REconfig-linux

github.com/f0wl/REconfig-linux

f0wl

f0wl/REconfig-linux

Configuration Extractor for the Linux variant of REvil Ransomware

1 Contributor | 0 Issues | 7 Stars | 2 Forks

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

```
f0wl@mw-Lab:~/code/REconfig-linux$ go run reconfig-linux.go ~/Downloads/revil-395249d3e6dae1caff6b5b2e1f75bacd


 ####  ##### #   #  ###  #   #   #   #   # #####     ##### #   # #   # #   # #   #
 #   # #     #   # #   # #   #  ###  #  ## #   #         # #   # ##  # #   # # # #
 ####  ####   #### #   # ##### # # # # # # # #     ###  # # # # ##### #   # # # #
 #     #         # #   # #   #  ###  ##  # #         # # ## # #   # #   #   # # #
 #     #####     #  ###  #   #   #   #   # #        #   # #   # #   # #     #####
 REconfig-linux

 REvil Linux Ransomware Configuration Extractor
 Marius 'f0wL' Genheimer | https://dissectingmalwa.re

→ Sample SHA-256: ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4
✓ Found the json config string.

✓ Wrote extracted config to 'config-395249d3e6dae1caff6b5b2e1f75bacd.json'
✓ Wrote decoded ransomnote to 'ransomnote-395249d3e6dae1caff6b5b2e1f75bacd.txt'
```

Verbose Mode

```
f0wl@mw-Lab:~/code/REconfig-linux$ go run reconfig-linux.go -print ~/Downloads/revil-395249d3e6dae1caff6b5b2e1f75bacd


 ####  ##### #   #  ###  #   #   #   #   # #####     ##### #   # #   # #   # #   #
 #   # #     #   # #   # #   #  ###  #  ## #   #         # #   # ##  # #   # # # #
 ####  ####   #### #   # ##### # # # # # # # #     ###  # # # # ##### #   # # # #
 #     #         # #   # #   #  ###  ##  # #         # # ## # #   # #   #   # # #
 #     #####     #  ###  #   #   #   #   # #        #   # #   # #   # #     #####
 REconfig-linux

 REvil Linux Ransomware Configuration Extractor
 Marius 'f0wL' Genheimer | https://dissectingmalwa.re

→ Sample SHA-256: ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4
✓ Found the json config string.

✓ Beautified JSON config:

{
  "pk": "r58UPwgbaRk5py762WpY/rEsl1jd936THXwqUwID/iM=",
  "pid": "$2a$12$V3e/gZmP0hFlQhnJLAyOM.Fsb56ksfw0p42oLlNwf2Jou485El04K",
  "sub": "7987",
  "dbg": false,
  "et": 0,
  "nbody": "LS0tPT09IFdlbGNvbWUuIEFnYWluLiA9PT0tLS0KClsrXSBXaGF0cyBIYXBwZW4/IFsrXQoKWW91ciBmaWxlcyBhcmUgZW5jcnlwdGVkLCBhbmQgY3VycmVudGx5IHVuYXZhaWxhYmxlLiBZb3UgY2FuIGNoZWNrIGl0OiBhbGwgZmlsZXMgb24geW91ciB
nV0IHlvdSBuZWVkIHRvIGZvbGxvdyBvdXIgaW5zdHJ1Y3Rpb25zLiBPdGhlcndpc2UsIHlvdSBjYW50IHJldHVybiB5b3VyIGRhdGEgKE5FVkVSKS4KClsrXSBXaGF0IGd1YXJhbnRlZXM/IFsrXQoKSXRzIGp1c3QgYSBidXNpbmVzcy4gV2UgYWJzb2x1dGVseSBkbyBu
5kIGxpYWJpbGl0aWVzIC0gbm9ib2R5IHdpbGwgbm90IGNvb3BlcmF0ZSB3aXRoIHVzLiBJdHMgbm90IGluIG91ciBpbnRlcmVzdHMuClRvIGNoZWNrIHRoZSBhYmlsaXR5IG9mIHJldHVybmluZyBmaWxlcywgWW91IHNob3VsZCBnbyB0byBvdXIgd2Vic2l0ZS4gVGhlc
gd2l0aCBvdXIgc2VydmljZSAtIGZvciB1cywgaXRzIGRvZXMgbm90IG1hdHRlci4gQnV0IHlvdSB3aWxsIGxvc2UgeW91ciB0aW1lIGFuZCBkYXRhLCBjYXVzZSBqdXN0IHdlIGhhdmUgdGhlIHByaXZhdGUga2V5LiBJbiBwcmFjdGlzZSAtIHRpbWUgaXMgbXVjaCBtb3
IFtSZWNvbW1lbmRlZF0gVXNpbmcgYSBUT1IgYnJvd3NlciEKICBhKSBEb3dubG9hZCBhbmQgaW5zdGFsbCBUT1IgYnJvd3NlciBmcm9tIHRoaXMgc2l0ZTogaHR0cHM6Ly90b3Jwcm9qZWN0Lm9yZy8KICBiKSBPcGVuIG91ciB3ZWJzaXRlOiBodHRwOi8vYXBsZWJ6dTQ
XIgY291bnRyeSwgdHJ5IHRvIHVzZSBWUE4hIEJ1dCB5b3UgY2FuIHVzZSBvdXIgc2Vjb25kYXJ5IHdlYnNpdGUuIEZvciB0aGlzOgogIGEpIE9wZW4geW91ciBhbnkgYnJvd3NlciAoQ2hyb21lLCBGaXJlZm94LCBPcGVyYSwgSUUsIEVkZ2UpCiAgYikgT3BlbiBvdXIg
wgdGhhdHMgd2h5IGZpcnN0IHZhcmlhbnQgbXVjaCBiZXR0ZXIgYW5kIG1vcmUgYXZhaWxhYmxlLgoKV2hlbiB5b3Ugb3BlbiBvdXIgd2Vic2l0ZSwgcHV0IHRoZSBmb2xsb3dpbmcgZGF0YSBpbiB0aGUgaW5wdXQgZm9ybToKS2V5OgoKCntLRVl9CgoKLS0tLS0tLS0tL
EQU5HRVIgISEhCkRPT1QgdHJ5IHRvIGNoYW5nZSBmaWxlcyBieSB5b3Vyc2VsZiwgRE9OVCB1c2UgYW55IHRoaXJkIHBhcnR5IHNvZnR3YXJlIGZvciByZXN0b3JpbmcgeW91ciBkYXRhIG9yIGFudGl2aXJ1cyBzb2x1dGlvbnMgLSBpdHMgbWF5IGVudGFpbCBkYW1nZS
aW4geW91ciBpbnRlcmVzdHMgdG8gZ2V0IHlvdXIgZmlsZXMgYmFjay4gRnJvbSBvdXIgc2lkZSwgd2UgKHRoZSBiZXN0IHNwZWNpYWxpc3RzKSBtYWtlIGV2ZXJ5dGhpbmcgZm9yIHJlc3RvcmluZywgYnV0IHBsZWFzZSBzaG91bGQgbm90IGludGVyZmVyZS4KISEhICE
  "nname": "{EXT}-readme.txt",
  "rdmcnt": 0,
  "ext": ".rhkrc"
}

✓ Extracted and base64 decoded Ransomnote:

---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension {EXT}.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.
```

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

Key	Value / Purpose
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 :)