GitHub - f0wl/REconfig-linux: Configuration Extractor for the Linux variant of REvil Ransomware

By f0wl

Archived: 2026-04-05 21:28:03 UTC

go report A+

REconfig-linux is a configuration extractor for the Linux variant of REvil Ransomware. It is capable of extracting the json config from the ELF file and decoding the ransomnote within it. By default the script will write the results to files in the current working directory, but you can also choose to print the config to stdout only by using the `-print` flag.

My Yara rule for the REvil Linux Ransomware can be found here.

A writeup by AT&T Alien Labs about this Ransomware variant can be found here.

Usage

```
go run reconfig-linux.go [-print] path/to/sample.elf
```

Screenshots

Non-verbose Mode

Verbose Mode

Configuration contents

The table below shows the keys used in the JSON configuration of REvil Linux Ransomware.

Key	Value / Purpose
pk	Base64 encoded Public Key
pid	Affiliate identifier (BCrypt Hash)
sub	Campaign identifier
dbg	Debug / Development Mode
nbody	Base64 encoded Ransomnote
nname	Filename of the Ransomnote
rdmcnt	Currently unknown integer (RandomCount?)
ext	File Extension (5 characters)

Testing

This configuration extractor has been tested successfully with the following samples:

SHA-256	Sample
ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4	Malshare
3d375d0ead2b63168de86ca2649360d9dcff75b3e0ffa2cf1e50816ec92b3b7d	Malshare
796800face046765bd79f267c56a6c93ee2800b76d7f38ad96e5acb92599fcd4	Malshare
d6762eff16452434ac1acc127f082906cc1ae5b0ff026d0d4fe725711db47763	Malshare

If you encounter an error with REconfig-linux please file a bug report via an issue. Contributions are always welcome :)
