ID: 824729
Sample Name: bok.arm4.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 05:16:18
Date: 12/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Linux Analysis Report bok.arm4.elf 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
General Information 3
Warnings 3
Runtime Messages 3
Process Tree 4
Malware Threat Intel 4
Yara Signatures 4
Memory Dumps 4
Snort Signatures 5
Joe Sandbox Signatures 9
AV Detection 9
Networking 9
System Summary 9
Data Obfuscation 9
Hooking and other Techniques for Hiding and Protection 9
Stealing of Sensitive Information 9
Remote Access Functionality 9
Mitre Att&ck Matrix 9
Malware Configuration 10
Behavior Graph 10
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
Public IPs 11
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 14
General 14
Static ELF Info 14
ELF header 14
Program Segments 14
Network Behavior 14
Snort IDS Alerts 14
TCP Packets 16
System Behavior 16
Analysis Process: bok.arm4.elf PID: 6225, Parent PID: 6124 16
General 16
File Activities 16
File Deleted 16
File Read 16
Analysis Process: bok.arm4.elf PID: 6227, Parent PID: 6225 16
General 16
Analysis Process: bok.arm4.elf PID: 6231, Parent PID: 6225 17
General 17
Analysis Process: bok.arm4.elf PID: 6233, Parent PID: 6231 17
General 17
File Activities 17
File Read 17
Directory Enumerated 17

Linux Analysis Report

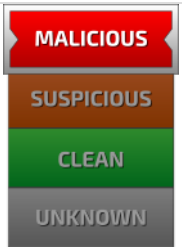
bok.arm4.elf

Overview

General Information

Sample Name:	bok.arm4.elf
Analysis ID:	824729
MD5:	ff8876ad3d74f5..
SHA1:	151f19870f309...
SHA256:	4463dcb9a23e...
Infos:	

Detection



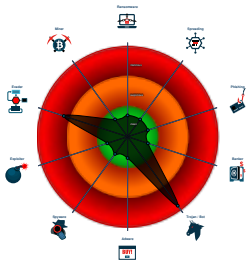
Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Snort IDS alert for network traffic
- Connects to many ports of the same...
- Sample deletes itself
- Sample is packed with UPX
- Uses known network protocols on n...
- Sample contains only a LOAD segm...
- Yara signature match
- Uses the "uname" system call to qu...

Classification



Analysis Advice

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

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

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

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	824729
Start date and time:	2023-03-12 05:16:18 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample file name:	bok.arm4.elf
Detection:	MAL
Classification:	mal100.troj.evad.linELF@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/bok.arm4.elf
PID:	6225
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	nkuvgpkpi/vwp2

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- bok.arm4.elf (PID: 6225, Parent: 6124, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/bok.arm4.elf
  - bok.arm4.elf New Fork (PID: 6227, Parent: 6225)
  - bok.arm4.elf New Fork (PID: 6231, Parent: 6225)
    - bok.arm4.elf New Fork (PID: 6233, Parent: 6231)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	**http://** osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
6225.1.00007fbe90030000.00007fbe90032000.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 (Nextron Systems)	• 0x1280:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x12f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1368:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13dc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1450:$xo1: oMXKNNC\x0D\x17\x0C\x12
6225.1.00007fbe90017000.00007fbe90029000.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth (Nextron Systems)	• 0x11398:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11408:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11478:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x114e8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11558:$xo1: oMXKNNC\x0D\x17\x0C\x12
6225.1.00007fbe90017000.00007fbe90029000.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth (Nextron Systems)	• 0x10824:$x1: POST /cdn-cgi/ • 0x110c0:$x2: /dev/misc/watchdog • 0x110b0:$x3: /dev/watchdog • 0x1121c:$s1: LCOGQGPTGP
6225.1.00007fbe90017000.00007fbe90029000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6225.1.00007fbe90017000.00007fbe90029000.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 1 entries				

Snort Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 154.19.234.248

Timestamp:	192.168.2.23154.19.234.2483434837215283522 2 03/12/23-05:17:57.544799
SID:	2835222
Source Port:	34348
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.207.118.67

Timestamp:	192.168.2.2341.207.118.6736896372152835222 03/12/23-05:18:37.130552
SID:	2835222
Source Port:	36896
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: 156.227.247.13

Timestamp:	192.168.2.23156.227.247.1334218372152835222 03/12/23-05:17:50.250143
SID:	2835222
Source Port:	34218
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: 154.38.248.168

Timestamp:	192.168.2.23154.38.248.16839184372152835222 03/12/23-05:18:32.237081
SID:	2835222
Source Port:	39184
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: 154.216.16.124

Timestamp:	192.168.2.23154.216.16.12449296372152835222 03/12/23-05:18:20.924509
SID:	2835222
Source Port:	49296
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: 154.213.169.4

Timestamp:	192.168.2.23154.213.169.436896372152835222 03/12/23-05:18:44.909112
SID:	2835222
Source Port:	36896
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: 154.213.173.160

Timestamp:	192.168.2.23154.213.173.16047660372152835222 03/12/23-05:18:44.622777
SID:	2835222
Source Port:	47660

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: 156.234.225.226	
Timestamp:	192.168.2.23156.234.225.226370323721528352222 03/12/23-05:17:29.066566
SID:	2835222
Source Port:	37032
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: 102.40.126.190	
Timestamp:	192.168.2.23102.40.126.190588843721528352222 03/12/23-05:18:05.376218
SID:	2835222
Source Port:	58884
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: 156.230.16.234	
Timestamp:	192.168.2.23156.230.16.23438748372152835222 03/12/23-05:18:30.058003
SID:	2835222
Source Port:	38748
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: 154.209.31.63	
Timestamp:	192.168.2.23154.209.31.6343486372152835222 03/12/23-05:17:45.055690
SID:	2835222
Source Port:	43486
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: 154.204.17.82	
Timestamp:	192.168.2.23154.204.17.8238056372152835222 03/12/23-05:18:36.979130
SID:	2835222
Source Port:	38056
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: 154.211.43.115	
Timestamp:	192.168.2.23154.211.43.11533822372152835222 03/12/23-05:18:36.710288
SID:	2835222
Source Port:	33822
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: 154.213.169.213	
Timestamp:	192.168.2.23154.213.169.213519523721528352222 03/12/23-05:18:40.580988
SID:	2835222
Source Port:	51952
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: 156.254.95.210	
Timestamp:	192.168.2.23156.254.95.21040830372152835222 03/12/23-05:18:44.343254
SID:	2835222
Source Port:	40830
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: 154.209.26.25	
Timestamp:	192.168.2.23154.209.26.2546366372152835222 03/12/23-05:18:10.783427
SID:	2835222
Source Port:	46366
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: 156.226.14.114	
Timestamp:	192.168.2.23156.226.14.11445010372152835222 03/12/23-05:18:20.661510
SID:	2835222
Source Port:	45010
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: 154.31.146.13	
Timestamp:	192.168.2.23154.31.146.1337040372152835222 03/12/23-05:17:49.802953
SID:	2835222
Source Port:	37040
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: 154.211.19.73	
Timestamp:	192.168.2.23154.211.19.7350986372152835222 03/12/23-05:18:24.485789
SID:	2835222
Source Port:	50986
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: 154.211.19.101	
Timestamp:	192.168.2.23154.211.19.10143806372152835222 03/12/23-05:18:14.073818
SID:	2835222
Source Port:	43806
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: 102.41.23.85	
Timestamp:	192.168.2.23102.41.23.8533974372152835222 03/12/23-05:17:14.142346
SID:	2835222
Source Port:	33974
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: 154.211.34.178	
Timestamp:	192.168.2.23154.211.34.17855604372152835222 03/12/23-05:17:31.611571
SID:	2835222
Source Port:	55604

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: 154.180.50.188	
Timestamp:	192.168.2.23154.180.50.18835924372152835222 03/12/23-05:18:42.971077
SID:	2835222
Source Port:	35924
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: 156.226.15.117	
Timestamp:	192.168.2.23156.226.15.11751314372152835222 03/12/23-05:17:42.504437
SID:	2835222
Source Port:	51314
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: 154.213.170.53	
Timestamp:	192.168.2.23154.213.170.5334086372152835222 03/12/23-05:17:57.826173
SID:	2835222
Source Port:	34086
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 156.254.80.218	
Timestamp:	192.168.2.23156.254.80.21852140372152835222 03/12/23-05:17:52.806535
SID:	2835222
Source Port:	52140
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: 154.213.160.194	
Timestamp:	192.168.2.23154.213.160.19445592372152835222 03/12/23-05:17:45.594474
SID:	2835222
Source Port:	45592
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: 156.254.41.166	
Timestamp:	192.168.2.23156.254.41.16636386372152835222 03/12/23-05:17:57.371110
SID:	2835222
Source Port:	36386
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.0.88.109	
Timestamp:	192.168.2.2341.0.88.10937906372152835222 03/12/23-05:17:26.528007
SID:	2835222
Source Port:	37906
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

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

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection

Sample deletes itself

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

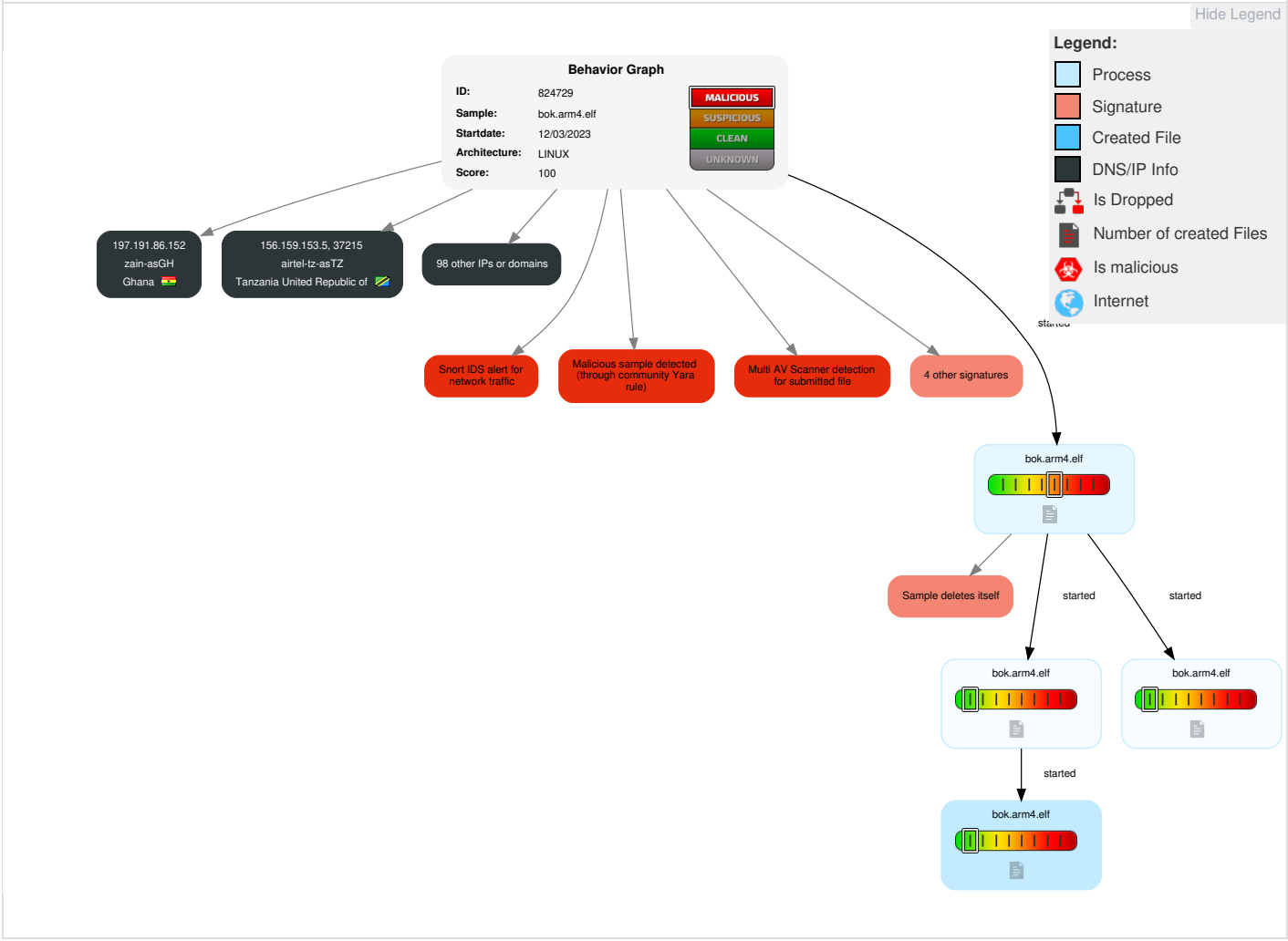
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 1 Obfuscated Files or Information	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File Deletion	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bok.arm4.elf	25%	Virustotal		Browse
bok.arm4.elf	23%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

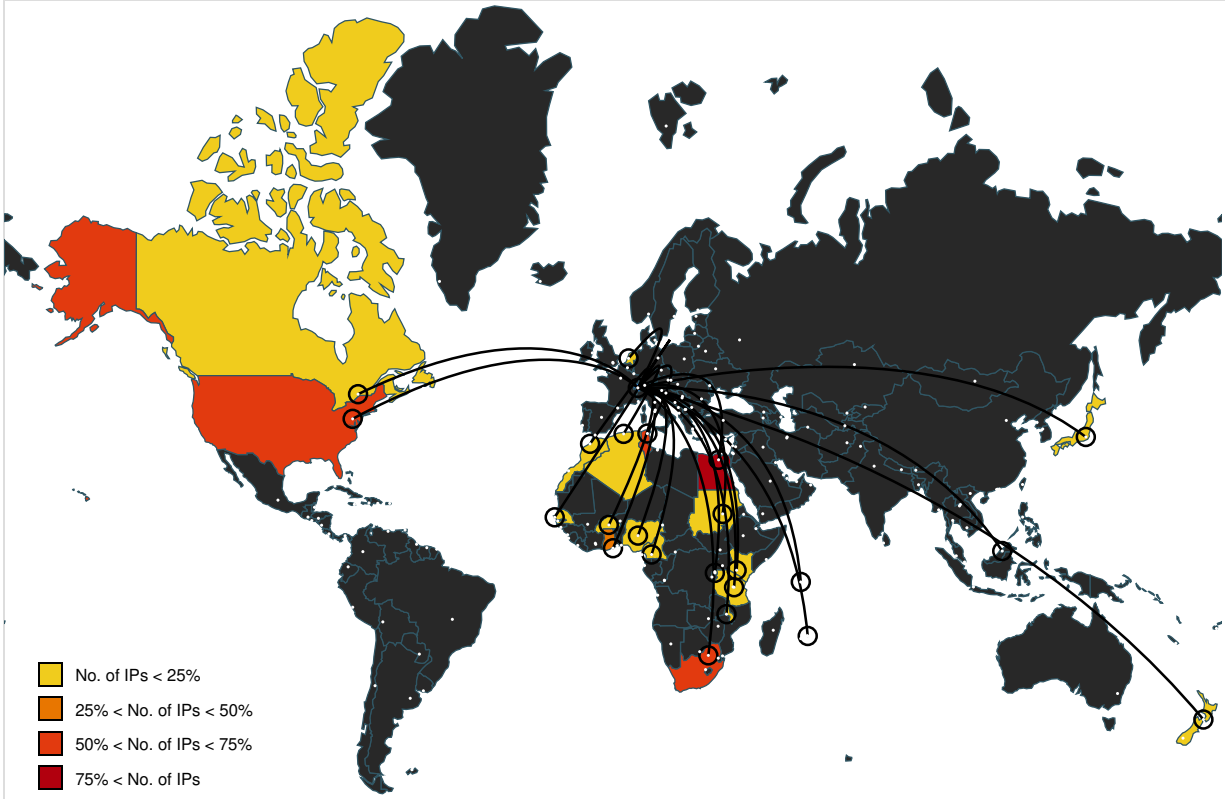
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.15.176.249	unknown	South Africa		29975	VODACOM-ZA	false
41.186.122.25	unknown	Rwanda		36890	MTNRW-ASNRW	false
154.208.6.173	unknown	Seychelles		40065	CNSERVERSUS	false
102.92.82.227	unknown	Nigeria		37075	ZAINUGASUG	false
156.252.248.209	unknown	Seychelles		53587	AZTUS	false
197.225.3.101	unknown	Mauritius		23889	MauritiusTelecomMU	false
41.68.176.212	unknown	Egypt		24835	RAYA-ASEG	false
102.100.91.163	unknown	Morocco		36925	ASMediMA	false
197.58.164.142	unknown	Egypt		8452	TE-ASTE-ASEG	false
154.12.167.37	unknown	United States		55286	SERVER-MANIACA	false
102.70.3.64	unknown	Malawi		37294	TNMMW	false
156.230.19.162	unknown	Seychelles		135357	SKHT-ASShenzhenKatherineHengTechnologyInformationCo	false
102.76.124.241	unknown	Morocco		6713	IAM-ASMA	false
41.53.150.173	unknown	South Africa		37168	CELL-CZA	false
41.205.177.107	unknown	unknown		36974	AFNET-ASCI	false
197.44.30.166	unknown	Egypt		8452	TE-ASTE-ASEG	false
154.172.105.135	unknown	Ghana		30986	SCANCOMGH	false
41.76.191.229	unknown	Kenya		37225	NETWIDEZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.83.202.14	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
154.238.173.206	unknown	Egypt		36992	ETISALAT-MISREG	false
41.131.206.203	unknown	Egypt		24863	LINKdotNET-ASEG	false
197.180.156.40	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
154.45.54.149	unknown	United States		394973	AARKIUS	false
154.137.125.109	unknown	Egypt		37069	MOBINILEG	false
41.230.97.150	unknown	Tunisia		37705	TOPNETTN	false
102.223.137.3	unknown	unknown		328096	TruIT-Uganda-ASUG	false
197.191.86.152	unknown	Ghana		37140	zain-asGH	false
41.152.180.54	unknown	Egypt		36992	ETISALAT-MISREG	false
197.207.57.201	unknown	Algeria		36947	ALGTEL-ASDZ	false
102.39.2.24	unknown	South Africa		11845	Vox-TelecomZA	false
154.248.34.184	unknown	Algeria		36947	ALGTEL-ASDZ	false
102.189.179.190	unknown	Egypt		24835	RAYA-ASEG	false
156.159.153.5	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
197.234.45.9	unknown	Nigeria		29286	SKYLOGIC-ASIT	false
41.69.166.105	unknown	Egypt		24835	RAYA-ASEG	false
197.102.171.164	unknown	South Africa		3741	ISZA	false
197.43.225.162	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.244.252.216	unknown	Cameroon		37620	VIETTEL-CM-ASCM	false
156.13.131.16	unknown	New Zealand		22192	SSHENETUS	false
102.20.106.72	unknown	unknown		37054	Telecom-MalagasyMG	false
154.46.181.233	unknown	United States		174	COGENT-174US	false
197.222.122.254	unknown	Egypt		37069	MOBINILEG	false
41.228.223.102	unknown	Tunisia		37693	TUNISIANATN	false
41.101.160.215	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.228.223.104	unknown	Tunisia		37693	TUNISIANATN	false
41.115.248.58	unknown	South Africa		16637	MTNNS-ASZA	false
156.57.94.231	unknown	Canada		855	CANET-ASN-4CA	false
154.138.186.246	unknown	Egypt		37069	MOBINILEG	false
156.19.45.163	unknown	United States		20115	CHARTER-20115US	false
197.44.30.189	unknown	Egypt		8452	TE-ASTE-ASEG	false
102.238.170.160	unknown	unknown		36926	CKL1-ASNKE	false
102.20.131.234	unknown	unknown		37054	Telecom-MalagasyMG	false
41.145.178.44	unknown	South Africa		5713	SAIX-NETZA	false
102.171.69.12	unknown	Tunisia		37693	TUNISIANATN	false
197.224.88.168	unknown	Mauritius		23889	MauritiusTelecomMU	false
197.31.148.1	unknown	Tunisia		37492	ORANGE-TN	false
156.69.160.242	unknown	New Zealand		297	AS297US	false
154.191.53.242	unknown	Egypt		8452	TE-ASTE-ASEG	false
102.49.146.60	unknown	Morocco		6713	IAM-ASMA	false
102.180.204.193	unknown	Burkina Faso		37577	Orange-BF	false
154.3.74.178	unknown	United States		174	COGENT-174US	false
197.21.65.71	unknown	Tunisia		37693	TUNISIANATN	false
41.157.30.78	unknown	South Africa		37168	CELL-CZA	false
102.123.192.249	unknown	Sudan		36972	MTNSD	false
197.226.240.74	unknown	Mauritius		23889	MauritiusTelecomMU	false
156.134.83.87	unknown	United States		12217	UPSUS	false
154.74.136.186	unknown	Tanzania United Republic of		37035	MIC-ASTZ	false
102.19.228.39	unknown	unknown		37054	Telecom-MalagasyMG	false
197.220.166.155	unknown	Ghana		37341	GLOMOBILEGH	false
154.90.150.5	unknown	Seychelles		139086	ONL-HKOCEANNETWORKLIMITEDHK	false
197.70.186.122	unknown	South Africa		16637	MTNNS-ASZA	false
197.252.28.241	unknown	Sudan		15706	SudatelSD	false
154.104.45.83	unknown	Tunisia		37693	TUNISIANATN	false
41.227.18.91	unknown	Tunisia		2609	TN-BB-ASTunisiaBackBoneASTN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.184.139.222	unknown	South Africa		37105	NEOLOGY-ASZA	false
102.71.74.71	unknown	Malawi		37294	TNMMW	false
154.160.107.246	unknown	Ghana		30986	SCANCOMGH	false
197.10.162.34	unknown	Tunisia		5438	ATI-TN	false
156.21.96.232	unknown	United States		29975	VODACOM-ZA	false
197.159.104.99	unknown	Kenya		37421	CellulantKE	false
197.129.147.248	unknown	Morocco		6713	IAM-ASMA	false
156.31.73.48	unknown	Brunei Darussalam		34542	SAFRANHE-ASFR	false
41.233.34.193	unknown	Egypt		8452	TE-ASTE-ASEG	false
154.181.109.188	unknown	Egypt		8452	TE-ASTE-ASEG	false
156.93.179.205	unknown	United States		10695	WAL-MARTUS	false
154.169.82.115	unknown	Ghana		30986	SCANCOMGH	false
102.117.64.194	unknown	Mauritius		23889	MauritiusTelecomMU	false
156.55.15.84	unknown	United States		20746	ASN-IDCTNOOMINCIT	false
41.45.188.9	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.217.104.36	unknown	Nigeria		37340	SpectranetNG	false
154.134.179.151	unknown	Egypt		37069	MOBINILEG	false
41.82.8.140	unknown	Senegal		8346	SONATEL-ASAutonomousSystemEU	false
102.134.128.199	unknown	South Africa		328370	BlueLabel-ASZA	false
154.34.112.125	unknown	Japan		4694	IDCFIDCFrontierIncJP	false
197.86.191.144	unknown	South Africa		10474	OPTINETZA	false
102.168.253.92	unknown	Tunisia		37693	TUNISIANATN	false
197.96.225.180	unknown	South Africa		3741	ISZA	false
154.54.76.14	unknown	United States		174	COGENT-174US	false
197.254.70.209	unknown	Kenya		15808	ACCESSKENYA-KEACCESSKENYAGROUP LTDisanISPservingKE	false
41.136.36.196	unknown	Mauritius		23889	MauritiusTelecomMU	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, no section header
Entropy (8bit):	7.942727344674702
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	bok.arm4.elf
File size:	29020
MD5:	ff8876ad3d74f54de1080fe2ac2a2fcd
SHA1:	151f19870f309dd13b6b2749c08a1f4f087f6176
SHA256:	4463dcb9a23e3cead700d2d8259d23ae0af161338195c246ff57d88983c2a12f
SHA512:	4d78737525794c724d1e50947d9c88e68708ab9d488356545bee9afa8a520dbf7e4bac4b56be52055a0c4534df7a890b435ff781505d308c1637145590d9159e
SSDEEP:	768:LgOG2wQY6KZq1kSz6d/lUYpOXmig3renrrjeWs3qV9PKs3UozDo:LgvwXDkSG9nOWigbOfjCO/zDo
TLSH:	79D2E0F59B9FD550E3200D39782C52D172364BF6D5BB23C36298F630B3CA44A11B651E
File Content Preview:	.ELF...a.....(.....4.....4. ... (.....op..op.....Q.td.....s.y.UPX!.....|...|.....S.....?.E.h;.}...^.....fT.`..%.",.....n7..lo....b.....w.c).w$Cb.W..

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

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	0x706f	0x706f	7.9460	0x5	R E	0x8000		
LOAD	0x1ee4	0x21ee4	0x21ee4	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23154.19.234.2 4834348372152835222 03/12/23- 05:17:57.544799	TCP	283522 2	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34348	37215	192.168.2.23	154.19.234.2 48

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2341.207.118.67368963721528352220 3/12/23-05:18:37.130552	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36896	37215	192.168.2.23	41.207.118.67
192.168.2.23156.227.247.13342183721528352220 3/12/23-05:17:50.250143	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34218	37215	192.168.2.23	156.227.247.13
192.168.2.23154.38.248.168391843721528352220 3/12/23-05:18:32.237081	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39184	37215	192.168.2.23	154.38.248.168
192.168.2.23154.216.16.124492963721528352220 3/12/23-05:18:20.924509	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49296	37215	192.168.2.23	154.216.16.124
192.168.2.23154.213.169.43689637215283522 03/12/23-05:18:44.909112	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36896	37215	192.168.2.23	154.213.169.4
192.168.2.23154.213.173.160476603721528352220 3/12/23-05:18:44.622777	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47660	37215	192.168.2.23	154.213.173.160
192.168.2.23156.234.225.226370323721528352220 3/12/23-05:17:29.066566	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37032	37215	192.168.2.23	156.234.225.226
192.168.2.23102.40.126.190588843721528352220 3/12/23-05:18:05.376218	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58884	37215	192.168.2.23	102.40.126.190
192.168.2.23156.230.16.234387483721528352220 3/12/23-05:18:30.058003	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38748	37215	192.168.2.23	156.230.16.234
192.168.2.23154.209.31.634348637215283522 03/12/23-05:17:45.055690	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43486	37215	192.168.2.23	154.209.31.63
192.168.2.23154.204.17.823805637215283522 03/12/23-05:18:36.979130	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38056	37215	192.168.2.23	154.204.17.82
192.168.2.23154.211.43.115338223721528352220 3/12/23-05:18:36.710288	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33822	37215	192.168.2.23	154.211.43.115
192.168.2.23154.213.169.213519523721528352220 3/12/23-05:18:40.580988	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51952	37215	192.168.2.23	154.213.169.213
192.168.2.23156.254.95.210408303721528352220 3/12/23-05:18:44.343254	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40830	37215	192.168.2.23	156.254.95.210
192.168.2.23154.209.26.254636637215283522 03/12/23-05:18:10.783427	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46366	37215	192.168.2.23	154.209.26.25
192.168.2.23156.226.14.114450103721528352220 3/12/23-05:18:20.661510	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45010	37215	192.168.2.23	156.226.14.114
192.168.2.23154.31.146.133704037215283522 03/12/23-05:17:49.802953	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37040	37215	192.168.2.23	154.31.146.13
192.168.2.23154.211.19.735098637215283522 03/12/23-05:18:24.485789	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50986	37215	192.168.2.23	154.211.19.73
192.168.2.23154.211.19.101438063721528352220 3/12/23-05:18:14.073818	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	43806	37215	192.168.2.23	154.211.19.101

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23102.41.23.85 33974372152835222 03/12/23-05:17:14.142346	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33974	37215	192.168.2.23	102.41.23.85
192.168.2.23154.211.34.178556043721528352222 03/12/23-05:17:31.611571	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55604	37215	192.168.2.23	154.211.34.178
192.168.2.23154.180.50.188359243721528352222 03/12/23-05:18:42.971077	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35924	37215	192.168.2.23	154.180.50.188
192.168.2.23156.226.15.117513143721528352222 03/12/23-05:17:42.504437	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51314	37215	192.168.2.23	156.226.15.117
192.168.2.23154.213.170.53340863721528352222 03/12/23-05:17:57.826173	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34086	37215	192.168.2.23	154.213.170.53
192.168.2.23156.254.80.218521403721528352222 03/12/23-05:17:52.806535	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52140	37215	192.168.2.23	156.254.80.218
192.168.2.23154.213.160.194455923721528352222 03/12/23-05:17:45.594474	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45592	37215	192.168.2.23	154.213.160.194
192.168.2.23156.254.41.166636863721528352222 03/12/23-05:17:57.371110	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	36386	37215	192.168.2.23	156.254.41.166
192.168.2.2341.0.88.1093790637215283522 2 03/12/23-05:17:26.528007	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37906	37215	192.168.2.23	41.0.88.109

TCP Packets

System Behavior

Analysis Process: bok.arm4.elf PID: 6225, Parent PID: 6124

General

Start time:	05:17:02
Start date:	12/03/2023
Path:	/tmp/bok.arm4.elf
Arguments:	/tmp/bok.arm4.elf
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Deleted

File Read

Analysis Process: bok.arm4.elf PID: 6227, Parent PID: 6225

General

Start time:	05:17:03
Start date:	12/03/2023
Path:	/tmp/bok.arm4.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: bok.arm4.elf PID: **6231**, Parent PID: **6225**

General

Start time:	05:17:03
Start date:	12/03/2023
Path:	/tmp/bok.arm4.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: bok.arm4.elf PID: **6233**, Parent PID: **6231**

General

Start time:	05:17:03
Start date:	12/03/2023
Path:	/tmp/bok.arm4.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated