

LINUX.ENCODER.1

The following steps and decryption tools have been designed for infections of the Linux.Encoder.1 ransomware.

First and foremost, download the following tool:

http://labs.bitdefender.com/wp-content/plugins/download-monitor/download.php?id=Decrypter_0-1.3.zip and unzip it in a location of your convenience. For this to work, you have NOT to delete any files.

Now carefully follow the following steps:

1. Run `sort_files.sh / > sorted.list` to obtain a list of the encrypted files sorted by encryption time * Note: run `sort_files.sh /path/to/vm/partition` if the data was on a vm
2. Most importantly, obtain the first file in that list, be it `X.encrypted` (`head -1 sorted.list`)
3. Find the seed using `./decrypter.py -f /path/to/X.encrypted`
4. If you have the seed you can safely decrypt the files. Run `./decrypter.py -s <seed> -l <sorted.list> -e <error.list>`
5. Check decryption was correct and clean the ".encrypted" files on your own.* Note: Unfortunately, the ransomware does not preserve ownership (user/group), some things might get broken because of this.
6. If you have files still encrypted they will appear in the file you provided as `<error.list>`. You will need to redo steps 2) -> 5) using the `<error.list>` until no more files.

Example run:

```
# bash decrypter/sort_files.sh > sorted_list
```

```
# head -1 sorted_list
```

```
1447255617.000000000000 ./d/home/user/.bash_logout.encrypted
```

```
python decrypter/decrypter.py -f ./d/home/user/.bash_logout.encrypted
```

```
[*] Seed: 1447255617
```

```
python decrypter/decrypter.py -s 1447255617 -l sorted_list -e error_list
```

```
.....
```

```
[FAILED] ./d/usr/share/doc/mlocate/README.encrypted
```

```
[OK] ./d/usr/share/doc/mlocate/TOD0.Debian.encrypted
```

```
[OK] ./d/usr/share/doc/readline-common/changelog.Debian.gz.encrypted
```

```
[FAILED] ./d/usr/share/doc/readline-common/copyright.encrypted
```

```
[FAILED] ./d/usr/share/doc/readline-common/inputrc.arrows.encrypted
```

```
[OK] ./d/usr/share/java/libintl.jar.encrypted
[*] recovered 7572 files
[*] failed to recover (probably bad seed) 9424 files
[*] 36 corrupted (probably truncated) files
```

5) => 2) (because 9424 files still encrypted)

```
# head -1 error_list
1447255625.0000000000 ./d/home/README_FOR_DECRYPT.txt.encrypted
```

```
# python decrypter/decrypter.py -f ./d/home/README_FOR_DECRYPT.txt.encrypted
[*] Seed: 1447255625
```

```
# python decrypter/decrypter.py -s 1447255625 -l error_list -e error_list2
```

```
.....
[FAILED] ./d/usr/share/doc/mlocate/changelog.gz.encrypted
[OK] ./d/usr/share/doc/mlocate/NEWS.gz.encrypted
[FAILED] ./d/usr/share/doc/mlocate/README.encrypted
[FAILED] ./d/usr/share/doc/readline-common/copyright.encrypted
[OK] ./d/usr/share/doc/readline-common/inputrc.arrows.encrypted
[*] recovered 5000 files
[*] failed to recover (probably bad seed) 4424 files
[*] 0 corrupted (probably truncated) files
```

5) => 2) (because 4424 files still encrypted)

```
# head -1 error_list2
1447255634.0000000000 ./d/root/test/size_10028.encrypted
```

```
# python decrypter/decrypter.py -f ./d/root/test/size_10028.encrypted
[*] Seed: 1447255634
```

```
# python decrypter/decrypter.py -s 1447255634 -l error_list2 -e error_list3
```

```
.....
[OK] ./d/usr/share/doc/libsqlite3-0/changelog.html.gz.encrypted
[OK] ./d/usr/share/doc/linux-image-2.6.32-5-amd64/changelog.Debian.gz.encrypted
[OK] ./d/usr/share/doc/locales-all/copyright.encrypted
[OK] ./d/usr/share/doc/lsb-base/copyright.encrypted
[OK] ./d/usr/share/doc/mlocate/AUTHORS.encrypted
```



[OK] ./d/usr/share/doc/mlocate/changelog.gz.encrypted
[OK] ./d/usr/share/doc/mlocate/README.encrypted
[OK] ./d/usr/share/doc/readline-common/copyright.encrypted
[*] recovered 4424 files
[*] failed to recover (probably bad seed) 0 files
[*] 0 corrupted (probably truncated) files

DONE!