f5fa8033000.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x20:$xo1: Dfs`eeh&<'9 • 0x94:$xo1: Dfs`eeh&<'9 • 0x104:$xo1: Dfs`eeh&<'9 • 0x150:$xo1: Dfs`eeh&<'9

Source	Rule	Description	Author	Strings
6241.1.00007f5fa8017000.00007f5fa802b000.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x12fa8:$xo1: Dfs`eeh&<'9 • 0x13020:$xo1: Dfs`eeh&<'9 • 0x13094:$xo1: Dfs`eeh&<'9 • 0x13104:$xo1: Dfs`eeh&<'9 • 0x13150:$xo1: Dfs`eeh&<'9
6241.1.00007f5fa8017000.00007f5fa802b000.r-x.sdmp	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
6236.1.00007f5fa8017000.00007f5fa802b000.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x12fa8:$xo1: Dfs`eeh&<'9 • 0x13020:$xo1: Dfs`eeh&<'9 • 0x13094:$xo1: Dfs`eeh&<'9 • 0x13104:$xo1: Dfs`eeh&<'9 • 0x13150:$xo1: Dfs`eeh&<'9
Click to see the 13 entries				

Snort Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 156.235.104.47

Timestamp:	192.168.2.23156.235.104.4736334372152835222 08/06/22-07:19:52.220960
SID:	2835222
Source Port:	36334
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: 156.235.104.85

Timestamp:	192.168.2.23156.235.104.8557800372152835222 08/06/22-07:19:39.853691
SID:	2835222
Source Port:	57800
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: 156.241.65.128

Timestamp:	192.168.2.23156.241.65.12841678372152835222 08/06/22-07:21:20.512607
SID:	2835222
Source Port:	41678
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: 156.241.116.44

Timestamp:	192.168.2.23156.241.116.4442230372152835222 08/06/22-07:20:00.956884
SID:	2835222
Source Port:	42230
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: 156.250.69.146	
Timestamp:	192.168.2.23156.250.69.14655152372152835222 08/06/22-07:19:39.989567
SID:	2835222
Source Port:	55152
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: 156.245.33.139	
Timestamp:	192.168.2.23156.245.33.13954504372152835222 08/06/22-07:19:52.314965
SID:	2835222
Source Port:	54504
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: 156.250.28.171	
Timestamp:	192.168.2.23156.250.28.17152738372152835222 08/06/22-07:20:29.967484
SID:	2835222
Source Port:	52738
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: 156.224.31.170	
Timestamp:	192.168.2.23156.224.31.17037664372152835222 08/06/22-07:20:49.079922
SID:	2835222
Source Port:	37664
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: 156.250.102.105	
Timestamp:	192.168.2.23156.250.102.10536504372152835222 08/06/22-07:20:29.956914
SID:	2835222
Source Port:	36504
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: 156.230.19.35	
Timestamp:	192.168.2.23156.230.19.3534282372152835222 08/06/22-07:20:27.532804
SID:	2835222
Source Port:	34282
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: 156.250.70.128	
Timestamp:	192.168.2.23156.250.70.12841324372152835222 08/06/22-07:21:02.363370
SID:	2835222
Source Port:	41324
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: 156.245.55.10	
Timestamp:	192.168.2.23156.245.55.1057952372152835222 08/06/22-07:19:21.831672
SID:	2835222
Source Port:	57952

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: 156.254.109.87

Timestamp:	192.168.2.23156.254.109.8743916372152835222 08/06/22-07:20:06.945366
SID:	2835222
Source Port:	43916
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: 156.250.115.240

Timestamp:	192.168.2.23156.250.115.240334203721528352222 08/06/22-07:21:20.543254
SID:	2835222
Source Port:	33420
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: 156.250.100.84

Timestamp:	192.168.2.23156.250.100.8457436372152835222 08/06/22-07:20:06.851930
SID:	2835222
Source Port:	57436
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: 156.241.99.17

Timestamp:	192.168.2.23156.241.99.1735304372152835222 08/06/22-07:19:43.361911
SID:	2835222
Source Port:	35304
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: 156.225.145.141

Timestamp:	192.168.2.23156.225.145.141559663721528352222 08/06/22-07:19:46.935588
SID:	2835222
Source Port:	55966
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a .tk domain - Likely Hostile - Source IP: 192.168.2.23 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.238.8.8.853706532012811 08/06/22-07:19:18.475451
SID:	2012811
Source Port:	53706
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 156.224.19.222

Timestamp:	192.168.2.23156.224.19.22252936372152835222 08/06/22-07:20:06.720074
SID:	2835222
Source Port:	52936
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: 156.224.9.206	
Timestamp:	192.168.2.23156.224.9.20653706372152835222 08/06/22-07:19:24.221104
SID:	2835222
Source Port:	53706
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: 156.245.56.125	
Timestamp:	192.168.2.23156.245.56.12560782372152835222 08/06/22-07:21:11.092379
SID:	2835222
Source Port:	60782
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: 156.226.75.228	
Timestamp:	192.168.2.23156.226.75.22833396372152835222 08/06/22-07:19:39.967769
SID:	2835222
Source Port:	33396
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: 156.250.94.104	
Timestamp:	192.168.2.23156.250.94.10446054372152835222 08/06/22-07:20:46.861808
SID:	2835222
Source Port:	46054
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: 156.244.93.42	
Timestamp:	192.168.2.23156.244.93.4250026372152835222 08/06/22-07:19:43.368461
SID:	2835222
Source Port:	50026
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: 156.238.15.204	
Timestamp:	192.168.2.23156.238.15.20444758372152835222 08/06/22-07:20:23.994081
SID:	2835222
Source Port:	44758
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: 156.245.36.181	
Timestamp:	192.168.2.23156.245.36.18148390372152835222 08/06/22-07:21:07.429076
SID:	2835222
Source Port:	48390
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: 156.245.60.140	
Timestamp:	192.168.2.23156.245.60.14053584372152835222 08/06/22-07:20:24.016463
SID:	2835222
Source Port:	53584

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: 156.226.30.161	
Timestamp:	192.168.2.23156.226.30.16142840372152835222 08/06/22-07:21:13.813244
SID:	2835222
Source Port:	42840
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: 156.235.104.136	
Timestamp:	192.168.2.23156.235.104.136380163721528352222 08/06/22-07:21:07.325992
SID:	2835222
Source Port:	38016
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: 156.241.125.136	
Timestamp:	192.168.2.23156.241.125.136563543721528352222 08/06/22-07:21:02.342117
SID:	2835222
Source Port:	56354
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: 156.250.15.224	
Timestamp:	192.168.2.23156.250.15.22444224372152835222 08/06/22-07:20:46.875148
SID:	2835222
Source Port:	44224
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: 156.230.25.40	
Timestamp:	192.168.2.23156.230.25.40525723721528352222 08/06/22-07:20:01.144639
SID:	2835222
Source Port:	52572
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: 156.241.103.120	
Timestamp:	192.168.2.23156.241.103.120467103721528352222 08/06/22-07:20:29.963710
SID:	2835222
Source Port:	46710
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: 156.244.125.1	
Timestamp:	192.168.2.23156.244.125.138204372152835222 08/06/22-07:20:00.952733
SID:	2835222
Source Port:	38204
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: 156.241.91.240	
Timestamp:	192.168.2.23156.241.91.24040938372152835222 08/06/22-07:19:24.295713
SID:	2835222
Source Port:	40938
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: 156.254.111.150	
Timestamp:	192.168.2.23156.254.111.15043388372152835222 08/06/22-07:20:01.152294
SID:	2835222
Source Port:	43388
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: 156.254.90.136	
Timestamp:	192.168.2.23156.254.90.13632874372152835222 08/06/22-07:19:24.221072
SID:	2835222
Source Port:	32874
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: 156.241.74.59	
Timestamp:	192.168.2.23156.241.74.5945650372152835222 08/06/22-07:21:17.178265
SID:	2835222
Source Port:	45650
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: 156.247.17.68	
Timestamp:	192.168.2.23156.247.17.6852950372152835222 08/06/22-07:19:25.518855
SID:	2835222
Source Port:	52950
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: 156.241.81.20	
Timestamp:	192.168.2.23156.241.81.2057262372152835222 08/06/22-07:20:46.869967
SID:	2835222
Source Port:	57262
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: 156.225.156.155	
Timestamp:	192.168.2.23156.225.156.155461283721528352222 08/06/22-07:21:13.807326
SID:	2835222
Source Port:	46128
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: 156.226.72.217	
Timestamp:	192.168.2.23156.226.72.21758034372152835222 08/06/22-07:20:49.212460
SID:	2835222
Source Port:	58034

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: 156.241.84.71	
Timestamp:	192.168.2.23156.241.84.7160110372152835222 08/06/22-07:19:25.876818
SID:	2835222
Source Port:	60110
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: 197.234.43.151	
Timestamp:	192.168.2.23197.234.43.151493343721528352222 08/06/22-07:19:52.351873
SID:	2835222
Source Port:	49334
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: 156.244.69.106	
Timestamp:	192.168.2.23156.244.69.10653374372152835222 08/06/22-07:19:29.489873
SID:	2835222
Source Port:	53374
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: 197.246.248.129	
Timestamp:	192.168.2.23197.246.248.129341303721528352222 08/06/22-07:20:39.259211
SID:	2835222
Source Port:	34130
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: 156.235.111.197	
Timestamp:	192.168.2.23156.235.111.197600863721528352222 08/06/22-07:21:07.326010
SID:	2835222
Source Port:	60086
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: 156.226.33.128	
Timestamp:	192.168.2.23156.226.33.12842834372152835222 08/06/22-07:20:07.122992
SID:	2835222
Source Port:	42834
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: 156.250.84.216	
Timestamp:	192.168.2.23156.250.84.21634314372152835222 08/06/22-07:21:13.530696
SID:	2835222
Source Port:	34314
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: 156.226.111.240	
Timestamp:	192.168.2.23156.226.111.24038052372152835222 08/06/22-07:21:07.604064
SID:	2835222
Source Port:	38052
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: 156.254.91.43	
Timestamp:	192.168.2.23156.254.91.4356600372152835222 08/06/22-07:19:52.243025
SID:	2835222
Source Port:	56600
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: 156.226.72.168	
Timestamp:	192.168.2.23156.226.72.16849466372152835222 08/06/22-07:20:00.976466
SID:	2835222
Source Port:	49466
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: 156.224.22.93	
Timestamp:	192.168.2.23156.224.22.9337258372152835222 08/06/22-07:19:46.797331
SID:	2835222
Source Port:	37258
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: 156.250.4.21	
Timestamp:	192.168.2.23156.250.4.2133800372152835222 08/06/22-07:19:29.496580
SID:	2835222
Source Port:	33800
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: 156.245.36.50	
Timestamp:	192.168.2.23156.245.36.5059962372152835222 08/06/22-07:20:07.124180
SID:	2835222
Source Port:	59962
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: 156.252.26.142	
Timestamp:	192.168.2.23156.252.26.14232834372152835222 08/06/22-07:19:29.389161
SID:	2835222
Source Port:	32834
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: 156.245.34.113	
Timestamp:	192.168.2.23156.245.34.11347958372152835222 08/06/22-07:20:53.752304
SID:	2835222
Source Port:	47958

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: 156.235.105.171	
Timestamp:	192.168.2.23156.235.105.171581203721528352222 08/06/22-07:20:00.838160
SID:	2835222
Source Port:	58120
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: 156.235.106.232	
Timestamp:	192.168.2.23156.235.106.232380523721528352222 08/06/22-07:19:46.804785
SID:	2835222
Source Port:	38052
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: 156.235.101.98	
Timestamp:	192.168.2.23156.235.101.9851636372152835222 08/06/22-07:21:11.184192
SID:	2835222
Source Port:	51636
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: 156.254.34.115	
Timestamp:	192.168.2.23156.254.34.11539034372152835222 08/06/22-07:20:06.738093
SID:	2835222
Source Port:	39034
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: 156.244.67.171	
Timestamp:	192.168.2.23156.244.67.17139928372152835222 08/06/22-07:20:54.031258
SID:	2835222
Source Port:	39928
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: 156.245.33.72	
Timestamp:	192.168.2.23156.245.33.7240872372152835222 08/06/22-07:19:43.361861
SID:	2835222
Source Port:	40872
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: 156.224.15.4	
Timestamp:	192.168.2.23156.224.15.453854372152835222 08/06/22-07:19:43.569760
SID:	2835222
Source Port:	53854
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: 156.244.101.196	
Timestamp:	192.168.2.23156.244.101.19635582372152835222 08/06/22-07:19:52.333819
SID:	2835222
Source Port:	35582
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: 197.238.136.194	
Timestamp:	192.168.2.23197.238.136.19433464372152835222 08/06/22-07:20:51.343241
SID:	2835222
Source Port:	33464
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: 156.225.153.226	
Timestamp:	192.168.2.23156.225.153.22651524372152835222 08/06/22-07:19:30.088494
SID:	2835222
Source Port:	51524
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: 156.227.241.65	
Timestamp:	192.168.2.23156.227.241.6543306372152835222 08/06/22-07:19:24.221136
SID:	2835222
Source Port:	43306
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: 156.240.104.170	
Timestamp:	192.168.2.23156.240.104.17051482372152835222 08/06/22-07:21:11.008228
SID:	2835222
Source Port:	51482
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: 156.241.8.155	
Timestamp:	192.168.2.23156.241.8.15538456372152835222 08/06/22-07:21:02.280154
SID:	2835222
Source Port:	38456
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: 156.244.84.167	
Timestamp:	192.168.2.23156.244.84.16735050372152835222 08/06/22-07:19:25.593415
SID:	2835222
Source Port:	35050
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: 156.238.60.21	
Timestamp:	192.168.2.23156.238.60.2147264372152835222 08/06/22-07:20:06.840968
SID:	2835222
Source Port:	47264

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: 156.241.90.49	
Timestamp:	192.168.2.23156.241.90.4941258372152835222 08/06/22-07:20:04.503966
SID:	2835222
Source Port:	41258
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: 156.250.127.75	
Timestamp:	192.168.2.23156.250.127.7536324372152835222 08/06/22-07:19:26.178572
SID:	2835222
Source Port:	36324
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: 156.226.33.59	
Timestamp:	192.168.2.23156.226.33.59429523721528352222 08/06/22-07:19:27.174349
SID:	2835222
Source Port:	42952
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: 156.244.74.195	
Timestamp:	192.168.2.23156.244.74.19541006372152835222 08/06/22-07:20:04.504021
SID:	2835222
Source Port:	41006
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: 156.250.124.11	
Timestamp:	192.168.2.23156.250.124.1149526372152835222 08/06/22-07:20:27.641269
SID:	2835222
Source Port:	49526
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: 156.244.72.51	
Timestamp:	192.168.2.23156.244.72.5148544372152835222 08/06/22-07:19:30.062165
SID:	2835222
Source Port:	48544
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: 156.244.90.79	
Timestamp:	192.168.2.23156.244.90.7934776372152835222 08/06/22-07:21:02.337983
SID:	2835222
Source Port:	34776
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: 156.226.35.147	
Timestamp:	192.168.2.23156.226.35.14742074372152835222 08/06/22-07:21:04.689014
SID:	2835222
Source Port:	42074
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: 156.225.148.36	
Timestamp:	192.168.2.23156.225.148.3636882372152835222 08/06/22-07:20:49.212415
SID:	2835222
Source Port:	36882
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: 156.241.67.223	
Timestamp:	192.168.2.23156.241.67.22337336372152835222 08/06/22-07:19:32.414471
SID:	2835222
Source Port:	37336
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: 156.244.103.61	
Timestamp:	192.168.2.23156.244.103.6132964372152835222 08/06/22-07:21:13.529327
SID:	2835222
Source Port:	32964
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: 156.250.105.255	
Timestamp:	192.168.2.23156.250.105.25554474372152835222 08/06/22-07:19:26.154807
SID:	2835222
Source Port:	54474
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: 156.224.21.151	
Timestamp:	192.168.2.23156.224.21.15147910372152835222 08/06/22-07:19:29.389496
SID:	2835222
Source Port:	47910
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: 156.250.113.0	
Timestamp:	192.168.2.23156.250.113.050732372152835222 08/06/22-07:20:24.003561
SID:	2835222
Source Port:	50732
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: 156.241.118.232	
Timestamp:	192.168.2.23156.241.118.23247680372152835222 08/06/22-07:21:04.696969
SID:	2835222
Source Port:	47680

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: 156.240.110.112	
Timestamp:	192.168.2.23156.240.110.11258798372152835222 08/06/22-07:19:32.332687
SID:	2835222
Source Port:	58798
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: 156.226.105.68	
Timestamp:	192.168.2.23156.226.105.6854090372152835222 08/06/22-07:20:58.709810
SID:	2835222
Source Port:	54090
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: 156.241.114.82	
Timestamp:	192.168.2.23156.241.114.8253964372152835222 08/06/22-07:20:46.873374
SID:	2835222
Source Port:	53964
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: 156.226.69.251	
Timestamp:	192.168.2.23156.226.69.25157096372152835222 08/06/22-07:21:13.836375
SID:	2835222
Source Port:	57096
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: 156.250.19.190	
Timestamp:	192.168.2.23156.250.19.19034684372152835222 08/06/22-07:21:20.519259
SID:	2835222
Source Port:	34684
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: 156.250.66.246	
Timestamp:	192.168.2.23156.250.66.24648736372152835222 08/06/22-07:19:25.592979
SID:	2835222
Source Port:	48736
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: 156.254.68.66	
Timestamp:	192.168.2.23156.254.68.6639534372152835222 08/06/22-07:21:13.731473
SID:	2835222
Source Port:	39534
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: 156.226.76.127	
Timestamp:	192.168.2.23156.226.76.12758024372152835222 08/06/22-07:21:07.140930
SID:	2835222
Source Port:	58024
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: 156.241.83.248	
Timestamp:	192.168.2.23156.241.83.24846166372152835222 08/06/22-07:19:29.498077
SID:	2835222
Source Port:	46166
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: 156.241.107.104	
Timestamp:	192.168.2.23156.241.107.10435974372152835222 08/06/22-07:21:00.015237
SID:	2835222
Source Port:	35974
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: 156.241.89.44	
Timestamp:	192.168.2.23156.241.89.4442634372152835222 08/06/22-07:19:39.964819
SID:	2835222
Source Port:	42634
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: 156.227.247.99	
Timestamp:	192.168.2.23156.227.247.9935490372152835222 08/06/22-07:19:32.332760
SID:	2835222
Source Port:	35490
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file

Networking

- Snort IDS alert for network traffic
- Connects to many ports of the same IP (likely port scanning)
- Uses known network protocols on non-standard ports

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

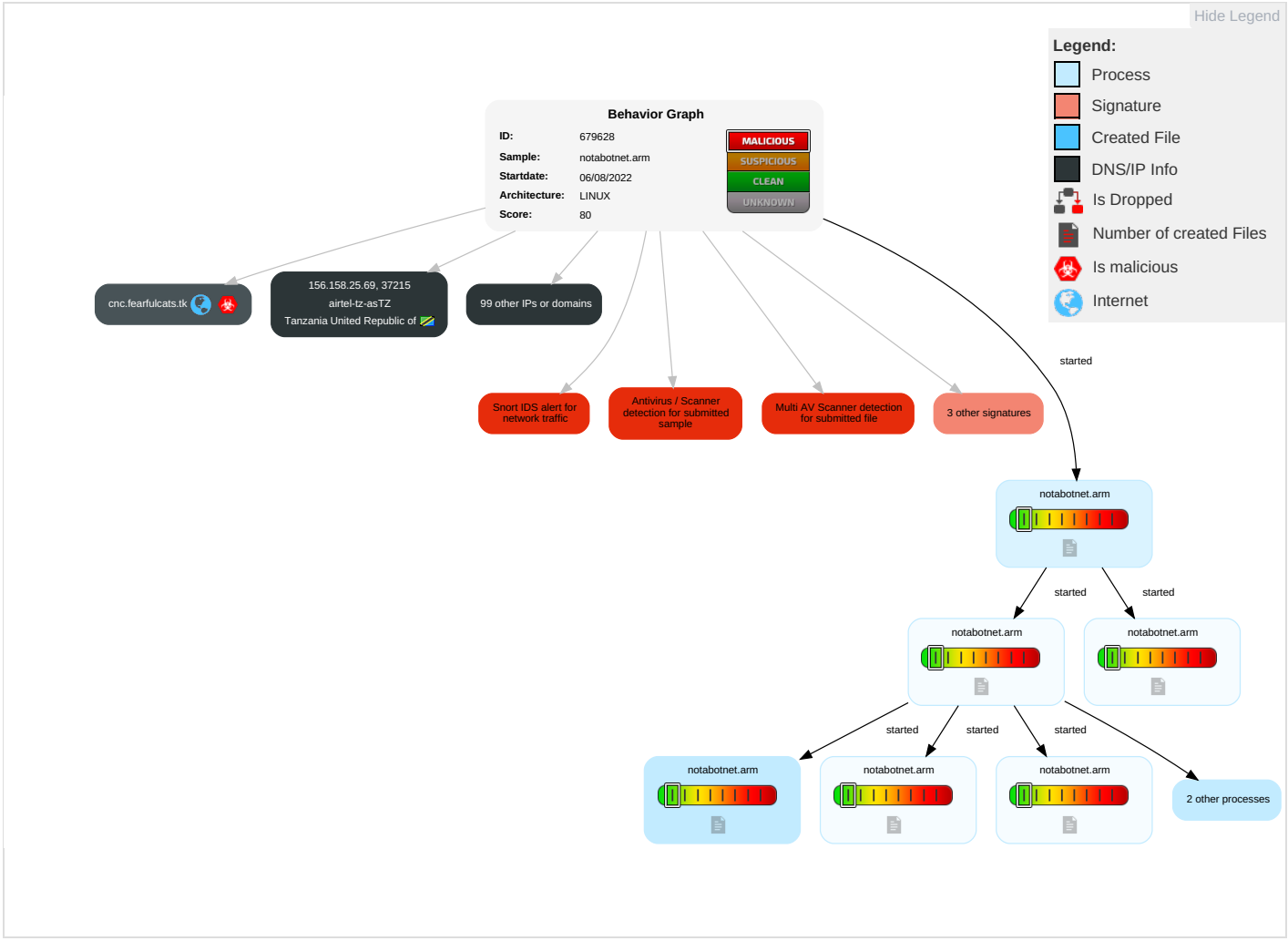
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	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	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	3 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
notabotnet.arm	55%	Virustotal		Browse
notabotnet.arm	40%	Metadefender		Browse
notabotnet.arm	65%	ReversingLabs	Linux.Trojan.Mirai	
notabotnet.arm	100%	Avira	LINUX/Mirai.owpty	

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cnc.fearfulcats.tk	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://cnc.fearfulcats.tk/notabotnet/notabotnet.arm7	9%	Virustotal		Browse
http://cnc.fearfulcats.tk/notabotnet/notabotnet.arm7	100%	Avira URL Cloud	malware	

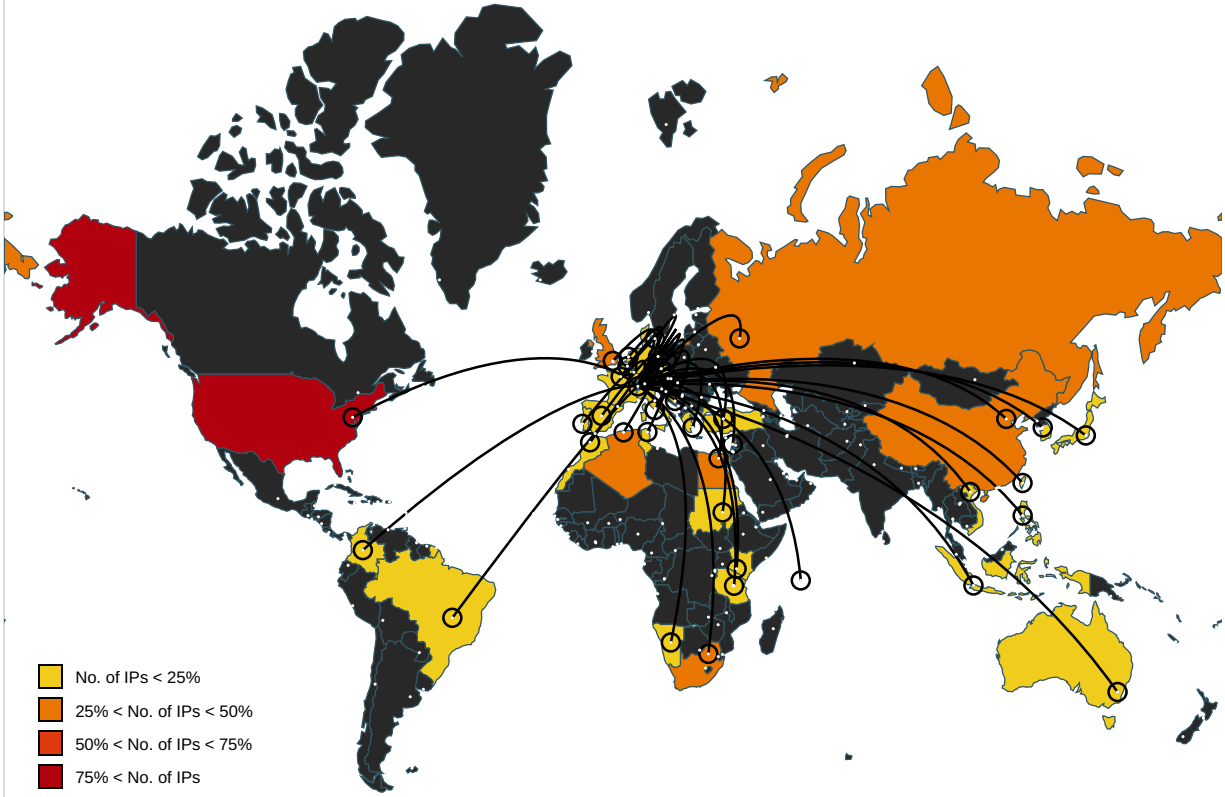
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cnc.fearfulcats.tk	185.225.73.158	true	true	• 10%, Virustotal, Browse	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.238.77.152	unknown	unknown		37705	TOPNETTN	false
78.234.76.85	unknown	France		12322	PROXADFR	false
121.252.20.84	unknown	Korea Republic of		24361	CNGI-NJ-IX-AS-APCERNET2IXatSoutheastUniversityCN	false
41.102.161.60	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.80.44.44	unknown	United States		393649	BOOZ-AS2US	false
197.140.232.156	unknown	Algeria		36891	ICOSNET-ASDZ	false
197.141.53.68	unknown	Algeria		36891	ICOSNET-ASDZ	false
109.197.226.231	unknown	Russian Federation		48642	KTEL-ASEkaterinburgRussiaRU	false
185.160.193.223	unknown	Lebanon		34458	SMARTNETSLB	false
212.83.26.52	unknown	Russian Federation		9039	IIAT-ASIIATAutonomousSystemRU	false
74.243.22.51	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
45.6.244.2	unknown	unknown		266249	CENTRALNETBR	false
185.50.154.144	unknown	United Kingdom		50203	UK-REYNOLDS-ASNGB	false
216.224.227.63	unknown	United States		39948	INIT-PHXUS	false
41.140.123.155	unknown	Morocco		36903	MT-MPLSMA	false
223.215.188.144	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
156.220.29.250	unknown	Egypt		8452	TE-ASTE-ASEG	false
156.50.27.196	unknown	Australia		29975	VODACOM-ZA	false
46.190.7.214	unknown	Greece		25472	WIND-ASGR	false
2.21.229.63	unknown	European Union		20940	AKAMAI-ASN1EU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.116.60.116	unknown	Italy		3269	ASN-IBSNAZIT	false
197.177.87.173	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
212.189.107.90	unknown	Netherlands		286	KPNNL	false
69.174.188.30	unknown	United States		54373	MESSAGEEXPRESSINTERNETUS	false
197.126.118.187	unknown	Egypt		36992	ETISALAT-MISREG	false
41.182.10.66	unknown	Namibia		36996	TELECOM-NAMIBIANA	false
24.172.203.219	unknown	United States		10796	TWC-10796-MIDWESTUS	false
197.143.201.76	unknown	Algeria		36891	ICOSNET-ASDZ	false
46.247.22.221	unknown	United Kingdom		39545	FLUIDATAGB	false
46.19.158.244	unknown	Germany		49603	NERDHERRSCHAFT-ASDE	false
2.83.183.179	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
197.109.134.76	unknown	South Africa		37168	CELL-CZA	false
112.229.16.38	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
81.140.127.234	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
158.81.167.165	unknown	United States		55102	NRG-NS-2US	false
156.246.150.175	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
104.188.187.209	unknown	United States		7018	ATT-INTERNET4US	false
197.117.202.165	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.240.121.94	unknown	Sudan		36998	SDN-MOBITELSD	false
20.230.47.159	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
185.65.120.87	unknown	Bosnia and Herzegowina		201719	TK-ASBA	false
218.48.113.15	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
182.11.165.222	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
212.95.22.32	unknown	Austria		8412	TMARennweg97-99AT	false
121.226.140.144	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
41.196.116.138	unknown	Egypt		24863	LINKdotNET-ASEG	false
88.98.151.123	unknown	United Kingdom		13037	ZEN-ASZenInternet-UKGB	false
181.242.140.206	unknown	Colombia		26611	COMCELSACO	false
43.29.198.215	unknown	Japan		4249	LILLY-ASUS	false
197.26.67.211	unknown	Tunisia		37671	GLOBALNET-ASTN	false
112.19.56.163	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
57.231.100.162	unknown	Belgium		2686	ATGS-MMD-ASUS	false
156.73.167.248	unknown	United States		2024	NUUS	false
112.126.151.130	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
204.119.210.106	unknown	United States		11404	AS-WAVE-1US	false
216.119.121.129	unknown	United States		14992	CRYSTALTECHUS	false
156.158.25.69	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
46.236.180.255	unknown	Russian Federation		34145	TOMTELRU	false
61.100.236.111	unknown	Korea Republic of		17609	SILLAUNIVERSITY-AS-KRSillaUnivKR	false
2.113.108.55	unknown	Italy		3269	ASN-IBSNAZIT	false
81.110.133.149	unknown	United Kingdom		5089	NTLGB	false
46.24.232.120	unknown	Spain		12430	VODAFONE_ESES	false
156.21.96.226	unknown	United States		29975	VODACOM-ZA	false
156.215.141.99	unknown	Egypt		8452	TE-ASTE-ASEG	false
101.234.204.165	unknown	Australia		45577	INTERVOLVE-MELBOURNE-AS-APIntervolvePtyLtdAU	false
101.14.115.244	unknown	Taiwan; Republic of China (ROC)		24158	TAIWANMOBILE-ASTaiwanMobileCoLtdTW	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.42.209.87	unknown	United States		4211	ASN-MARICOPA1US	false
81.6.84.78	unknown	Turkey		15897	VODAFONETURKEYTR	false
156.239.196.240	unknown	Seychelles		133201	COMING-ASABCDEGROUPCOMPANYLIMITEDHK	false
41.169.198.130	unknown	South Africa		36937	Neotel-ASZA	false
41.21.252.51	unknown	South Africa		36994	Vodacom-VBZA	false
41.143.104.52	unknown	Morocco		36903	MT-MPLSMA	false
156.43.93.64	unknown	United Kingdom		3549	LVLT-3549US	false
41.182.10.18	unknown	Namibia		36996	TELECOM-NAMIBIANA	false
41.134.159.161	unknown	South Africa		10474	OPTINETZA	false
41.97.63.188	unknown	Algeria		36947	ALGTEL-ASDZ	false
2.107.146.150	unknown	Denmark		3292	TDCTDCASDK	false
46.46.21.139	unknown	Russian Federation		15638	UTLUssuriyskRU	false
61.201.44.46	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
61.195.128.45	unknown	Japan		10002	ICTIGAUENOCABLETELEVISIONCOLTDJP	false
197.193.232.100	unknown	Egypt		36992	ETISALAT-MISREG	false
2.225.217.215	unknown	Italy		12874	FASTWEBIT	false
197.12.31.243	unknown	Tunisia		37703	ATLAXTN	false
118.203.72.187	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
61.122.128.129	unknown	Japan		17504	NETCOMNRINetcomLtdJP	false
156.71.93.236	unknown	United States		297	AS297US	false
212.80.66.204	unknown	Czech Republic		29208	DIALTELECOM-ASDialTelecomasSK	false
61.9.73.100	unknown	Philippines		23944	SKYBB-AS-APSKYBroadbandSKYCableCorporationPH	false
61.88.137.72	unknown	Australia		7474	OPTUSCOM-AS01-AUSingTelOptusPtyLtdAU	false
66.42.199.17	unknown	United States		6181	FUSE-NETUS	false
152.234.60.251	unknown	Brazil		7738	TelemarNorteLesteSABR	false
207.244.186.203	unknown	United States		11776	ATLANTICBB-JOHNSTOWNUS	false
197.169.124.227	unknown	South Africa		37168	CELL-CZA	false
197.100.219.11	unknown	South Africa		3741	ISZA	false
46.245.236.154	unknown	France		8426	CLARANET-ASClaraNETLTDGB	false
5.3.209.124	unknown	Russian Federation		42682	ERTH-NNOV-ASRU	false
46.105.63.204	unknown	France		16276	OVHFR	false
197.137.214.198	unknown	Kenya		36914	KENET-ASKE	false
41.3.151.135	unknown	South Africa		29975	VODACOM-ZA	false
1.54.72.181	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.13515344056359
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	notabotnet.arm
File size:	80156
MD5:	d8edb88e8280e241f06c014b85d0362f
SHA1:	d9262e6ab9d9a92342fff5fe38758f59b37a1561
SHA256:	4d365f4c4e3f94622f7e7fd786ba773de51f4bd41ecf9ff2295f3628ab5c440c
SHA512:	512545099f0789aca1d0775f918dc2b8627c4fef4814cbb279de45d6defdc76a5f7fabd1643417423130d9534a186b1458abe2abb697ce337ef22a0f433e4155
SSDEEP:	1536:6Muq7Gf9ER0B0dFdA4ThnpOwLjoUoB8t46vqH3CJV9IP:huqGff4x8wfXo84gqXCJV
TLSH:	F0731986BC80E626CBC01677FA2F508D37156BD8E1DA33029D155FA07BCE81F1D6BA85
File Content Preview:	.ELF...a.....(.....4....7.....4. ...(.....5...5..... 5.. 5.. 5..,.....Q.td.....-...L."....F.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	79756
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x11b10	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x19bc0	0x11bc0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x19bd4	0x11bd4	0x1948	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x23520	0x13520	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x23528	0x13528	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x23534	0x13534	0x218	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x2374c	0x1374c	0x4f0	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1374c	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x1351c	0x1351c	6.1558	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x13520	0x23520	0x23520	0x22c	0x71c	2.9664	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.235.104.473633437215283522208/06/22-07:19:52.220960	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36334	37215	192.168.2.23	156.235.104.47
192.168.2.23156.235.104.855780037215283522208/06/22-07:19:39.853691	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57800	37215	192.168.2.23	156.235.104.85
192.168.2.23156.241.65.128416783721528352208/06/22-07:21:20.512607	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41678	37215	192.168.2.23	156.241.65.128
192.168.2.23156.241.116.444223037215283522208/06/22-07:20:00.956884	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42230	37215	192.168.2.23	156.241.116.44
192.168.2.23156.250.69.146551523721528352208/06/22-07:19:39.989567	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55152	37215	192.168.2.23	156.250.69.146
192.168.2.23156.245.33.139545043721528352208/06/22-07:19:52.314965	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54504	37215	192.168.2.23	156.245.33.139
192.168.2.23156.250.28.171527383721528352208/06/22-07:20:29.967484	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52738	37215	192.168.2.23	156.250.28.171
192.168.2.23156.224.31.170376643721528352208/06/22-07:20:49.079922	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37664	37215	192.168.2.23	156.224.31.170
192.168.2.23156.250.102.105365043721528352208/06/22-07:20:29.956914	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36504	37215	192.168.2.23	156.250.102.105
192.168.2.23156.230.19.353428237215283522208/06/22-07:20:27.532804	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34282	37215	192.168.2.23	156.230.19.35

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.250.70.1 28413243721528352222 08/06/22-07:21:02.363370	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41324	37215	192.168.2.23	156.250.70.128
192.168.2.23156.245.55.1 057952372152835222 08/06/22-07:19:21.831672	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57952	37215	192.168.2.23	156.245.55.10
192.168.2.23156.254.109.8743916372152835222 08/06/22-07:20:06.945366	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43916	37215	192.168.2.23	156.254.109.87
192.168.2.23156.250.115.24033420372152835222 08/06/22-07:21:20.543254	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33420	37215	192.168.2.23	156.250.115.240
192.168.2.23156.250.100.8457436372152835222 08/06/22-07:20:06.851930	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57436	37215	192.168.2.23	156.250.100.84
192.168.2.23156.241.99.1 735304372152835222 08/06/22-07:19:43.361911	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35304	37215	192.168.2.23	156.241.99.17
192.168.2.23156.225.145.14155596372152835222 08/06/22-07:19:46.935588	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55966	37215	192.168.2.23	156.225.145.141
192.168.2.238.8.8.853706532012811 08/06/22-07:19:18.475451	UDP	2012811	ET DNS Query to a .tk domain - Likely Hostile	53706	53	192.168.2.23	8.8.8.8
192.168.2.23156.224.19.2 2252936372152835222 08/06/22-07:20:06.720074	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52936	37215	192.168.2.23	156.224.19.222
192.168.2.23156.224.9.20 653706372152835222 08/06/22-07:19:24.221104	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53706	37215	192.168.2.23	156.224.9.206
192.168.2.23156.245.56.1 2560782372152835222 08/06/22-07:21:11.092379	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60782	37215	192.168.2.23	156.245.56.125
192.168.2.23156.226.75.2 2833396372152835222 08/06/22-07:19:39.967769	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33396	37215	192.168.2.23	156.226.75.228
192.168.2.23156.250.94.1 044605437215283522 2 08/06/22-07:20:46.861808	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46054	37215	192.168.2.23	156.250.94.104
192.168.2.23156.244.93.4 250026372152835222 08/06/22-07:19:43.368461	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50026	37215	192.168.2.23	156.244.93.42
192.168.2.23156.238.15.2 0444758372152835222 08/06/22-07:20:23.994081	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44758	37215	192.168.2.23	156.238.15.204
192.168.2.23156.245.36.1 8148390372152835222 08/06/22-07:21:07.429076	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48390	37215	192.168.2.23	156.245.36.181
192.168.2.23156.245.60.1 4053584372152835222 08/06/22-07:20:24.016463	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53584	37215	192.168.2.23	156.245.60.140
192.168.2.23156.226.30.1 6142840372152835222 08/06/22-07:21:13.813244	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42840	37215	192.168.2.23	156.226.30.161
192.168.2.23156.235.104.13638016372152835222 08/06/22-07:21:07.325992	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38016	37215	192.168.2.23	156.235.104.136

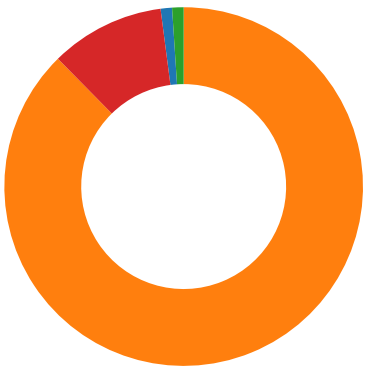
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.241.125.13656354372152835222 08/06/22-07:21:02.342117	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56354	37215	192.168.2.23	156.241.125.136
192.168.2.23156.250.15.2244424372152835222 08/06/22-07:20:46.875148	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44224	37215	192.168.2.23	156.250.15.224
192.168.2.23156.230.25.405257372152835222 08/06/22-07:20:01.144639	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52572	37215	192.168.2.23	156.230.25.40
192.168.2.23156.241.103.12046710372152835222 08/06/22-07:20:29.963710	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46710	37215	192.168.2.23	156.241.103.120
192.168.2.23156.244.125.138204372152835222 08/06/22-07:20:00.952733	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38204	37215	192.168.2.23	156.244.125.1
192.168.2.23156.241.91.2404093837215283522 08/06/22-07:19:24.295713	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40938	37215	192.168.2.23	156.241.91.240
192.168.2.23156.254.111.15043388372152835222 08/06/22-07:20:01.152294	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43388	37215	192.168.2.23	156.254.111.150
192.168.2.23156.254.90.1363287437215283522 08/06/22-07:19:24.221072	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	32874	37215	192.168.2.23	156.254.90.136
192.168.2.23156.241.74.594565037215283522 08/06/22-07:21:17.178265	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45650	37215	192.168.2.23	156.241.74.59
192.168.2.23156.247.17.685295037215283522 08/06/22-07:19:25.518855	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52950	37215	192.168.2.23	156.247.17.68
192.168.2.23156.241.81.2057262372152835222 08/06/22-07:20:46.869967	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57262	37215	192.168.2.23	156.241.81.20
192.168.2.23156.225.156.15546128372152835222 08/06/22-07:21:13.807326	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46128	37215	192.168.2.23	156.225.156.155
192.168.2.23156.226.72.2175803437215283522 08/06/22-07:20:49.212460	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58034	37215	192.168.2.23	156.226.72.217
192.168.2.23156.241.84.7160110372152835222 08/06/22-07:19:25.876818	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60110	37215	192.168.2.23	156.241.84.71
192.168.2.23197.234.43.1514933437215283522 08/06/22-07:19:52.351873	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49334	37215	192.168.2.23	197.234.43.151
192.168.2.23156.244.69.1065337437215283522 08/06/22-07:19:29.489873	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53374	37215	192.168.2.23	156.244.69.106
192.168.2.23197.246.248.12934130372152835222 08/06/22-07:20:39.259211	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34130	37215	192.168.2.23	197.246.248.129
192.168.2.23156.235.111.19760086372152835222 08/06/22-07:21:07.326010	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60086	37215	192.168.2.23	156.235.111.197
192.168.2.23156.226.33.1284283437215283522 08/06/22-07:20:07.122992	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42834	37215	192.168.2.23	156.226.33.128

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.250.84.2163431437215283522208/06/22-07:21:13.530696	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34314	37215	192.168.2.23	156.250.84.216
192.168.2.23156.226.111.2403805237215283522208/06/22-07:21:07.604064	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38052	37215	192.168.2.23	156.226.111.240
192.168.2.23156.254.91.435660037215283522208/06/22-07:19:52.243025	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56600	37215	192.168.2.23	156.254.91.43
192.168.2.23156.226.72.1684946637215283522208/06/22-07:20:00.976466	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49466	37215	192.168.2.23	156.226.72.168
192.168.2.23156.224.22.933725837215283522208/06/22-07:19:46.797331	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37258	37215	192.168.2.23	156.224.22.93
192.168.2.23156.250.4.2133800372152835222208/06/22-07:19:29.496580	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33800	37215	192.168.2.23	156.250.4.21
192.168.2.23156.245.36.505996237215283522208/06/22-07:20:07.124180	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59962	37215	192.168.2.23	156.245.36.50
192.168.2.23156.252.26.1423283437215283522208/06/22-07:19:29.389161	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	32834	37215	192.168.2.23	156.252.26.142
192.168.2.23156.245.34.1134795837215283522208/06/22-07:20:53.752304	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47958	37215	192.168.2.23	156.245.34.113
192.168.2.23156.235.105.171581203721528352222208/06/22-07:20:00.838160	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58120	37215	192.168.2.23	156.235.105.171
192.168.2.23156.235.106.232380523721528352222208/06/22-07:19:46.804785	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38052	37215	192.168.2.23	156.235.106.232
192.168.2.23156.235.101.985163637215283522208/06/22-07:21:11.184192	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51636	37215	192.168.2.23	156.235.101.98
192.168.2.23156.254.34.1153903437215283522208/06/22-07:20:06.738093	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39034	37215	192.168.2.23	156.254.34.115
192.168.2.23156.244.67.1713992837215283522208/06/22-07:20:54.031258	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39928	37215	192.168.2.23	156.244.67.171
192.168.2.23156.245.33.7240872372152835222208/06/22-07:19:43.361861	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40872	37215	192.168.2.23	156.245.33.72
192.168.2.23156.224.15.453854372152835222208/06/22-07:19:43.569760	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53854	37215	192.168.2.23	156.224.15.4
192.168.2.23156.244.101.19635582372152835222208/06/22-07:19:52.333819	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35582	37215	192.168.2.23	156.244.101.196
192.168.2.23197.238.136.19433464372152835222208/06/22-07:20:51.343241	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33464	37215	192.168.2.23	197.238.136.194
192.168.2.23156.225.153.22651524372152835222208/06/22-07:19:30.088494	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51524	37215	192.168.2.23	156.225.153.226

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.227.241.654330637215283522208/06/22-07:19:24.221136	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43306	37215	192.168.2.23	156.227.241.65
192.168.2.23156.240.104.170514823721528352208/06/22-07:21:11.008228	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51482	37215	192.168.2.23	156.240.104.170
192.168.2.23156.241.8.155384563721528352208/06/22-07:21:02.280154	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38456	37215	192.168.2.23	156.241.8.155
192.168.2.23156.244.84.167350503721528352208/06/22-07:19:25.593415	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35050	37215	192.168.2.23	156.244.84.167
192.168.2.23156.238.60.214726437215283522208/06/22-07:20:06.840968	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47264	37215	192.168.2.23	156.238.60.21
192.168.2.23156.241.90.494125837215283522208/06/22-07:20:04.503966	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41258	37215	192.168.2.23	156.241.90.49
192.168.2.23156.250.127.753632437215283522208/06/22-07:19:26.178572	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36324	37215	192.168.2.23	156.250.127.75
192.168.2.23156.226.33.594295237215283522208/06/22-07:19:27.174349	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42952	37215	192.168.2.23	156.226.33.59
192.168.2.23156.244.74.195410063721528352208/06/22-07:20:04.504021	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41006	37215	192.168.2.23	156.244.74.195
192.168.2.23156.250.124.11495263721528352208/06/22-07:20:27.641269	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49526	37215	192.168.2.23	156.250.124.11
192.168.2.23156.244.72.514854437215283522208/06/22-07:19:30.062165	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48544	37215	192.168.2.23	156.244.72.51
192.168.2.23156.244.90.793477637215283522208/06/22-07:21:02.337983	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34776	37215	192.168.2.23	156.244.90.79
192.168.2.23156.226.35.147420743721528352208/06/22-07:21:04.689014	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42074	37215	192.168.2.23	156.226.35.147
192.168.2.23156.225.148.363688237215283522208/06/22-07:20:49.212415	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36882	37215	192.168.2.23	156.225.148.36
192.168.2.23156.241.67.223373637215283522208/06/22-07:19:32.414471	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37336	37215	192.168.2.23	156.241.67.223
192.168.2.23156.244.103.613296437215283522208/06/22-07:21:13.529327	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	32964	37215	192.168.2.23	156.244.103.61
192.168.2.23156.250.105.255544743721528352208/06/22-07:19:26.154807	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54474	37215	192.168.2.23	156.250.105.255
192.168.2.23156.224.21.151479103721528352208/06/22-07:19:29.389496	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47910	37215	192.168.2.23	156.224.21.151
192.168.2.23156.250.113.050732372152835222208/06/22-07:20:24.003561	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50732	37215	192.168.2.23	156.250.113.0

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.241.118.232476803721528352222 08/06/22-07:21:04.696969	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47680	37215	192.168.2.23	156.241.118.232
192.168.2.23156.240.110.112587983721528352222 08/06/22-07:19:32.332687	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58798	37215	192.168.2.23	156.240.110.112
192.168.2.23156.226.105.685409037215283522 08/06/22-07:20:58.709810	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54090	37215	192.168.2.23	156.226.105.68
192.168.2.23156.241.114.825396437215283522 08/06/22-07:20:46.873374	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53964	37215	192.168.2.23	156.241.114.82
192.168.2.23156.226.69.251570963721528352222 08/06/22-07:21:13.836375	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57096	37215	192.168.2.23	156.226.69.251
192.168.2.23156.250.19.190346843721528352222 08/06/22-07:21:20.519259	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34684	37215	192.168.2.23	156.250.19.190
192.168.2.23156.250.66.246487363721528352222 08/06/22-07:19:25.592979	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48736	37215	192.168.2.23	156.250.66.246
192.168.2.23156.254.68.663953437215283522 08/06/22-07:21:13.731473	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39534	37215	192.168.2.23	156.254.68.66
192.168.2.23156.226.76.127580243721528352222 08/06/22-07:21:07.140930	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58024	37215	192.168.2.23	156.226.76.127
192.168.2.23156.241.83.248461663721528352222 08/06/22-07:19:29.498077	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46166	37215	192.168.2.23	156.241.83.248
192.168.2.23156.241.107.104359743721528352222 08/06/22-07:21:00.015237	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35974	37215	192.168.2.23	156.241.107.104
192.168.2.23156.241.89.444263437215283522 08/06/22-07:19:39.964819	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42634	37215	192.168.2.23	156.241.89.44
192.168.2.23156.227.247.993549037215283522 08/06/22-07:19:32.332760	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35490	37215	192.168.2.23	156.227.247.99

Network Port Distribution



Total Packets: 97

- 2323 undefined
- 80 (HTTP)
- 23 (Telnet)
- 443 (HTTPS)

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 07:19:18.475450993 CEST	192.168.2.23	8.8.8.8	0x63da	Standard query (0)	cnc.fearfulcats.tk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 07:19:18.604743958 CEST	8.8.8.8	192.168.2.23	0x63da	No error (0)	cnc.fearfulcats.tk		185.225.73.158	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: notabotnet.arm PID: **6236**, Parent PID: **6127**

General

Start time:	07:19:17
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm
Arguments:	/tmp/notabotnet.arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: notabotnet.arm PID: **6238**, Parent PID: **6236**

General

Start time:	07:19:17
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: notabotnet.arm PID: **6239**, Parent PID: **6236**

General

Start time:	07:19:17
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: notabotnet.arm PID: **6241**, Parent PID: **6239**

General

Start time:	07:19:17
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: notabotnet.arm PID: **6243**, Parent PID: **6239**

General

Start time:	07:19:17
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: notabotnet.arm PID: **6246**, Parent PID: **6239**

General

Start time:	07:19:17
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: notabotnet.arm PID: **6248**, Parent PID: **6239**

General

Start time:	07:19:17
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: notabotnet.arm PID: **6251**, Parent PID: **6239**

General

Start time:	07:19:17
Start date:	06/08/2022
Path:	/tmp/notabotnet.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1