Princess Locker decryptor

By Posted on

Published: 2016-11-17 · Archived: 2026-04-05 14:04:37 UTC

[UPDATE: 19th March 2018] – ***I keep getting e-mails from people asking me why my decryptor doesn't work. Please understand, this is an obsolete tool, it was written in 2016 for the FIRST VERSION of Princess Locker. The current version is improved and no longer decryptable.***

[UPDATE: 28th Nov 2016] – ***unfortunately, recently a new variant appeared, that fixed the bug which allowed me crack this ransomware. If generating the key takes more than few minutes, it probably means that you has been infected by the new version of Princess. I am sorry, but I am not capable of helping in such case.***

If you are a researcher curious how I cracked it, you can see the decryptor's source code:
https://github.com/hasherezade/decryptors_archive/tree/master/princesslocker_decrypt

---

The presented decryptor works ONLY for the first version of Princess Locker ransomware (tested on sample: 14c32fd132942a0f3cc579adbd8a51ed):

Ransom note example:

In this thread you will find all the information and updates about the progress.

Currently I prepared a set of two EXPERIMENTAL tools: **keygen** and **decryptor**.

You can download the full package from here.

See it in action on YouTube: https://www.youtube.com/watch?v=Ted84CoOPvg

Use the keygen first in order to find your key. If this operation went successful, you can use decryptor to decrypt your other files.

The tools are protected with PE-Lock (special thanks to Bartosz Wójcik).

HOW TO USE

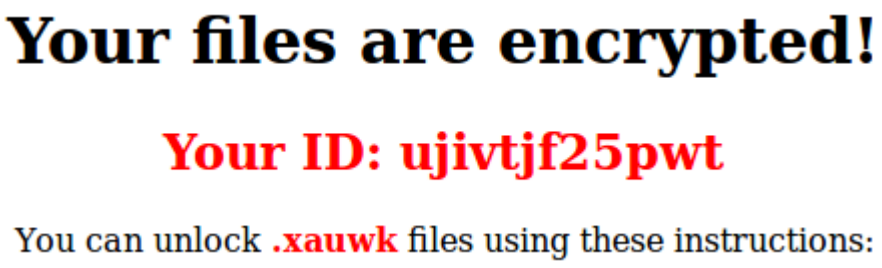
In order to use the keygen you must find one file, that you can provide in both forms: unencrypted and encrypted. You also need to supply the added extension. It is beneficial (but not required) to supply the unique ID from your ransom note.
Usage:

```
PrincessKeygen.exe [encrypted file] [original file] [added extension] [*unique id]
```

* – optional parameter

Example:

Read the data from your ransom note:



And supply them to the keygen:

```
PrincessKeygen.exe "square1.bmp.xauwk" "square1.bmp" xauwk ujivtjf25pwt
```

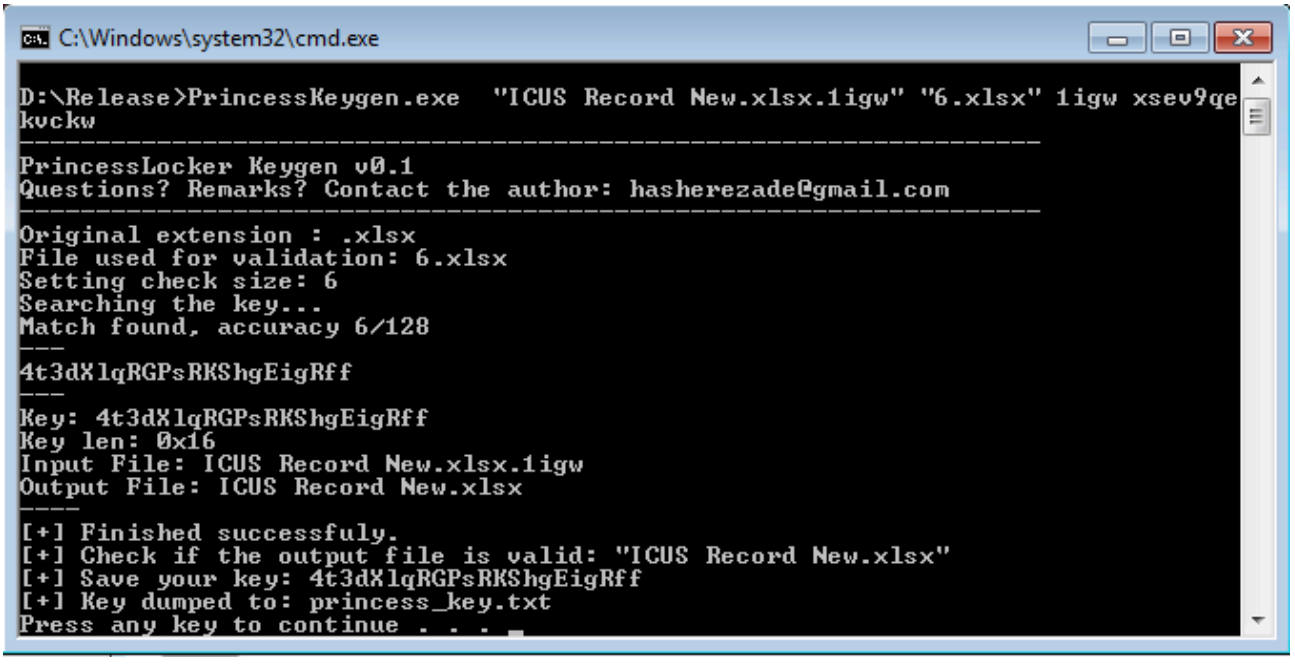
What if you don't have any original file?

In case if you don't have the original copy of any of your encrypted files, you can use an encrypted file of one of the following formats:

doc, png, gif, pdf, docx, xlsx, ppt, xls

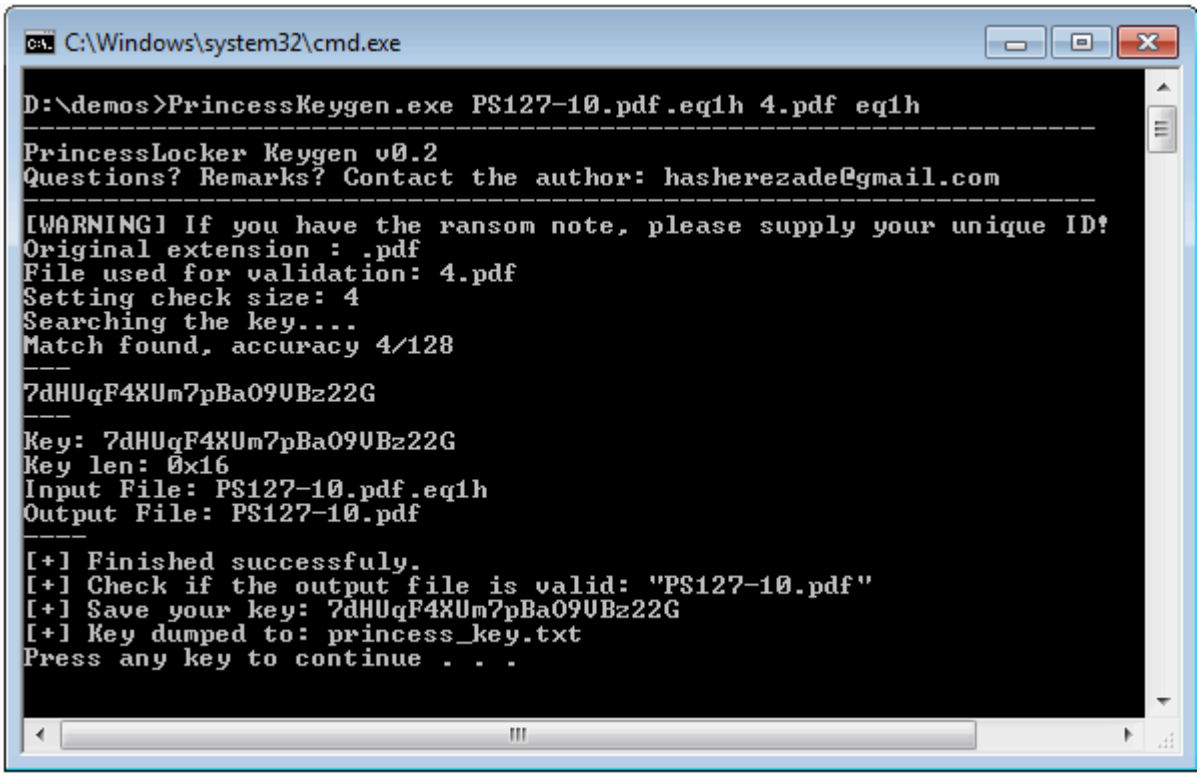
Then, instead of the original file, supply the preprepared header – you can find the set here. However, this method may, in some rare cases, produce invalid results – so, supplying the original file is recommended.

Example:



What if you don't have the ransom note?

It's OK. Just supply the extension – but be warned that cracking may take a bit longer.



Check if your output file is valid. If so, save the key and use it to decrypt rest of your files, with the help of PrincessDecryptor.

Usage:

```
PrincessDecryptor.exe [key] [ransom extension] [*file/directory]
```

* – optional parameter – default is current directory

About hasherezade

Programmer and researcher, interested in InfoSec.

Source: https://hshrzd.wordpress.com/2016/11/17/princess-locker-decryptor/