ID: 830835
Sample Name: jLj9r6JMDk.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 18:20:38
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

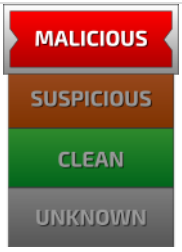
jLj9r6JMDk.elf

Overview

General Information

Sample Name:	jLj9r6JMDk.elf
Original Sample Name:	8ae7efa328fec…
Analysis ID:	830835
MD5:	8ae7efa328fec…
SHA1:	8bbe17f81b4da..
SHA256:	3978ed2047b1…
Tags:	32 arm elf mirai
Infos:	

Detection



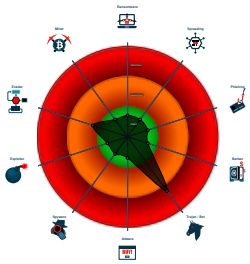
Mirai

Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Yara signature match
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Sample contains strings indicative o…

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.

Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

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:	830835
Start date and time:	2023-03-20 18:20:38 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
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:	jLj9r6JMDk.elf
Original Sample Name:	8ae7efa328fec5e08a5de6468a446f4a.elf
Detection:	MAL
Classification:	mal64.troj.linELF@0/0@0/0

Runtime Messages

Command:	/tmp/jLj9r6JMDk.elf
PID:	6230
Exit Code:	255
Exit Code Info:	
Killed:	False

Standard Output:	
Standard Error:	/lib/ld-uClibc.so.0: No such file or directory

Process Tree

- **system is lnxubuntu20**
  - jLj9r6JMDk.elf (PID: 6230, Parent: 6131, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/jLj9r6JMDk.elf
- **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

Initial Sample

Source	Rule	Description	Author	Strings
jLj9r6JMDk.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
jLj9r6JMDk.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x8cf4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d08:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d1c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d30:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d44:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d58:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d6c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d80:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d94:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8da8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8dbc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8dd0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8de4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8df8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e0c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e20:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e34:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e48:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e70:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F

Memory Dumps

Source	Rule	Description	Author	Strings
6230.1.00007fc8c8028000.00007fc8c8029000.rw-.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x14:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x28:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x3c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x50:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x64:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x78:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xa0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xb4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6230.1.00007fc8c8017000.00007fc8c8021000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6230.1.00007fc8c8017000.00007fc8c8021000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x8cf4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d08:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d1c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d30:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d44:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d58:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d6c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d80:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8d94:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8da8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8dbc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8dd0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8de4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8df8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e0c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e20:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e34:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e48:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e70:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
Process Memory Space: jLj9r6JMDk.elf PID: 6230	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x73d:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x751:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x765:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x779:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x78d:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x7a1:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x7b5:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x7c9:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x7dd:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x7f1:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x805:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11f46:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11f5a:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11f6e:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11f82:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11f96:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11faa:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11fbe:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11fd2:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11fe6:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11ffa:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

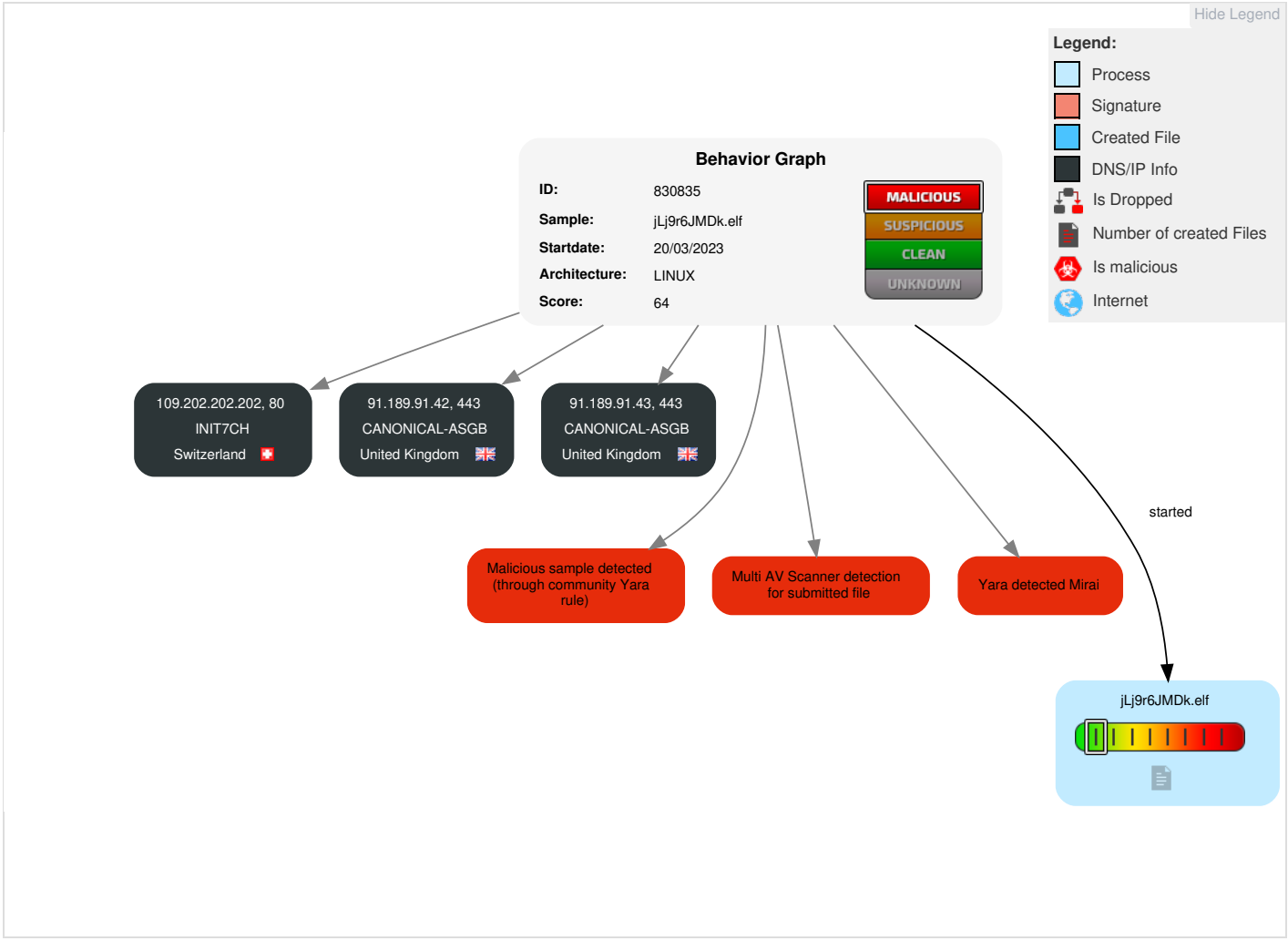
Mitre Att&ck Matrix

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	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 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
jLj9r6JMDk.elf	54%	ReversingLabs	Linux.Trojan.Mirai	
jLj9r6JMDk.elf	47%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

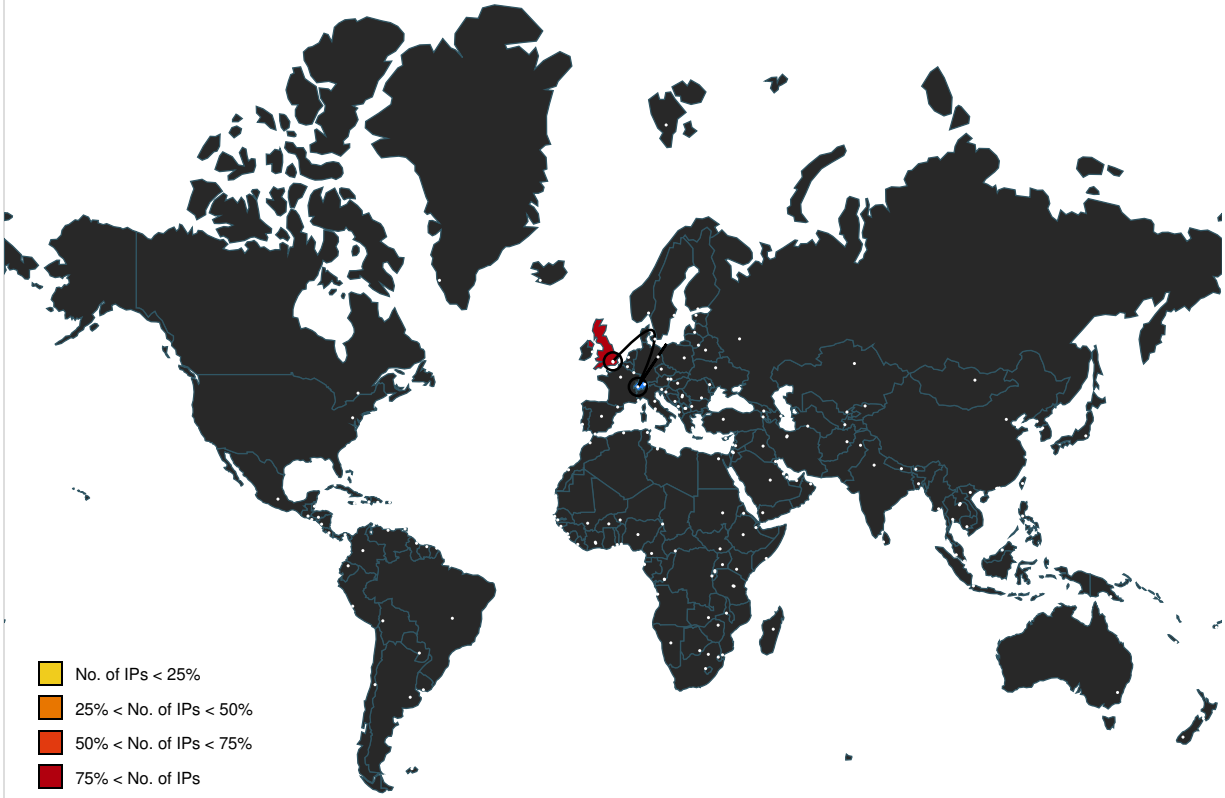
Domains and IPs

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
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	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), dynamically linked, interpreter /lib/ld-uClibc.so.0, stripped
Entropy (8bit):	6.078711447230125
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	jLj9r6JMDk.elf
File size:	40748
MD5:	8ae7efa328fec5e08a5de6468a446f4a
SHA1:	8bbe17f81b4dabcac4e15fdc1c938e524c45dd68
SHA256:	3978ed2047b1ae6757eb424c4858c644dd2f6ade4023cddcb6582e2b5532f107
SHA512:	0666776ab1a1fe924aecf590270b56de2571f1e75ac6ce1f49ff938aa2df08a0683bbd47537b77335ee60753d22ff3209651db384bfa556076309fe71d2ba6cc
SSDEEP:	768:QgFcCbwsG5f0OlnlUlQOBFdApwA3b9zjWl6v+bJ/9kJXoT1/N/wW5:QmbPG5fXlUlbH4pmQv+gJWOW
TLSH:	6A03E751BC829A67C2E1137AB66E5A8D336167ECD2CFB217DD204B207AD511F0D23F85
File Content Preview:	.ELF...a.....(.....4...\.....4. ... (.....4...4...4.....4...4.....8...8...8.....L...L...L.....Q.td...../lib/ld-uCl

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:	

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.interp	PROGBITS	0x80f4	0xf4	0x14	0x0	0x2	A	0	0	1
.hash	HASH	0x8108	0x108	0x234	0x4	0x2	A	3	0	4
.dynsym	DYNSYM	0x833c	0x33c	0x480	0x10	0x2	A	4	1	4
.dynstr	STRTAB	0x87bc	0x7bc	0x230	0x0	0x2	A	0	0	1
.rel.plt	REL	0x89ec	0x9ec	0x1a0	0x8	0x2	A	3	7	4
.init	PROGBITS	0x8b8c	0xb8c	0x18	0x0	0x6	AX	0	0	4
.plt	PROGBITS	0x8ba4	0xba4	0x284	0x4	0x6	AX	0	0	4
.text	PROGBITS	0x8e28	0xe28	0x7ddc	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x10c04	0x8c04	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x10c18	0x8c18	0xe1c	0x0	0x2	A	0	0	4

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.ctors	PROGBITS	0x19a38	0x9a38	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x19a40	0x9a40	0x8	0x0	0x3	WA	0	0	4
.dynamic	DYNAMIC	0x19a4c	0x9a4c	0x98	0x8	0x3	WA	4	0	4
.got	PROGBITS	0x19ae4	0x9ae4	0xdc	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x19bc0	0x9bc0	0x28	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x19be8	0x9be8	0x124	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x9be8	0x73	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
PHDR	0x34	0x8034	0x8034	0xc0	0xc0	2.2460	0x5	R E	0x4		
INTERP	0xf4	0x80f4	0x80f4	0x14	0x14	3.6842	0x4	R	0x1	/lib/ld-uClibc.so.0	.interp
LOAD	0x0	0x8000	0x8000	0x9a34	0x9a34	6.1250	0x5	R E	0x8000		.interp .hash .dynsym .dynstr .rel.plt .init .plt .text .fini .rodata
LOAD	0x9a38	0x19a38	0x19a38	0x1b0	0x2d4	2.3215	0x6	RW	0x8000		.ctors .dtors .dynamic .got .data .bss
DYNAMIC	0x9a4c	0x19a4c	0x19a4c	0x98	0x98	1.8984	0x6	RW	0x4		.dynamic
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Dynamic Tags

Type	Meta	Value	Tag
DT_NEEDED	sharedlib	libc.so.0	0x1
DT_INIT	value	0x8b8c	0xc
DT_FINI	value	0x10c04	0xd
DT_HASH	value	0x8108	0x4
DT_STRTAB	value	0x87bc	0x5
DT_SYMTAB	value	0x833c	0x6
DT_STRSZ	bytes	560	0xa
DT_SYMENT	bytes	16	0xb
DT_DEBUG	value	0x0	0x15
DT_PLTGOT	value	0x19ae4	0x3
DT_PLTRELSZ	bytes	416	0x2
DT_PLTREL	pltrel	DT_REL	0x14
DT_JMPREL	value	0x89ec	0x17
DT_NULL	value	0x0	0x0

Symbols

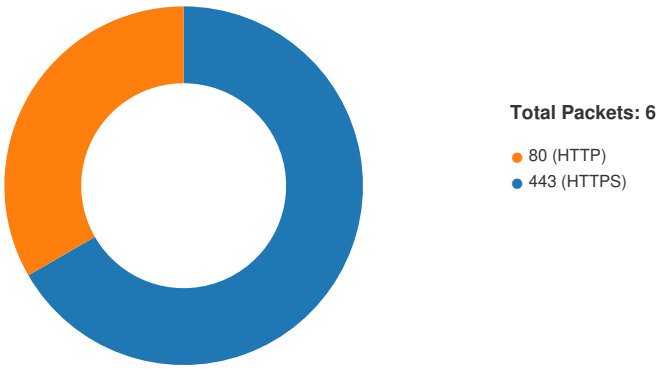
Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
			.dynsym	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__aeabi_idiv0			.dynsym	0x10b74	4	FUNC	<unknown>	DEFAULT	8
__aeabi_ldiv0			.dynsym	0x10b74	4	FUNC	<unknown>	DEFAULT	8
__aeabi_uidiv			.dynsym	0x108b4	0	FUNC	<unknown>	DEFAULT	8
__aeabi_uidivmod			.dynsym	0x109ac	24	FUNC	<unknown>	DEFAULT	8
__bss_end__			.dynsym	0x19d0c	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__bss_start			.dynsym	0x19be8	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__bss_start__			.dynsym	0x19be8	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__data_start			.dynsym	0x19bc0	0	NOTYPE	<unknown>	DEFAULT	17
__div0			.dynsym	0x10b74	4	FUNC	<unknown>	DEFAULT	8
__end__			.dynsym	0x19d0c	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__errno_location			.dynsym	0x8d98	32	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__modsi3			.dynsym	0x10a90	228	FUNC	<unknown>	DEFAULT	8
__muldi3			.dynsym	0x10b78	80	FUNC	<unknown>	DEFAULT	8
__uClibc_main			.dynsym	0x8d2c	488	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__udivsi3			.dynsym	0x108b4	248	FUNC	<unknown>	DEFAULT	8

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__umodsi3			.dynsym	0x109c4	204	FUNC	<unknown>	DEFAULT	8
_bss_end__			.dynsym	0x19d0c	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_edata			.dynsym	0x19be8	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_end			.dynsym	0x19d0c	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_exit			.dynsym	0x8db0	40	FUNC	<unknown>	DEFAULT	SHN_UNDEF
_start			.dynsym	0x8f08	80	FUNC	<unknown>	DEFAULT	8
abort			.dynsym	0x8c6c	352	FUNC	<unknown>	DEFAULT	SHN_UNDEF
accept			.dynsym	0x8c78	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
bind			.dynsym	0x8ca8	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
calloc			.dynsym	0x8c84	88	FUNC	<unknown>	DEFAULT	SHN_UNDEF
clock			.dynsym	0x8dd4	52	FUNC	<unknown>	DEFAULT	SHN_UNDEF
close			.dynsym	0x8e04	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
closedir			.dynsym	0x8dec	196	FUNC	<unknown>	DEFAULT	SHN_UNDEF
connect			.dynsym	0x8bc4	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
exit			.dynsym	0x8da4	172	FUNC	<unknown>	DEFAULT	SHN_UNDEF
fcntl			.dynsym	0x8df8	116	FUNC	<unknown>	DEFAULT	SHN_UNDEF
fork			.dynsym	0x8d20	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
free			.dynsym	0x8e10	288	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getpid			.dynsym	0x8bdc	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getppid			.dynsym	0x8d50	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getsockname			.dynsym	0x8e1c	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getsockopt			.dynsym	0x8d80	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
inet_addr			.dynsym	0x8cb4	36	FUNC	<unknown>	DEFAULT	SHN_UNDEF
kill			.dynsym	0x8c9c	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
listen			.dynsym	0x8d14	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
malloc			.dynsym	0x8c0c	400	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memcpy			.dynsym	0x8bf4	4	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memmove			.dynsym	0x8bd0	4	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memset			.dynsym	0x8d38	156	FUNC	<unknown>	DEFAULT	SHN_UNDEF
open			.dynsym	0x8dc8	92	FUNC	<unknown>	DEFAULT	SHN_UNDEF
opendir			.dynsym	0x8d68	264	FUNC	<unknown>	DEFAULT	SHN_UNDEF
prctl			.dynsym	0x8be8	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
rand			.dynsym	0x8cd8	4	FUNC	<unknown>	DEFAULT	SHN_UNDEF
read			.dynsym	0x8ce4	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
readdir			.dynsym	0x8c54	224	FUNC	<unknown>	DEFAULT	SHN_UNDEF
readlink			.dynsym	0x0	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
realloc			.dynsym	0x8cfc	312	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
recv			.dynsym	0x8bb8	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
recvfrom			.dynsym	0x8c30	52	FUNC	<unknown>	DEFAULT	SHN_UNDEF
remove			.dynsym	0x8c18	72	FUNC	<unknown>	DEFAULT	SHN_UNDEF
select			.dynsym	0x8c48	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
send			.dynsym	0x8c60	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sendto			.dynsym	0x8cf0	52	FUNC	<unknown>	DEFAULT	SHN_UNDEF
setsid			.dynsym	0x8de0	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
setsockopt			.dynsym	0x8cc0	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sleep			.dynsym	0x8c24	420	FUNC	<unknown>	DEFAULT	SHN_UNDEF
socket			.dynsym	0x8c3c	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sprintf			.dynsym	0x8d74	52	FUNC	<unknown>	DEFAULT	SHN_UNDEF
srand			.dynsym	0x8d44	148	FUNC	<unknown>	DEFAULT	SHN_UNDEF
stat			.dynsym	0x8d8c	80	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strlen			.dynsym	0x8dbc	96	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strstr			.dynsym	0x8ccc	248	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strtok			.dynsym	0x8d08	36	FUNC	<unknown>	DEFAULT	SHN_UNDEF
system			.dynsym	0x8c00	336	FUNC	<unknown>	DEFAULT	SHN_UNDEF
time			.dynsym	0x8d5c	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
write			.dynsym	0x8c90	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: jLj9r6JMDk.elf PID: **6230**, Parent PID: **6131**

General

Start time:	18:21:29
Start date:	20/03/2023
Path:	/tmp/jLj9r6JMDk.elf
Arguments:	/tmp/jLj9r6JMDk.elf
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read