Overview

Zenbox Linux Verdict

22/100

Non Malicious

Report generated:	22/02/2023 09:47:30
Guest System:	Ubuntu 20.04 Ultimate

File Info

File name:	RvALAkYy
File type:	ELF 32-bit LSB executable, ARM, EABI5 version 1 (GNU/Linux), statically linked, no section header
File size:	5.6 MB
SHA256:	5987472321673fd54f2aebcc33ede6541897410df36a7f4a1bd984a2f724e772
SHA1:	3f519fafbc497b13783cb773c9efd7281ef83005
MD5:	2d690589a83ca0198189e37eb1dc4ebd
SHA512:	294cc0014264bbe4c137895a887bc8d8eab0a4ed710a8808bcb4045e051083b337bbafecddcc98119a381b650d9afabae6a40985e8d3421f47da087b11aa4f17
Entropy:	7.999966301460679
Submission path:	/tmp
SSDEEP:	98304:qudXvbrlSvD5eKLkQUFnDiEGY8OAi1/huFy8Gk0+sjqxV3SYhYa9pnghzlDkEoVA:qWbgLoOKiiX8fxz3SYhYabgaDk7+Xv
Preview:	.ELF.....(.....vZ.4.....4. ...(.....c.Y.c.Y.....[...[.....h.....Q.td.....,9..UPX!.....p...p.....r.....?.E.h;.....#..$.....[*...*..%4k.X.S.V`\.....V...wh.....c...S...

Indicators

System Summary (2)

1.0	Sample contains only a LOAD segment without any section mappings
0.0	Classification label

Data Obfuscation (1)

2.0	Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection (1)

1.0	ELF contains segments with high entropy indicating compressed/encrypted content

Malware Analysis System Evasion (2)

1.0	Uses the "uname" system call to query kernel version information (possible evasion)
0.0	May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)

Networking (3)

1.0	Tries to connect to HTTP servers, but all servers are down (expired dropper behavior)
0.0	Connects to IPs without corresponding DNS lookups
0.0	URLs found in memory or binary data

Analysis Advice (5)

0.0	Static ELF header machine description suggests that the sample might not execute correctly on this machine.
0.0	Exit code information suggests that the sample terminated abnormally, try to lookup the sample's target architecture.
0.0	All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.
0.0	Non-zero exit code suggests an error during the execution. Lookup the error code for hints.
0.0	Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

Mitre Attack

Defense Evasion

- T1027 Obfuscated Files or Information confidence: high

Discovery

- T1518.001 Security Software Discovery confidence: medium

Network Info

URL Info (1)

http://upx.sf.net from-memory reputation: high from: RvALAkYy

IP Info (1)

IP	Country
169.254.169.254	Reserved

Processes Extra Info

Process: python3.8 PID: **5015** Parent PID: **5004**

None

Process: RvALAkYy PID: **5002** Parent PID: **4909**

None

Screenshots

Not found.