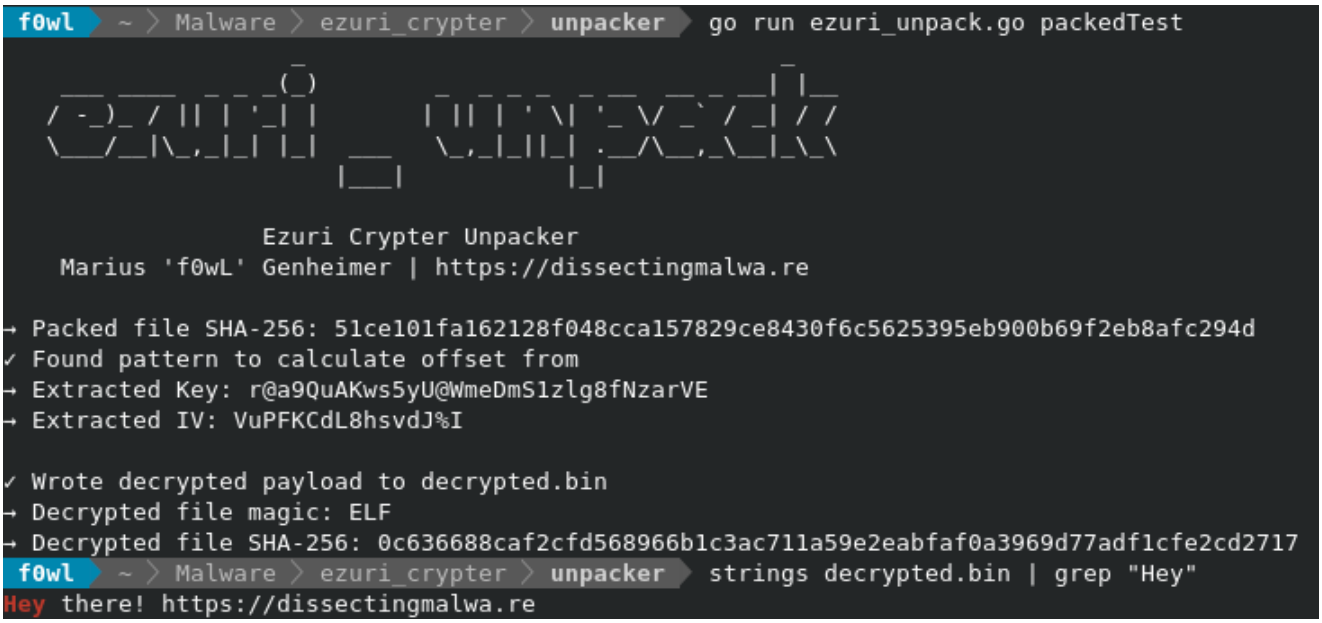
ezuri_unpack

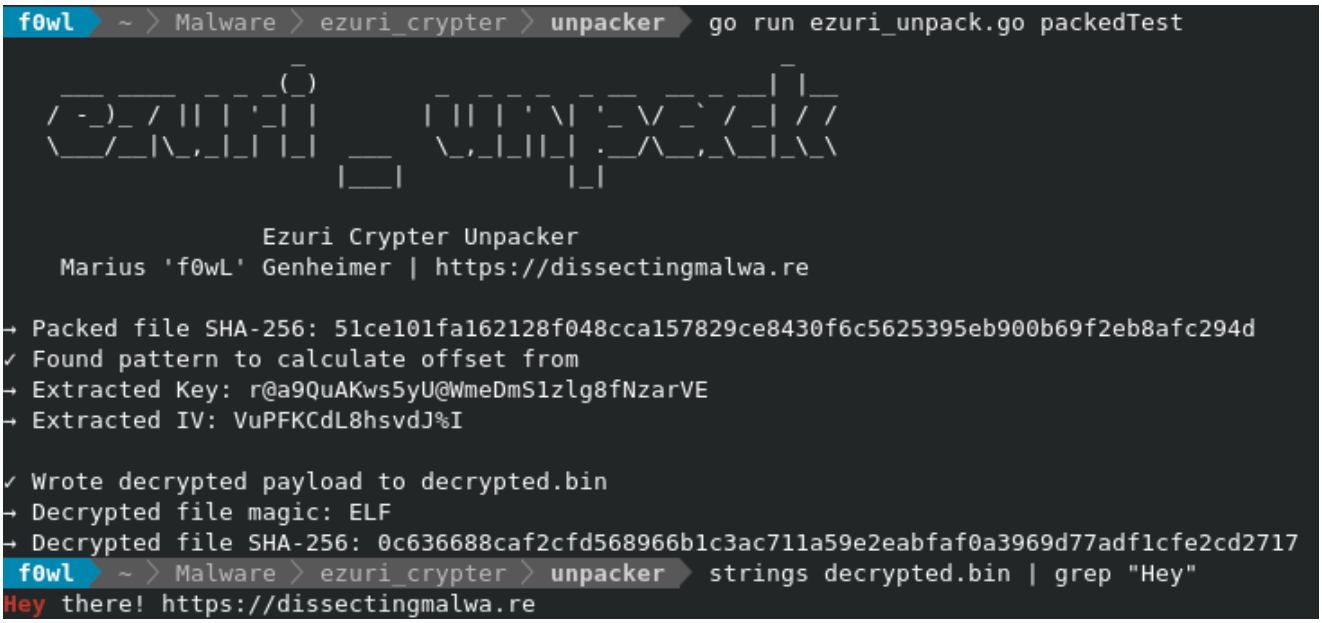
github.com/f0wl/ezuri_unpack

f0wl



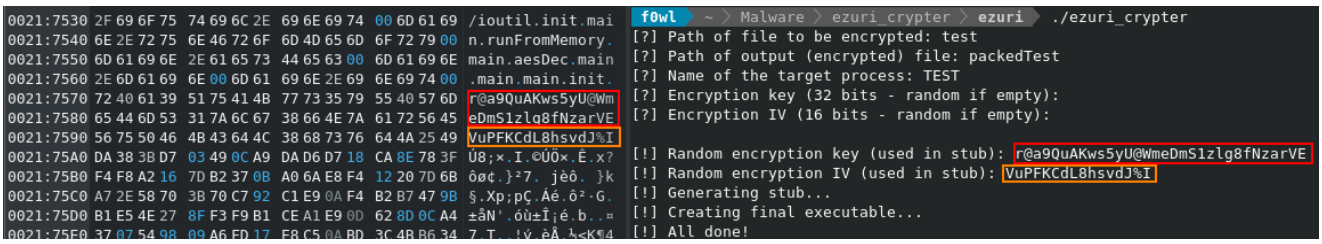
go report A+

A simple unpacking script for the Ezuri ELF Crypter. Based on the analysis done by Ofer Caspi and Fernando Martinez of AT&T Alien Labs: https://cybersecurity.att.com/blogs/labs-research/malware-using-new-ezuri-memory-loader



How does it work?

The payload is encrypted with AES CFB and will be decrypted and run via memfd_create by the stub. Key and IV are stored in the binary.



Testing the script

1. Build the test payload `gcc test.c -o test`
2. Build and run guitmz/ezuri
3. To unpack it again: `go run ezuri_unpack.go packed.bin`

I also tested it with the packed Linux.Cephei sample mentioned in the report. Link to Virustotal