JoeSandbox Cloud BASIC

ID: 679629
Sample Name: notabotnet.mips
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:22:28
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Linux Analysis Report notabotnet.mips 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 6
Joe Sandbox Signatures 13
AV Detection 13
Networking 13
Hooking and other Techniques for Hiding and Protection 13
Stealing of Sensitive Information 13
Remote Access Functionality 13
Mitre Att&ck Matrix 13
Malware Configuration 14
Behavior Graph 14
Antivirus, Machine Learning and Genetic Malware Detection 15
Initial Sample 15
Dropped Files 15
Domains 15
URLs 15
Domains and IPs 15
Contacted Domains 16
URLs from Memory and Binaries 16
World Map of Contacted IPs 16
Public IPs 16
Joe Sandbox View / Context 18
IPs 18
Domains 18
ASNs 19
JA3 Fingerprints 19
Dropped Files 19
Created / dropped Files 19
Static File Info 19
General 19
Static ELF Info 19
ELF header 19
Sections 20
Program Segments 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 23
TCP Packets 23
DNS Queries 23
DNS Answers 23
System Behavior 23
Analysis Process: notabotnet.mips PID: 6226, Parent PID: 6121 23
General 23
File Activities 24
File Read 24
Analysis Process: notabotnet.mips PID: 6228, Parent PID: 6226 24
General 24
Analysis Process: notabotnet.mips PID: 6229, Parent PID: 6226 24
General 24
Analysis Process: notabotnet.mips PID: 6232, Parent PID: 6229 24
General 24
Analysis Process: notabotnet.mips PID: 6233, Parent PID: 6229 24
General 24
File Activities 24
File Read 24
Directory Enumerated 24
Analysis Process: notabotnet.mips PID: 6235, Parent PID: 6229 24
General 24
Analysis Process: notabotnet.mips PID: 6239, Parent PID: 6229 25
General 25
Analysis Process: notabotnet.mips PID: 6241, Parent PID: 6229 25

Copyright Joe Security LLC 2022

Linux Analysis Report

notabotnet.mips

Overview

General Information

Sample Name:	notabotnet.mips
Analysis ID:	679629
MD5:	a2af0d91b6e84e..
SHA1:	10c1dee864fb8fd..
SHA256:	7601ce34f58f7f8..
Tags:	Mirai
Infos:	

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

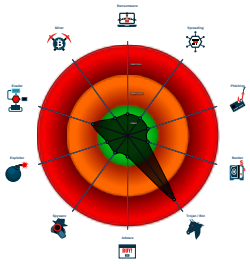
Mirai

Score:	88
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…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…

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.

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:	35.0.0 Citrine
Analysis ID:	679629
Start date and time: 06/08/202207:22:28	2022-08-06 07:22:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	notabotnet.mips
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:	mal88.troj.linMIPS@0/0@1/0

Warnings

Runtime Messages

Command:	/tmp/notabotnet.mips
PID:	6226
Exit Code:	0
Exit Code Info:	
Killed:	False

Copyright Joe Security LLC 2022

Standard Output:	xXxSlicexXxxVEGA.
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- notabotnet.mips (PID: 6226, Parent: 6121, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/notabotnet.mips
  - notabotnet.mips New Fork (PID: 6228, Parent: 6226)
  - notabotnet.mips New Fork (PID: 6229, Parent: 6226)
    - notabotnet.mips New Fork (PID: 6232, Parent: 6229)
    - notabotnet.mips New Fork (PID: 6233, Parent: 6229)
    - notabotnet.mips New Fork (PID: 6235, Parent: 6229)
    - notabotnet.mips New Fork (PID: 6239, Parent: 6229)
    - notabotnet.mips New Fork (PID: 6241, Parent: 6229)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
notabotnet.mips	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	• 0x17e8c:$xo1: Dfs`eeh&<'9 • 0x17f04:$xo1: Dfs`eeh&<'9 • 0x17f78:$xo1: Dfs`eeh&<'9 • 0x17fe8:$xo1: Dfs`eeh&<'9 • 0x18034:$xo1: Dfs`eeh&<'9
notabotnet.mips	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	

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
6232.1.00007feda045a000.00007feda045b000.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

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
6228.1.00007feda045a000.00007feda045b000.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:$xo1: Dfs`eeh&<'9
6226.1.00007feda0400000.00007feda0419000.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x17e8c:$xo1: Dfs`eeh&<'9 • 0x17f04:$xo1: Dfs`eeh&<'9 • 0x17f78:$xo1: Dfs`eeh&<'9 • 0x17fe8:$xo1: Dfs`eeh&<'9 • 0x18034:$xo1: Dfs`eeh&<'9
6226.1.00007feda0400000.00007feda0419000.r-x.sdmp	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
6228.1.00007feda0400000.00007feda0419000.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	• 0x17e8c:$xo1: Dfs`eeh&<'9 • 0x17f04:$xo1: Dfs`eeh&<'9 • 0x17f78:$xo1: Dfs`eeh&<'9 • 0x17fe8:$xo1: Dfs`eeh&<'9 • 0x18034:$xo1: Dfs`eeh&<'9
Click to see the 10 entries				

Snort Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 156.226.90.218

Timestamp:	192.168.2.23156.226.90.21852826372152835222 08/06/22-07:23:16.432753
SID:	2835222
Source Port:	52826
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: 156.250.119.160

Timestamp:	192.168.2.23156.250.119.16041654372152835222 08/06/22-07:23:27.011828
SID:	2835222
Source Port:	41654
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: 197.214.103.132

Timestamp:	192.168.2.23197.214.103.13250728372152835222 08/06/22-07:23:53.676873
SID:	2835222
Source Port:	50728
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:	192.168.2.238.8.8.849581532012811 08/06/22-07:23:14.095323
SID:	2012811
Source Port:	49581
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: 156.250.92.165

Timestamp:	192.168.2.23156.250.92.16538646372152835222 08/06/22-07:23:40.260566
SID:	2835222
Source Port:	38646
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: 156.244.80.94

Timestamp:	192.168.2.23156.244.80.9459200372152835222 08/06/22-07:23:39.639416
SID:	2835222
Source Port:	59200
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: 156.226.11.15

Timestamp:	192.168.2.23156.226.11.1552072372152835222 08/06/22-07:23:43.667446
SID:	2835222
Source Port:	52072
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: 156.245.51.25

Timestamp:	192.168.2.23156.245.51.2550694372152835222 08/06/22-07:23:39.952103
SID:	2835222
Source Port:	50694
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: 156.254.79.89

Timestamp:	192.168.2.23156.254.79.8953116372152835222 08/06/22-07:24:04.605598
SID:	2835222
Source Port:	53116
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: 156.235.102.132

Timestamp:	192.168.2.23156.235.102.13237424372152835222 08/06/22-07:23:43.645321
SID:	2835222
Source Port:	37424
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: 156.250.122.40

Timestamp:	192.168.2.23156.250.122.4049938372152835222 08/06/22-07:23:27.033187

SID:	2835222
Source Port:	49938
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: 156.226.27.134

Timestamp:	192.168.2.23156.226.27.13433390372152835222 08/06/22-07:24:04.960889
SID:	2835222
Source Port:	33390
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: 156.244.72.40

Timestamp:	192.168.2.23156.244.72.4047196372152835222 08/06/22-07:23:53.439628
SID:	2835222
Source Port:	47196
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: 156.244.109.94

Timestamp:	192.168.2.23156.244.109.9445444372152835222 08/06/22-07:23:29.654745
SID:	2835222
Source Port:	45444
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: 156.226.90.241

Timestamp:	192.168.2.23156.226.90.24160120372152835222 08/06/22-07:23:53.442635
SID:	2835222
Source Port:	60120
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: 156.250.103.88

Timestamp:	192.168.2.23156.250.103.8844052372152835222 08/06/22-07:24:04.660457
SID:	2835222
Source Port:	44052
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: 156.224.11.12

Timestamp:	192.168.2.23156.224.11.1233306372152835222 08/06/22-07:24:04.797279
SID:	2835222
Source Port:	33306
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: 156.241.133.165

Timestamp:	192.168.2.23156.241.133.16536340372152835222 08/06/22-07:23:39.554681
SID:	2835222
Source Port:	36340
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: 156.250.113.198

Timestamp:	192.168.2.23156.250.113.19853300372152835222 08/06/22-07:23:27.034689
SID:	2835222
Source Port:	53300
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: 156.254.48.52

Timestamp:	192.168.2.23156.254.48.52417423372152835222 08/06/22-07:23:29.567245
SID:	2835222
Source Port:	41742
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: 156.250.74.27

Timestamp:	192.168.2.23156.250.74.27507523372152835222 08/06/22-07:23:16.433919
SID:	2835222
Source Port:	50752
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: 156.226.82.58

Timestamp:	192.168.2.23156.226.82.58512883372152835222 08/06/22-07:23:53.744332
SID:	2835222
Source Port:	51288
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: 156.224.29.157

Timestamp:	192.168.2.23156.224.29.15750298372152835222 08/06/22-07:24:10.214896
SID:	2835222
Source Port:	50298
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: 156.226.84.107

Timestamp:	192.168.2.23156.226.84.10759142372152835222 08/06/22-07:23:53.439665
SID:	2835222
Source Port:	59142
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: 156.241.91.214

Timestamp:	192.168.2.23156.241.91.21454440372152835222 08/06/22-07:23:33.249369
SID:	2835222
Source Port:	54440
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: 156.244.110.224

Timestamp:	192.168.2.23156.244.110.22454676372152835222 08/06/22-07:23:59.102835

SID:	2835222
Source Port:	54676
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: 156.241.125.36

Timestamp:	192.168.2.23156.241.125.36554163721528352 22 08/06/22-07:23:53.476267
SID:	2835222
Source Port:	55416
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: 156.245.55.200

Timestamp:	192.168.2.23156.245.55.20053560372152835222 08/06/22-07:24:04.679076
SID:	2835222
Source Port:	53560
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: 156.226.98.226

Timestamp:	192.168.2.23156.226.98.22635010372152835222 08/06/22-07:23:33.273831
SID:	2835222
Source Port:	35010
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: 156.250.79.6

Timestamp:	192.168.2.23156.250.79.649098372152835222 08/06/22-07:23:27.034355
SID:	2835222
Source Port:	49098
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: 156.250.18.224

Timestamp:	192.168.2.23156.250.18.22450598372152835222 08/06/22-07:23:53.729151
SID:	2835222
Source Port:	50598
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: 156.230.20.31

Timestamp:	192.168.2.23156.230.20.31525343721528352 22 08/06/22-07:23:27.220458
SID:	2835222
Source Port:	52534
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: 156.238.63.45

Timestamp:	192.168.2.23156.238.63.45425723721528352 22 08/06/22-07:23:27.305057
SID:	2835222
Source Port:	42572
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: 197.234.61.235

Timestamp:	192.168.2.23197.234.61.23542192372152835222 08/06/22-07:23:31.722171
SID:	2835222
Source Port:	42192
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: 156.241.66.242

Timestamp:	192.168.2.23156.241.66.24244510372152835222 08/06/22-07:23:29.651725
SID:	2835222
Source Port:	44510
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: 156.250.9.158

Timestamp:	192.168.2.23156.250.9.15837962372152835222 08/06/22-07:24:04.676872
SID:	2835222
Source Port:	37962
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: 156.235.97.94

Timestamp:	192.168.2.23156.235.97.9458838372152835222 08/06/22-07:23:39.548075
SID:	2835222
Source Port:	58838
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: 156.235.96.124

Timestamp:	192.168.2.23156.235.96.12434606372152835222 08/06/22-07:23:43.645351
SID:	2835222
Source Port:	34606
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: 156.224.20.130

Timestamp:	192.168.2.23156.224.20.13050850372152835222 08/06/22-07:23:53.608016
SID:	2835222
Source Port:	50850
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: 156.224.13.140

Timestamp:	192.168.2.23156.224.13.14060786372152835222 08/06/22-07:24:02.348307
SID:	2835222
Source Port:	60786
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: 156.245.34.63

Timestamp:	192.168.2.23156.245.34.6360668372152835222 08/06/22-07:23:39.647282

SID:	2835222
Source Port:	60668
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: 156.244.119.22

Timestamp:	192.168.2.23156.244.119.2252904372152835222 08/06/22-07:23:27.039494
SID:	2835222
Source Port:	52904
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: 156.226.103.26

Timestamp:	192.168.2.23156.226.103.2647596372152835222 08/06/22-07:23:27.316869
SID:	2835222
Source Port:	47596
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: 156.241.90.38

Timestamp:	192.168.2.23156.241.90.3842742372152835222 08/06/22-07:23:39.649878
SID:	2835222
Source Port:	42742
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: 156.226.96.33

Timestamp:	192.168.2.23156.226.96.3347718372152835222 08/06/22-07:23:40.227571
SID:	2835222
Source Port:	47718
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: 156.250.65.100

Timestamp:	192.168.2.23156.250.65.10041802372152835222 08/06/22-07:23:52.152505
SID:	2835222
Source Port:	41802
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: 156.250.115.61

Timestamp:	192.168.2.23156.250.115.6136870372152835222 08/06/22-07:23:33.241907
SID:	2835222
Source Port:	36870
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: 156.244.124.47

Timestamp:	192.168.2.23156.244.124.4735554372152835222 08/06/22-07:23:39.639516
SID:	2835222
Source Port:	35554
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: 156.245.59.247

Timestamp:	192.168.2.23156.245.59.24755638372152835222 08/06/22-07:23:40.240392
SID:	2835222
Source Port:	55638
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: 197.246.131.18

Timestamp:	192.168.2.23197.246.131.18551823721528352 22 08/06/22-07:23:50.863914
SID:	2835222
Source Port:	55182
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: 156.250.116.151

Timestamp:	192.168.2.23156.250.116.15154632372152835222 08/06/22-07:23:53.717828
SID:	2835222
Source Port:	54632
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

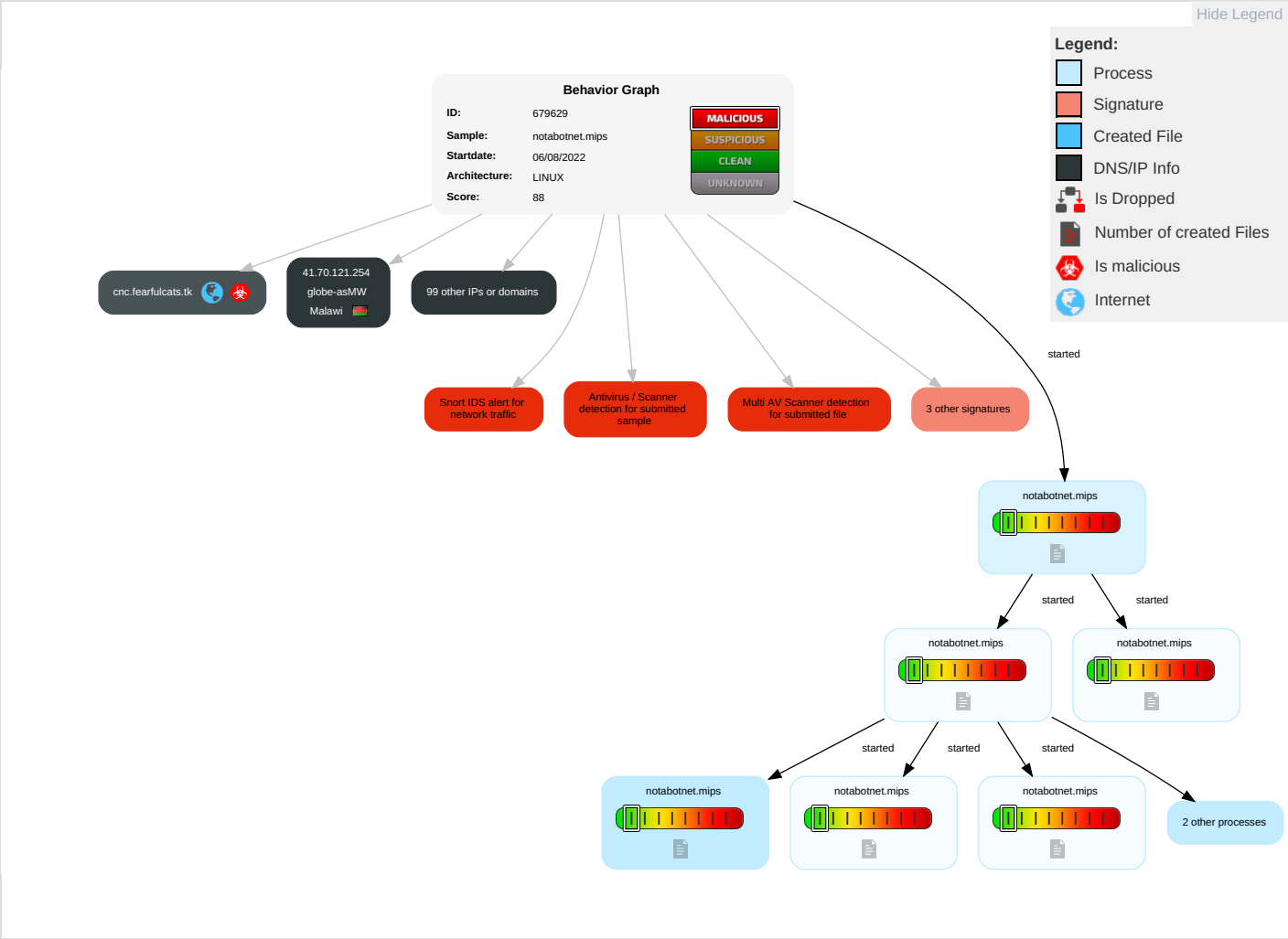
Mitre Att&ck Matrix

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.mips	63%	Virustotal		Browse
notabotnet.mips	43%	Metadefender		Browse
notabotnet.mips	73%	ReversingLabs	Linux.Trojan.Mirai	
notabotnet.mips	100%	Avira	LINUX/Mirai.frpfm	

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	

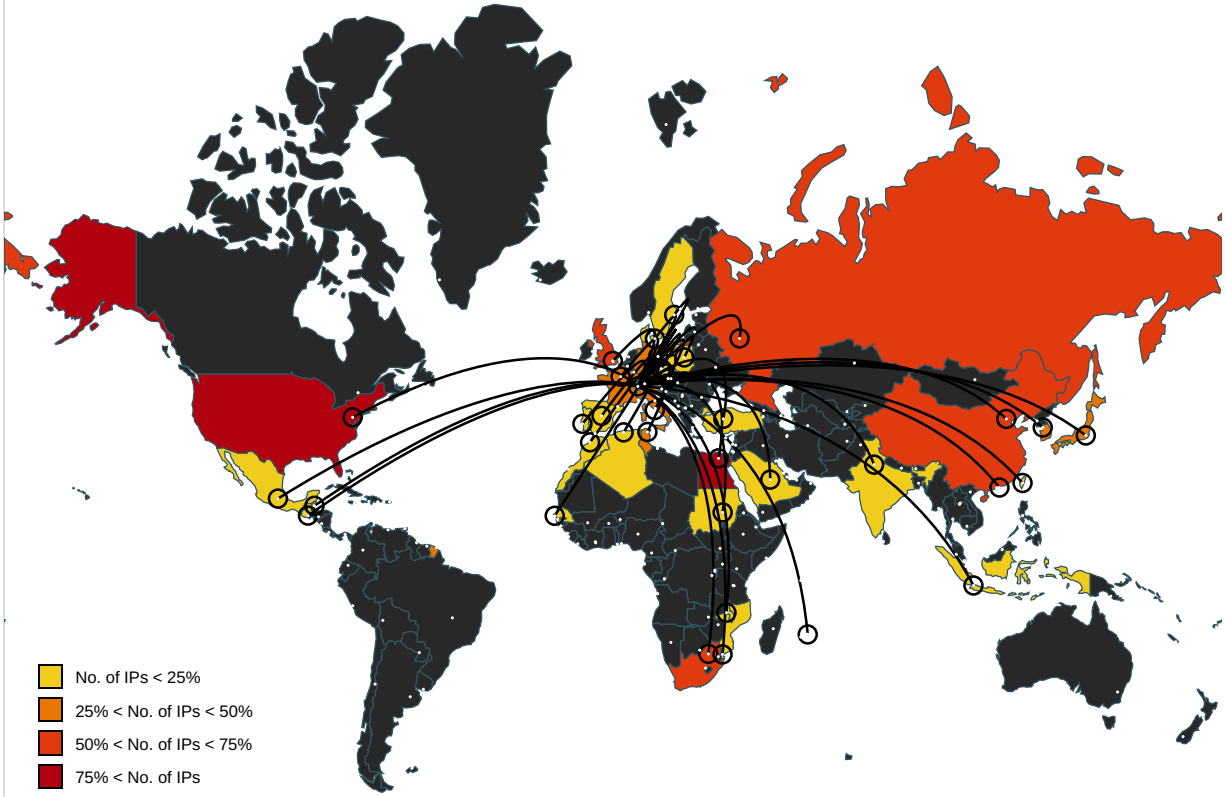
Domains and IPs

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
85.25.248.123	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
212.111.23.63	unknown	Czech Republic		25424	INEXT-CZInterneXt2000sroCZ	false
41.203.39.8	unknown	South Africa		36968	ECN-AS1ZA	false
2.236.57.130	unknown	Italy		12874	FASTWEBIT	false
88.146.106.157	unknown	Czech Republic		29208	DIALTELECOM-ASDialTelecomasSK	false
81.71.37.219	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
41.149.186.115	unknown	South Africa		5713	SAIX-NETZA	false
2.61.16.214	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
220.139.15.174	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
41.36.218.220	unknown	Egypt		8452	TE-ASTE-ASEG	false
212.144.211.137	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
14.98.60.191	unknown	India		45820	TTSL-MEISISPTataTeleservicesISPASIN	false
156.17.87.102	unknown	Poland		8970	WASKWROCMAN-EDUeducationalpartofWASKnetworkWroclaw	false
148.250.229.42	unknown	Mexico		6503	AxtelSABdeCVMX	false
212.94.221.121	unknown	France		12409	HRNETFR	false
91.57.203.208	unknown	Germany		3320	DTAGInternetserviceproviderperationsDE	false
46.48.175.143	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
41.137.15.186	unknown	Morocco		36884	MAROCCONNECTMA	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.82.47.203	unknown	Senegal		8346	SONATEL-ASAutonomousSystemEU	false
85.80.175.85	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
2.222.184.195	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
94.13.68.25	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
188.110.100.164	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
201.153.215.139	unknown	Mexico		8151	UninetSAdeCVMX	false
197.249.194.123	unknown	Mozambique		25139	TVCABO-ASEU	false
185.14.58.161	unknown	Spain		202054	S4N-ASES	false
112.213.114.229	unknown	Hong Kong		38197	SUNHK-DATA-AS-APSunNetworkHongKongLimited-HongKong	false
156.18.227.163	unknown	France		1945	FR-LYRESLyonRechercheetEnseignementSuperieurLyRESE	false
213.109.189.126	unknown	Russian Federation		9009	M247GB	false
41.129.114.59	unknown	Egypt		24863	LINKdotNET-ASEG	false
41.3.103.245	unknown	South Africa		29975	VODACOM-ZA	false
95.166.18.178	unknown	Denmark		3292	TDCTDCASDK	false
60.16.195.158	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
85.4.56.39	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
156.99.71.219	unknown	United States		1998	STATE-OF-MNUS	false
61.104.154.65	unknown	Korea Republic of		38114	TERANET-AS-KRShinjinNetworkKR	false
197.12.117.167	unknown	Tunisia		37703	ATLAXTN	false
197.153.12.72	unknown	Morocco		36925	ASMediMA	false
188.187.46.42	unknown	Russian Federation		51570	SPB-ASRU	false
156.112.197.152	unknown	United States		5961	DNIC-ASBLK-05800-06055US	false
48.238.232.58	unknown	United States		2686	ATGS-MMD-ASUS	false
41.230.97.173	unknown	Tunisia		37705	TOPNETTN	false
85.246.119.80	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
24.160.165.225	unknown	United States		10796	TWC-10796-MIDWESTUS	false
41.97.63.154	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.193.80.149	unknown	Egypt		8452	TE-ASTE-ASEG	false
2.236.57.147	unknown	Italy		12874	FASTWEBIT	false
156.127.187.99	unknown	United States		393504	XNSTGCA	false
43.52.121.37	unknown	Japan		4249	LILLY-ASUS	false
197.240.45.187	unknown	unknown		37705	TOPNETTN	false
197.55.181.96	unknown	Egypt		8452	TE-ASTE-ASEG	false
2.92.140.58	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
156.20.255.207	unknown	United States		23005	SWITCH-LTDUS	false
41.70.121.254	unknown	Malawi		37098	globe-asMW	false
95.108.149.22	unknown	Russian Federation		13238	YANDEXRU	false
190.143.181.212	unknown	Guatemala		13682	TelguaGT	false
95.61.241.252	unknown	Spain		12430	VODAFONE_ESES	false
94.50.19.31	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
63.4.59.172	unknown	United States		701	UUNETUS	false
156.70.138.58	unknown	United States		297	AS297US	false
41.60.37.47	unknown	Mauritius		30969	ZOL-ASGB	false
176.47.187.2	unknown	Saudi Arabia		3249	ESTPAKEE	false
61.205.132.172	unknown	Japan		9617	ZAQJupiterTelecommunicationsCoLtdJP	false
182.210.89.225	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
43.125.153.126	unknown	Japan		4249	LILLY-ASUS	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.31.187.159	unknown	Tunisia		37492	ORANGE-TN	false
197.17.114.151	unknown	Tunisia		37693	TUNISIANATN	false
185.124.0.132	unknown	United Kingdom		204085	NGSGB	false
197.55.34.215	unknown	Egypt		8452	TE-ASTE-ASEG	false
94.46.221.211	unknown	United Kingdom		42831	UKSERVERS-ASUKDedicatedServersHostingandCo-Location	false
121.41.250.148	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
86.104.222.5	unknown	United Kingdom		209574	QUEST-ITGB	false
197.223.200.117	unknown	Egypt		37069	MOBINILEG	false
43.121.222.103	unknown	Japan		4249	LILLY-ASUS	false
182.5.164.185	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
156.215.116.49	unknown	Egypt		8452	TE-ASTE-ASEG	false
121.127.117.54	unknown	Korea Republic of		9756	CHEONANVITSSEN-AS-KRTbroadChungbuBroadcastingCoKR	false
156.3.38.249	unknown	United States		2920	LACOEUS	false
5.242.233.201	unknown	Sweden		1257	TELE2EU	false
61.188.227.224	unknown	China		139220	CHINANET-SICHUAN-CHUANXI-IDCSichuanChuanxnIDCCN	false
197.73.244.17	unknown	South Africa		16637	MTNNS-ASZA	false
122.23.120.95	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
197.195.100.233	unknown	Egypt		36992	ETISALAT-MISREG	false
197.82.246.89	unknown	South Africa		10474	OPTINETZA	false
66.37.163.76	unknown	United States		6534	OCEANIC-CABLEUS	false
41.105.231.153	unknown	Algeria		36947	ALGTEL-ASDZ	false
190.197.57.33	unknown	Belize		10269	BelizeTelemediaLimitedBZ	false
95.10.181.2	unknown	Turkey		9121	TTNETTR	false
61.241.225.212	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
156.191.172.60	unknown	Egypt		36992	ETISALAT-MISREG	false
156.43.93.58	unknown	United Kingdom		3549	LVLT-3549US	false
2.197.106.51	unknown	Italy		16232	ASN-TIMServiceProviderIT	false
212.51.251.100	unknown	Austria		12762	VTG-AT	false
101.69.14.107	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
176.177.102.196	unknown	France		5410	BOUYGTEL-ISPFR	false
197.165.241.195	unknown	Egypt		24863	LINKdotNET-ASEG	false
156.55.39.50	unknown	United States		22146	LANDAMUS	false
41.127.73.159	unknown	South Africa		16637	MTNNS-ASZA	false
212.45.152.172	unknown	Italy		8816	IT-STCOMIT	false
41.95.229.226	unknown	Sudan		36998	SDN-MOBITELSD	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.444246881535002
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	notabotnet.mips
File size:	105656
MD5:	a2af0d91b6e84e614eda94b4e7b8cac4
SHA1:	10c1dee864fb8fdb1770f87065c72b4acef91368
SHA256:	7601ce34f58f7f8a7a046a0682a406e05ebe72f2cb0a3938cb166d1f3dfd2e6e
SHA512:	81bf61a4961e806524f23e3e80f01cb11c48ee86038280ff0cb038c54f94883f7dd992689e92aaa1e79ed6fe74b746a4441cc1f7e8d18126629c269aa4ac1d84
SSDEEP:	1536:klToz925rlxLwnLf5IdMLldP2QfghplO9NyvhieBaqxDmAD5P/4tbXQN+ZLA:mAyrlxLU+dMT2Q4jluNpeBaqxio5sWX
TLSH:	38A3724D7E215F7EFBAC823897B74F249248339A2AF1D5C4C1ACED015E7028A641FB65
File Content Preview:	.ELF.....@.`...4.....4. ...(.....@...@.....0...0.....E...E.....$...h.....dt.Q.....<...'.....!'.....<...'.....!... ....'9... ..... <...'.....!...$....'9m

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	105096
Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x16cc0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x416de0	0x16de0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x416e40	0x16e40	0x15f0	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x459000	0x19000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x459008	0x19008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x459014	0x19014	0x404	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x459420	0x19420	0x258	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x459680	0x19680	0x3a4	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x459a24	0x19a24	0x20	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x459a50	0x19a24	0x518	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x69c	0x19a24	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x19a24	0x64	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x18430	0x18430	5.5447	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x19000	0x459000	0x459000	0xa24	0xf68	4.3591	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.226.90.2185282637215283522208/06/22-07:23:16.432753	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52826	37215	192.168.2.23	156.226.90.218
192.168.2.23156.250.119.16041654372152835222 08/06/22-07:23:27.011828	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41654	37215	192.168.2.23	156.250.119.160
192.168.2.23197.214.103.13250728372152835222 08/06/22-07:23:53.676873	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50728	37215	192.168.2.23	197.214.103.132
192.168.2.238.8.8.849581532012811 08/06/22-07:23:14.095323	UDP	2012811	ET DNS Query to a .tk domain - Likely Hostile	49581	53	192.168.2.23	8.8.8.8
192.168.2.23156.250.92.1653864637215283522 08/06/22-07:23:40.260566	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38646	37215	192.168.2.23	156.250.92.165
192.168.2.23156.244.80.945920037215283522 08/06/22-07:23:39.639416	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59200	37215	192.168.2.23	156.244.80.94
192.168.2.23156.226.11.155207237215283522 08/06/22-07:23:43.667446	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52072	37215	192.168.2.23	156.226.11.15
192.168.2.23156.245.51.255069437215283522 08/06/22-07:23:39.952103	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50694	37215	192.168.2.23	156.245.51.25

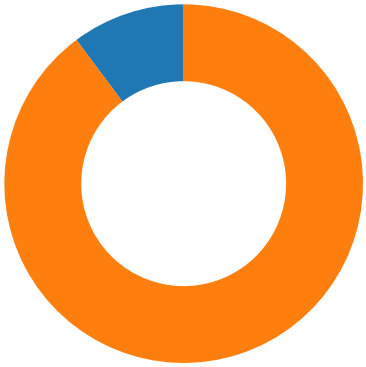
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.254.79.895311637215283522208/06/22-07:24:04.605598	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53116	37215	192.168.2.23	156.254.79.89
192.168.2.23156.235.102.13237424372152835222 08/06/22-07:23:43.645321	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37424	37215	192.168.2.23	156.235.102.132
192.168.2.23156.250.122.4049938372152835222 08/06/22-07:23:27.033187	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49938	37215	192.168.2.23	156.250.122.40
192.168.2.23156.226.27.13433390372152835222 08/06/22-07:24:04.960889	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33390	37215	192.168.2.23	156.226.27.134
192.168.2.23156.244.72.404719637215283522208/06/22-07:23:53.439628	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47196	37215	192.168.2.23	156.244.72.40
192.168.2.23156.244.109.9445444372152835222 08/06/22-07:23:29.654745	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45444	37215	192.168.2.23	156.244.109.94
192.168.2.23156.226.90.2416012037215283522208/06/22-07:23:53.442635	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60120	37215	192.168.2.23	156.226.90.241
192.168.2.23156.250.103.8844052372152835222 08/06/22-07:24:04.660457	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44052	37215	192.168.2.23	156.250.103.88
192.168.2.23156.224.11.123330637215283522208/06/22-07:24:04.797279	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33306	37215	192.168.2.23	156.224.11.12
192.168.2.23156.241.133.16536340372152835222 08/06/22-07:23:39.554681	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36340	37215	192.168.2.23	156.241.133.165
192.168.2.23156.250.113.19853300372152835222 08/06/22-07:23:27.034689	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53300	37215	192.168.2.23	156.250.113.198
192.168.2.23156.254.48.524174237215283522208/06/22-07:23:29.567245	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41742	37215	192.168.2.23	156.254.48.52
192.168.2.23156.250.74.2750752372152835222 08/06/22-07:23:16.433919	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50752	37215	192.168.2.23	156.250.74.27
192.168.2.23156.226.82.585128837215283522208/06/22-07:23:53.744332	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51288	37215	192.168.2.23	156.226.82.58
192.168.2.23156.224.29.1575029837215283522208/06/22-07:24:10.214896	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50298	37215	192.168.2.23	156.224.29.157
192.168.2.23156.226.84.1075914237215283522208/06/22-07:23:53.439665	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59142	37215	192.168.2.23	156.226.84.107
192.168.2.23156.241.91.2145444037215283522208/06/22-07:23:33.249369	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54440	37215	192.168.2.23	156.241.91.214
192.168.2.23156.244.110.22454676372152835222 08/06/22-07:23:59.102835	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54676	37215	192.168.2.23	156.244.110.224
192.168.2.23156.241.125.3655416372152835222 08/06/22-07:23:53.476267	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55416	37215	192.168.2.23	156.241.125.36

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.245.55.2 0053560372152835222 08/06/22- 07:24:04.679076	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53560	37215	192.168.2.23	156.245.55.200
192.168.2.23156.226.98.2 2635010372152835222 08/06/22- 07:23:33.273831	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35010	37215	192.168.2.23	156.226.98.226
192.168.2.23156.250.79.6 49098372152835222 08/06/22- 07:23:27.034355	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49098	37215	192.168.2.23	156.250.79.6
192.168.2.23156.250.18.2 2450598372152835222 08/06/22- 07:23:53.729151	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50598	37215	192.168.2.23	156.250.18.224
192.168.2.23156.230.20.3 1525343721528352 22 08/06/22- 07:23:27.220458	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52534	37215	192.168.2.23	156.230.20.31
192.168.2.23156.238.63.4 5425723721528352 22 08/06/22- 07:23:27.305057	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42572	37215	192.168.2.23	156.238.63.45
192.168.2.23197.234.61.2 3542192372152835222 08/06/22- 07:23:31.722171	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42192	37215	192.168.2.23	197.234.61.235
192.168.2.23156.241.66.2 4244510372152835222 08/06/22- 07:23:29.651725	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44510	37215	192.168.2.23	156.241.66.242
192.168.2.23156.250.9.15 8379623721528352 22 08/06/22- 07:24:04.676872	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37962	37215	192.168.2.23	156.250.9.158
192.168.2.23156.235.97.9 4588383721528352 22 08/06/22- 07:23:39.548075	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58838	37215	192.168.2.23	156.235.97.94
192.168.2.23156.235.96.1 2434606372152835222 08/06/22- 07:23:43.645351	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34606	37215	192.168.2.23	156.235.96.124
192.168.2.23156.224.20.1 3050850372152835222 08/06/22- 07:23:53.608016	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50850	37215	192.168.2.23	156.224.20.130
192.168.2.23156.224.13.1 4060786372152835222 08/06/22- 07:24:02.348307	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60786	37215	192.168.2.23	156.224.13.140
192.168.2.23156.245.34.6 3606683721528352 22 08/06/22- 07:23:39.647282	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60668	37215	192.168.2.23	156.245.34.63
192.168.2.23156.244.119. 2252904372152835222 08/06/22- 07:23:27.039494	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52904	37215	192.168.2.23	156.244.119.22
192.168.2.23156.226.103. 2647596372152835222 08/06/22- 07:23:27.316869	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47596	37215	192.168.2.23	156.226.103.26
192.168.2.23156.241.90.3 8427423721528352 22 08/06/22- 07:23:39.649878	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42742	37215	192.168.2.23	156.241.90.38
192.168.2.23156.226.96.3 3477183721528352 22 08/06/22- 07:23:40.227571	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47718	37215	192.168.2.23	156.226.96.33
192.168.2.23156.250.65.1 0041802372152835222 08/06/22- 07:23:52.152505	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41802	37215	192.168.2.23	156.250.65.100

Copyright Joe Security LLC 2022

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23156.250.115.6136870372152835222 08/06/22-07:23:33.241907	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36870	37215	192.168.2.23	156.250.115.61
192.168.2.23156.244.124.4735554372152835222 08/06/22-07:23:39.639516	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35554	37215	192.168.2.23	156.244.124.47
192.168.2.23156.245.59.2475563837215283522 2 08/06/22-07:23:40.240392	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55638	37215	192.168.2.23	156.245.59.247
192.168.2.23197.246.131.1855182372152835222 08/06/22-07:23:50.863914	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55182	37215	192.168.2.23	197.246.131.18
192.168.2.23156.250.116.15154632372152835222 08/06/22-07:23:53.717828	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54632	37215	192.168.2.23	156.250.116.151

Network Port Distribution



Total Packets: 98

- 23 (Telnet)
- 2323 undefined

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 07:23:14.095323086 CEST	192.168.2.23	8.8.8.8	0xa787	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 07:23:14.113378048 CEST	8.8.8.8	192.168.2.23	0xa787	No error (0)	cnc.fearfulcats.tk		185.225.73.158	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: notabotnet.mips PID: **6226**, Parent PID: **6121**

General

Start time:	07:23:13
Start date:	06/08/2022
Path:	/tmp/notabotnet.mips
Arguments:	/tmp/notabotnet.mips
File size:	5777432 bytes

MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: notabotnet.mips PID: **6228**, Parent PID: **6226**

General

Start time:	07:23:13
Start date:	06/08/2022
Path:	/tmp/notabotnet.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: notabotnet.mips PID: **6229**, Parent PID: **6226**

General

Start time:	07:23:13
Start date:	06/08/2022
Path:	/tmp/notabotnet.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: notabotnet.mips PID: **6232**, Parent PID: **6229**

General

Start time:	07:23:13
Start date:	06/08/2022
Path:	/tmp/notabotnet.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: notabotnet.mips PID: **6233**, Parent PID: **6229**

General

Start time:	07:23:13
Start date:	06/08/2022
Path:	/tmp/notabotnet.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: notabotnet.mips PID: **6235**, Parent PID: **6229**

General

Start time:	07:23:13
Start date:	06/08/2022
Path:	/tmp/notabotnet.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: notabotnet.mips PID: **6239**, Parent PID: **6229**

General

Start time:	07:23:13
Start date:	06/08/2022
Path:	/tmp/notabotnet.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: notabotnet.mips PID: **6241**, Parent PID: **6229**

General

Start time:	07:23:13
Start date:	06/08/2022
Path:	/tmp/notabotnet.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Copyright Joe Security LLC 2022