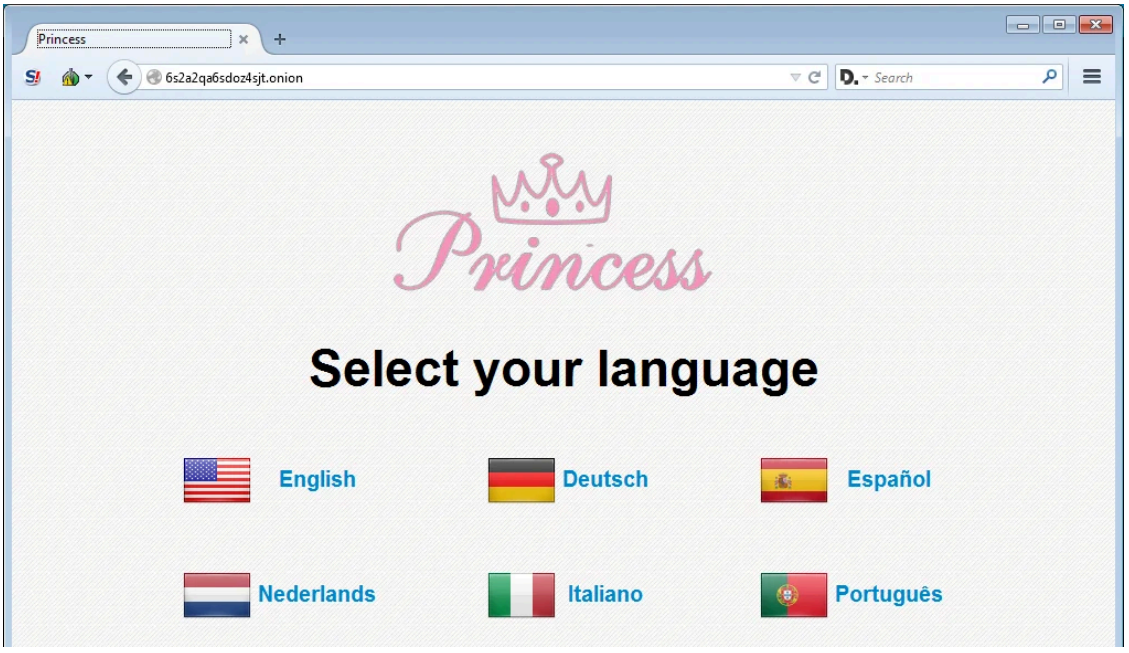
Introducing Her Royal Highness, the Princess Locker Ransomware

By Lawrence Abrams

Published: 2016-09-28 · Archived: 2026-04-05 14:04:42 UTC

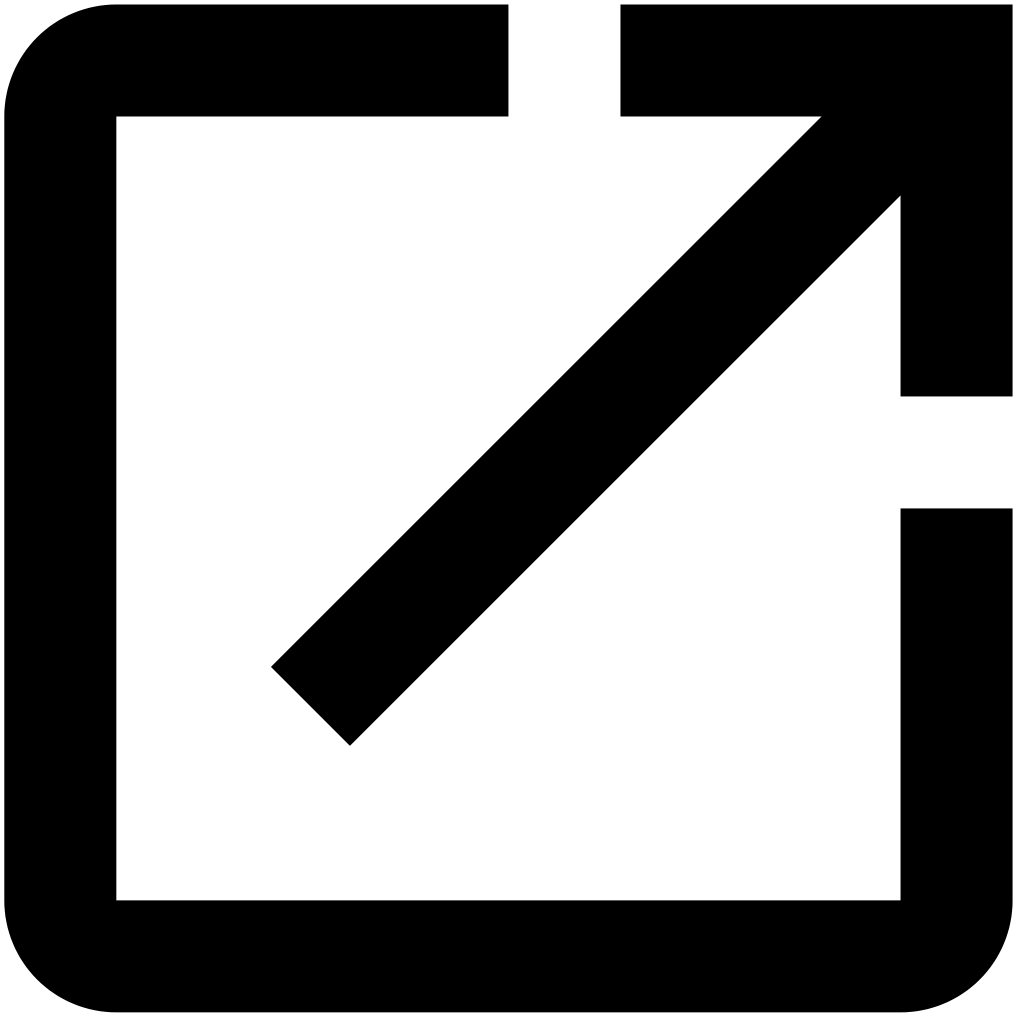


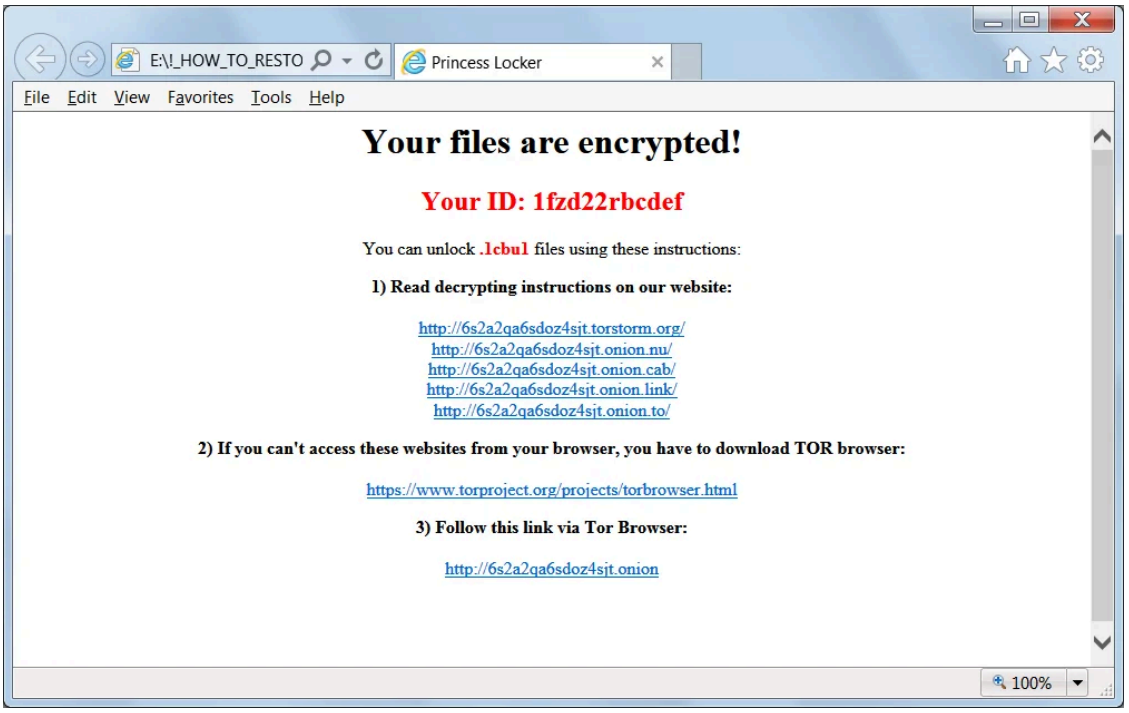
Today we bring you Princess Locker; the ransomware only royalty could love. First discovered by SenseCy on darkweb forums and later by Michael Gillespie through his ID-Ransomware platform, Princess Locker encrypts a victim's data and then demands a hefty ransom amount of 3 bitcoins, or approximately $1,800 USD, to purchase a decryptor. If payment is not made in the specified timeframe, then the ransom payment doubles to 6 bitcoins

Not much is known about Princess Locker other than having seen a few encrypted files and ransom notes uploaded to ID-Ransomware. From what has been gather gathered, when a person is infected, the ransomware will encrypt the victim's files and then append a random extension to encrypted files and a unique ID is created for the victim. This ID, extension, and encryption is then most likely sent up to the ransomware's Command & Control server.

Ransom notes are also created and displayed, which are named **!_HOW_TO_RESTORE_[extension].TXT** and **!_HOW_TO_RESTORE_[extension].html.**


DIE LINKE.
0:00

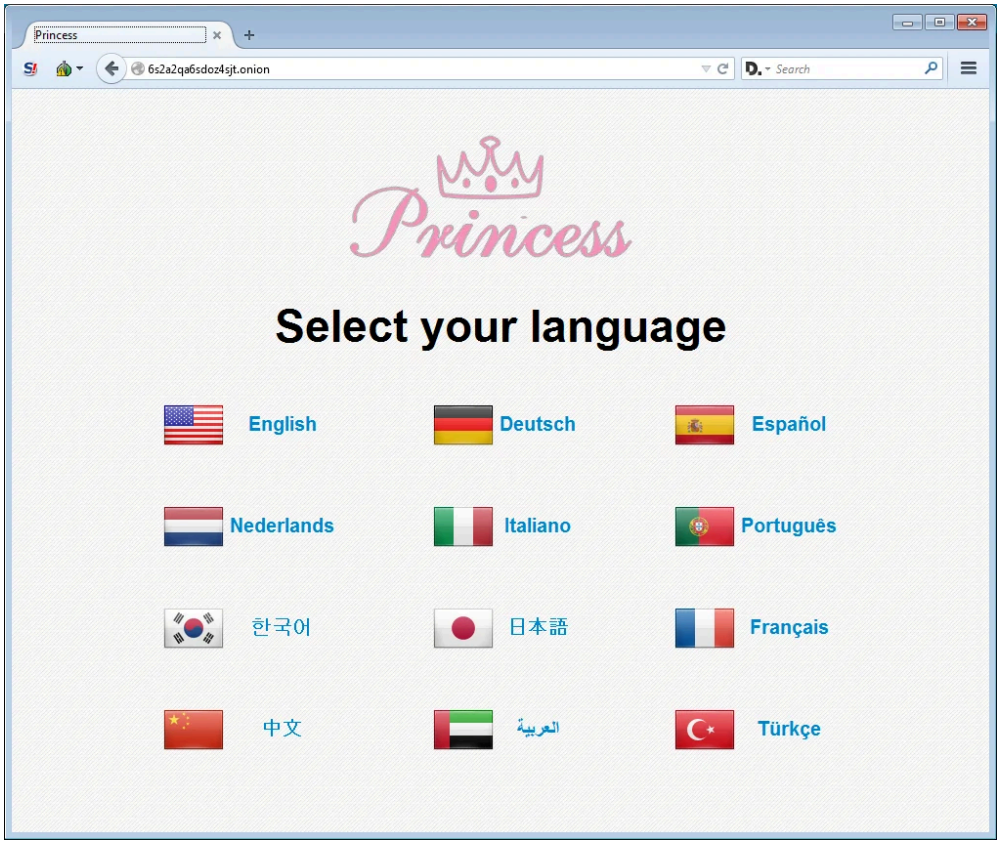




These ransom notes contain the victim's ID and links to the TOR payment sites where a victim can login to see payment information.

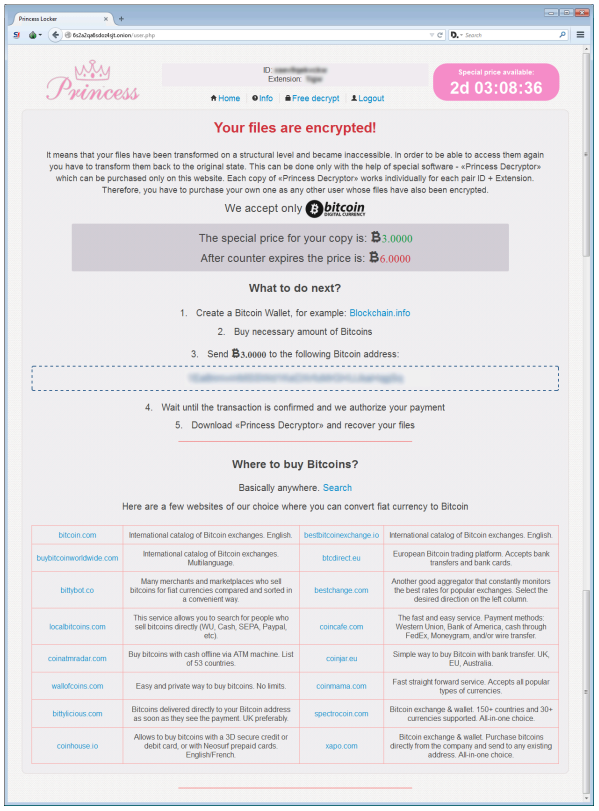
The Princess Locker Payment Site

The Princess Locker payment site is your standard ransomware site with no special features. When victim's access the Princess Locker payment site they will be greeted with a page asking them to select a language that looks almost identical to Cerber's language selection page.



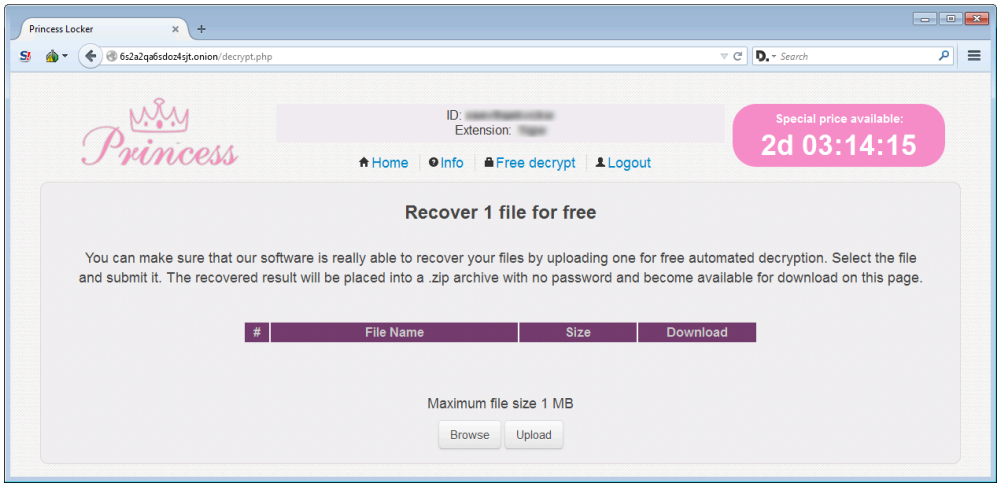
Language Selection Screen

They will then be presented with a login prompt where they need to enter the victim ID provided in the ransom note. Once logged in they will see the main payment site, which contains information such as the ransom amount, the bitcoin address to send payment to, and the answers to common questions.



Princess Locker Payment Site

The payment site also provides the ability to decrypt 1 file free. Unfortunately, since we do not have a sample of the ransomware, and I didn't want to waste a victim's free decryption, I do not know if this feature works or not.



Free File Decryption

The one item that is missing from the payment site is a support page that victim's can use to contact the malware developers. If this ransomware goes into wider distribution, I would not be surprised to see one added.

We are still actively looking for a sample of this ransomware, so if one is encountered, please upload it here.
