ID: 626474
Sample Name: 0rK5XxDyLK
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:19:55
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

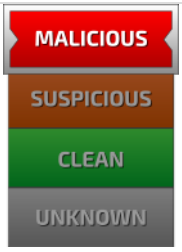
0rK5XxDyLK

Overview

General Information

Sample Name:	0rK5XxDyLK
Analysis ID:	626474
MD5:	b440222d627a07.
SHA1:	63be0315c844d0..
SHA256:	eae51f23834e02..
Tags:	32 arm elf mirai
Infos:	

Detection



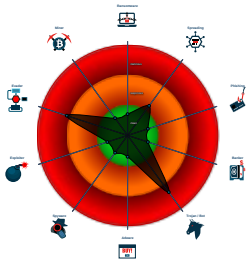
Mirai

Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- 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…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample listens on a socket

Classification



Analysis Advice

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

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626474
Start date and time: 14/05/202204:19:55	2022-05-14 04:19:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0rK5XxDyLK
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:	mal64.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/0rK5XxDyLK
PID:	6225
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 0rK5XxDyLK (PID: 6225, Parent: 6126, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/0rK5XxDyLK
  - 0rK5XxDyLK New Fork (PID: 6227, Parent: 6225)
    - 0rK5XxDyLK New Fork (PID: 6333, Parent: 6227)
    - 0rK5XxDyLK New Fork (PID: 6334, Parent: 6227)
      - 0rK5XxDyLK New Fork (PID: 6337, Parent: 6334)
        - 0rK5XxDyLK New Fork (PID: 6346, Parent: 6337)
        - 0rK5XxDyLK New Fork (PID: 6347, Parent: 6337)
      - 0rK5XxDyLK New Fork (PID: 6339, Parent: 6334)
      - 0rK5XxDyLK New Fork (PID: 6341, Parent: 6334)
    - 0rK5XxDyLK New Fork (PID: 6228, Parent: 6225)
    - 0rK5XxDyLK New Fork (PID: 6230, Parent: 6225)
      - 0rK5XxDyLK New Fork (PID: 6233, Parent: 6230)
        - 0rK5XxDyLK New Fork (PID: 6329, Parent: 6233)
        - 0rK5XxDyLK New Fork (PID: 6331, Parent: 6233)
      - 0rK5XxDyLK New Fork (PID: 6235, Parent: 6230)
      - 0rK5XxDyLK New Fork (PID: 6238, Parent: 6230)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
0rK5XxDyLK	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x7c94:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x7d03:$s2: $Id: UPX • 0x7cb4:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

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

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

Data Obfuscation

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

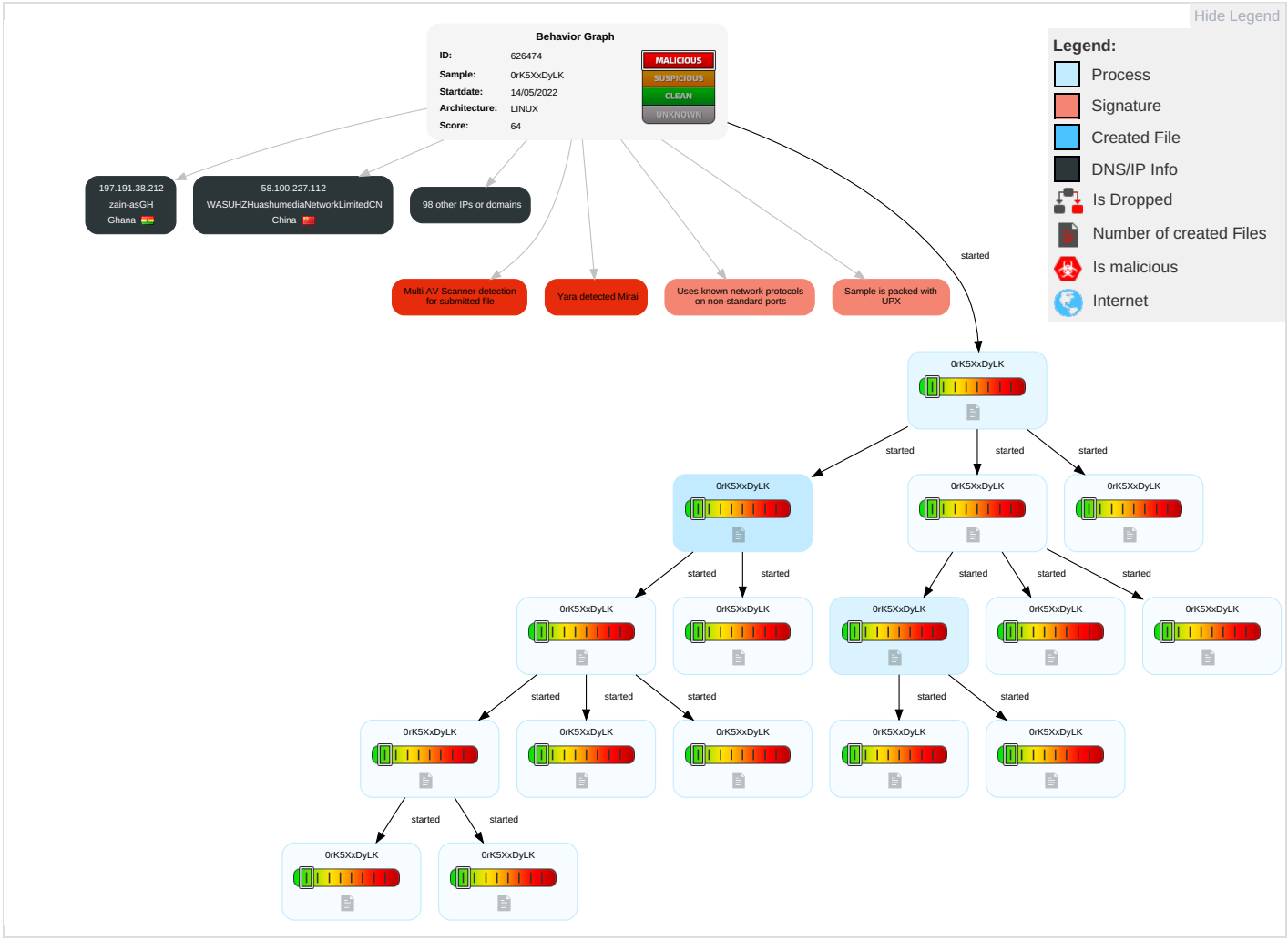
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Obfuscated Files or Information	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	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
0rK5XxDyLK	44%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

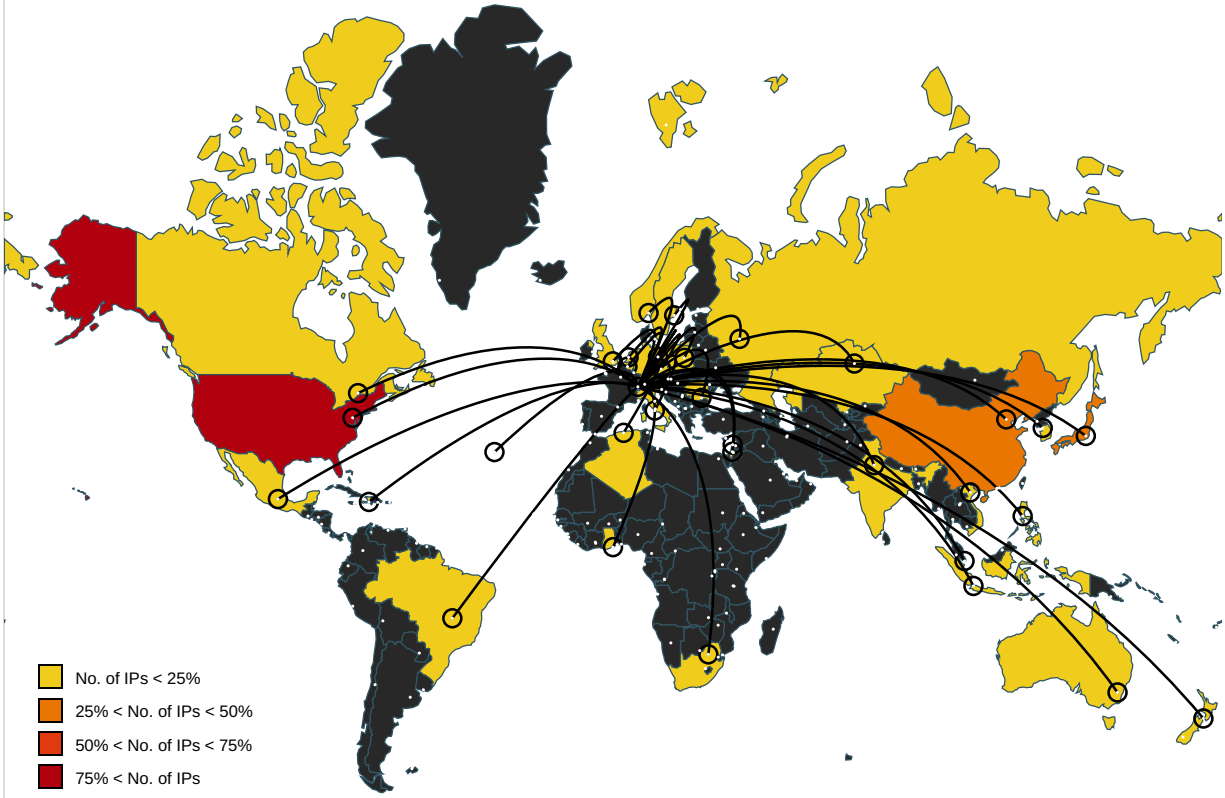
Domains and IPs

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
40.65.28.97	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
32.162.72.166	unknown	United States		2686	ATGS-MMD-ASUS	false
69.24.167.28	unknown	United States		12112	HICKORYTECHUS	false
163.4.93.231	unknown	United States		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
59.108.139.67	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
179.116.97.20	unknown	Brazil		26599	TELEFONICABRASILSABR	false
198.195.18.138	unknown	United States		292	ESNET-WESTUS	false
133.210.98.97	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
58.0.56.30	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
217.77.161.109	unknown	Czech Republic		16019	VODAFONE-CZ-ASCZ	false
188.88.104.40	unknown	Netherlands		31615	TMO-NL-ASNL	false
157.25.81.84	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
208.115.194.18	unknown	United States		46475	LIMESTONENETWORKSUS	false
165.12.32.162	unknown	Australia		9509	DESE-AS-APDepartmentofEducationSkillsandEmploymentAU	false
2.224.26.192	unknown	Italy		12874	FASTWEBIT	false
191.196.72.66	unknown	Brazil		26599	TELEFONICABRASILSABR	false
73.147.11.134	unknown	United States		7922	COMCAST-7922US	false
12.41.212.231	unknown	United States		7018	ATT-INTERNET4US	false
210.212.102.255	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
149.80.195.122	unknown	United States		188	SAIC-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
240.86.253.25	unknown	Reserved		unknown	unknown	false
202.163.232.221	unknown	Philippines		7629	EPLDT-AS-AP5FLVLocsinBldgPH	false
139.230.83.249	unknown	Australia		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
202.27.232.212	unknown	New Zealand		9303	KCCS-AS-APKCComputerServiceLtdNZ	false
119.242.183.16	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
135.61.219.174	unknown	United States		18676	AVAYAUS	false
208.130.249.102	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
4.69.47.217	unknown	United States		3356	LEVEL3US	false
88.101.33.114	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	false
197.191.38.212	unknown	Ghana		37140	zain-asGH	false
8.81.11.32	unknown	United States		3356	LEVEL3US	false
113.154.228.171	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
114.80.214.95	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
207.157.237.94	unknown	United States		54179	VCOEUS	false
158.110.4.166	unknown	Italy		137	ASGARRConsortiumGARREU	false
242.164.162.77	unknown	Reserved		unknown	unknown	false
81.244.107.99	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
58.129.119.241	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
42.115.58.166	unknown	Viet Nam		131178	KINGCORP-KHOpenNetISPCambodiaKH	false
221.107.68.221	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
115.71.204.176	unknown	Korea Republic of		45996	GNJ-AS-KRDAOUTECHNOLOGYKR	false
58.100.227.112	unknown	China		24139	WASUHZHuashumediaNetworkLimitedCN	false
197.141.89.118	unknown	Algeria		36891	ICOSNET-ASDZ	false
40.2.62.48	unknown	United States		4249	LILLY-ASUS	false
108.117.148.95	unknown	United States		10507	SPCSUS	false
41.145.34.47	unknown	South Africa		5713	SAIX-NETZA	false
189.246.1.186	unknown	Mexico		8151	UninetSAdeCVMX	false
67.254.165.68	unknown	United States		12271	TWC-12271-NYCUS	false
180.248.103.16	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
93.41.34.144	unknown	Italy		12874	FASTWEBIT	false
34.234.241.12	unknown	United States		14618	AMAZON-AESUS	false
32.226.239.62	unknown	United States		2686	ATGS-MMD-ASUS	false
95.76.74.181	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
243.235.191.223	unknown	Reserved		unknown	unknown	false
79.112.6.242	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
147.57.192.50	unknown	United States		4193	WA-STATE-GOVUS	false
58.94.183.140	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
62.90.145.99	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
142.23.219.7	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
107.145.98.212	unknown	United States		33363	BHN-33363US	false
156.55.64.11	unknown	United States		20746	ASN-IDCTNOOMINCIT	false
54.131.116.212	unknown	United States		14618	AMAZON-AESUS	false
91.232.101.156	unknown	Lebanon		57513	MIC1-ALFA-ASLB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
164.40.33.156	unknown	Kazakhstan		29355	KCELL-ASKZ	false
81.228.227.218	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
111.141.71.201	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
106.60.197.208	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
133.101.130.45	unknown	Japan		24254	KYOTO-SUKyotoSangyoUniversityJP	false
59.155.189.143	unknown	China		7474	OPTUSCOM-AS01-AUSingTelOptusPtyLtdAU	false
95.221.2.207	unknown	Russian Federation		12714	TI-ASMoscowRussiaRU	false
109.163.11.54	unknown	Norway		25400	TELIA-NORWAY-ASTeliaNorwayCoreNetworksNO	false
101.19.76.73	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
34.142.42.104	unknown	United States		2686	ATGS-MMD-ASUS	false
220.44.89.251	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
44.76.143.93	unknown	United States		7377	UCSDUS	false
249.208.147.139	unknown	Reserved		unknown	unknown	false
87.242.158.223	unknown	United Kingdom		12708	ONETEL-ASTalkTalkCommunicationsLimitedGB	false
20.80.57.39	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
248.133.183.13	unknown	Reserved		unknown	unknown	false
96.9.165.164	unknown	Singapore		134809	VIEWQWEST-AS-APViewQwestSdnBhdMY	false
202.165.68.144	unknown	Australia		18206	VPIS-APVADSManagedBusinessInternetServiceProviderMY	false
97.181.172.133	unknown	United States		6167	CELLCO-PARTUS	false
245.30.195.121	unknown	Reserved		unknown	unknown	false
101.192.59.230	unknown	China		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
200.2.159.234	unknown	Haiti		27759	ACCESSHAITISAHT	false
221.191.185.62	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
135.205.221.37	unknown	United States		6431	ATT-RESEARCHUS	false
92.239.100.223	unknown	United Kingdom		5089	NTLGB	false
251.32.142.47	unknown	Reserved		unknown	unknown	false
165.20.0.68	unknown	United States		37284	Aljeel-netLY	false
251.49.161.2	unknown	Reserved		unknown	unknown	false
53.115.60.76	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
68.210.193.185	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
37.8.121.95	unknown	Palestinian Territory Occupied		15975	HADARA-ASPS	false
208.217.74.34	unknown	United States		701	UUNETUS	false
126.122.128.205	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
85.43.244.34	unknown	Italy		3269	ASN-IBSNAZIT	false
65.26.228.220	unknown	United States		10796	TWC-10796-MIDWESTUS	false
9.146.150.56	unknown	United States		3356	LEVEL3US	false
143.248.120.130	unknown	Korea Republic of		1781	KAIST-DAEJEON-AS-KRKoreaAdvancedInstituteofScienceand	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, EABI4 version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.977316541944295
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	0rK5XxDyLK
File size:	48696
MD5:	b440222d627a07ae7733f9e706b88902
SHA1:	63be0315c844d0a25b61caa609255d9375306acf
SHA256:	eae51f23834e02da2ca18bbf28d2327726fd50c18b4e2c2f4ff451fca58a69aa
SHA512:	6004d2d776de254ea3e75a9107656bf61d7692885329f9826a6eaaa9a4a3c0a6237bb1d915721aff3b66aed4dbd7d6dfcc687d0eeae7147d98c3c398f396d180
SSDEEP:	768:nK7y1XGO1LCNgukEkvwtqPnH7u83nc0iFo9q3UELWt/iw+kvBGg6+fYtrBHs:P12O1LCNguovDPH7TcrPLWhiw+kvBGgl
TLSH:	702302532093BA03E03058FE45628CCDB51AA6BDB1BE7BA725494E194C35D93ECB18ED
File Content Preview:	.ELF.....(.....4.....4. ...(..... b.. b.. b.....Q.td.....OUPX!.....p...p.....h.....?.E.h;....#..$...o.....=..B.*...5N&"a..mk.c.....}<.....M.Q....[

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0xf1a0

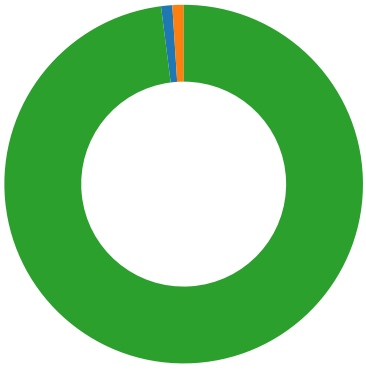
ELF header	
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x838d	0x838d	4.0415	0x5	R E	0x8000		
LOAD	0x6220	0x26220	0x26220	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



Total Packets: 99

- 23 (Telnet)
- 1312 undefined
- 443 (HTTPS)

TCP Packets

System Behavior

Analysis Process: 0rK5XxDyLK PID: **6225**, Parent PID: **6126**

General

Start time:	04:20:40
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	/tmp/0rK5XxDyLK
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: 0rK5XxDyLK PID: **6227**, Parent PID: **6225**

General

Start time:	04:20:41
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: 0rK5XxDyLK PID: **6333**, Parent PID: **6227**

General

Start time:	04:23:35
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6334**, Parent PID: **6227**

General

Start time:	04:23:35
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6337**, Parent PID: **6334**

General

Start time:	04:23:35
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6346**, Parent PID: **6337**

General

Start time:	04:23:40
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6347**, Parent PID: **6337**

General

Start time:	04:23:40
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK

Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6339**, Parent PID: **6334**

General

Start time:	04:23:35
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6341**, Parent PID: **6334**

General

Start time:	04:23:35
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6228**, Parent PID: **6225**

General

Start time:	04:20:41
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6230**, Parent PID: **6225**

General

Start time:	04:20:41
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6233**, Parent PID: **6230**

General

Start time:	04:20:41
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: 0rK5XxDyLK PID: **6329**, Parent PID: **6233**

General	
Start time:	04:23:35
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6331**, Parent PID: **6233**

General	
Start time:	04:23:35
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6235**, Parent PID: **6230**

General	
Start time:	04:20:41
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: 0rK5XxDyLK PID: **6238**, Parent PID: **6230**

General	
Start time:	04:20:41
Start date:	14/05/2022
Path:	/tmp/0rK5XxDyLK
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1