Overview

Zenbox Linux Verdict

21/100

Non Malicious

Report generated:	17/07/2023 13:14:40
Guest System:	Ubuntu 20.04 Ultimate

File Info

File name:	1hkUuKXeNa
File type:	ELF 64-bit LSB executable, ARM aarch64, version 1 (SYSV), statically linked, no section header
File size:	5.74 MB
SHA256:	a62e88db6c56c69edb95b5032334132e50be1a8feba4c5bb7e39f5d55ecd69e3
SHA1:	e18cf64747c29658c992823c1c0e2642333eda6a
MD5:	f7de30df91b2a6745336337665e3ae49
SHA512:	aadcd3b4b9ef5c315924c36b6572ca17a2aa80830b5eaf6a80f2f5b29efaa82cb78b56d54ba1a11fa7f17240d7768f3b18d6ba3e9317600620bb2a6af240adca
Entropy:	7.999970862384102
Submission path:	/tmp
SSDEEP:	98304:x/gJrnSYg9pzvLvwN7i51odZqpI/rPpEfuVjxbjDRXN6t7aqwXz4HlbYH+YGFhN7:SJrnivLj1UqpArPCu55jDRcozQIGvdGe
Preview:	.ELF.....\.....@.....@.8...@.....P.[.....P.[.....].....].....0.4.....Q.td.....U.tUPX!t..*.....

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 (1)

0.0	URLs found in memory or binary data

Analysis Advice (2)

0.0	Static ELF header machine description suggests that the sample might not execute correctly on this machine.
0.0	Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

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: 1hkUuKXeNa

Processes Extra Info

Process: 1hkUuKXeNa PID: **3196** Parent PID: **3113**

None

Screenshots

Not found.