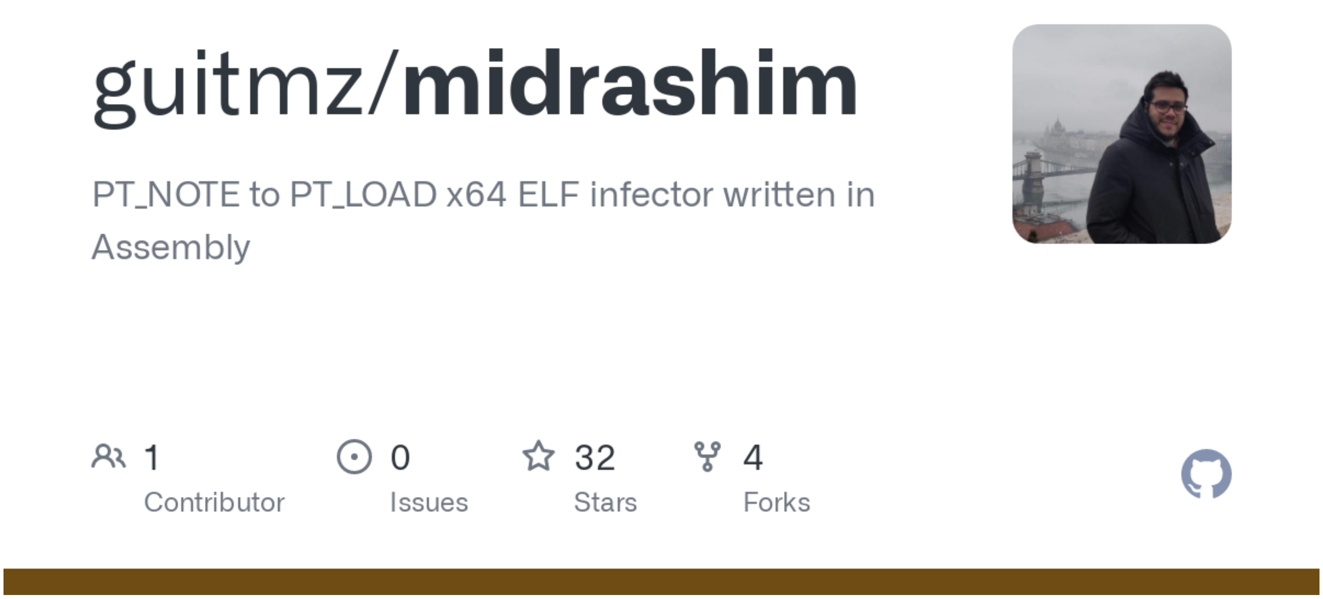
guitmz/midrashim: PT_NOTE to PT_LOAD x64 ELF infector written in Assembly

github.com/guitmz/midrashim

guitmz



guitmz/**midrashim**

PT_NOTE to PT_LOAD x64 ELF infector written in Assembly

1 Contributor

0 Issues

32 Stars

4 Forks

Linux.Midrashim

This is my first x64 ELF infector written in full Assembly. It contains a non destructive payload and will infect other ELF (PIE is also supported) on current directory only and not recursively. It uses `PT_NOTE to PT_LOAD` infection technique.

Build

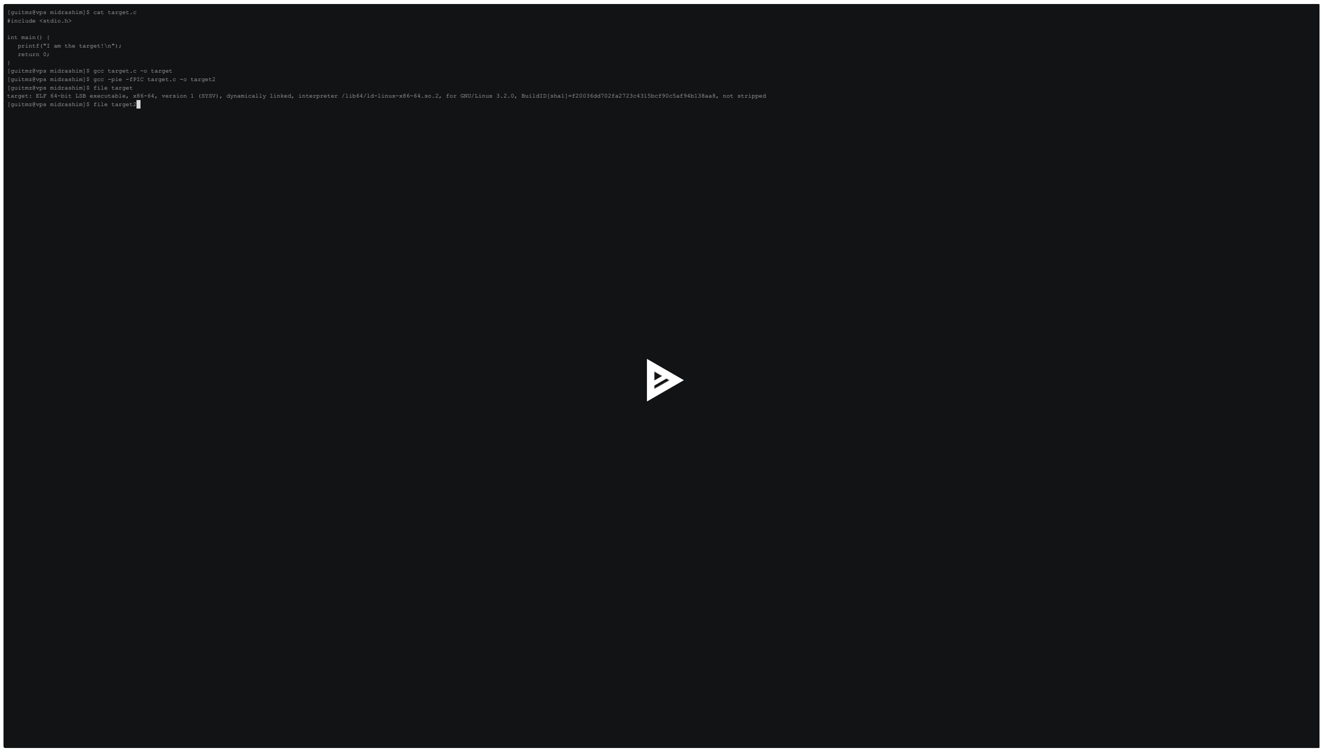
Assemble it with FASM x64.

```
$ fasm Linux.Midrashim.asm
flat assembler  version 1.73.25  (16384 kilobytes memory, x64)
3 passes, 2631 bytes.

$ file Linux.Midrashim
ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, stripped

$ sha256sum Linux.Midrashim
8f1a835ad6f5c58b397109e28409ec0556d6d374085361c6525f73d5ca5785eb  Linux.Midrashim
```

Demo



```
[guitmz@vps midrashim]$ cat target.c
#include <stdio.h>

int main() {
   printf("I am the target!\n");
   return 0;
}
[guitmz@vps midrashim]$ gcc target.c -o target
[guitmz@vps midrashim]$ gcc -pie -fPIC target.c -o target2
[guitmz@vps midrashim]$ file target
target: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=f20036dd702fa2723c4315bcf90c5af94b138aa8, not stripped
[guitmz@vps midrashim]$ file target2
```

References: