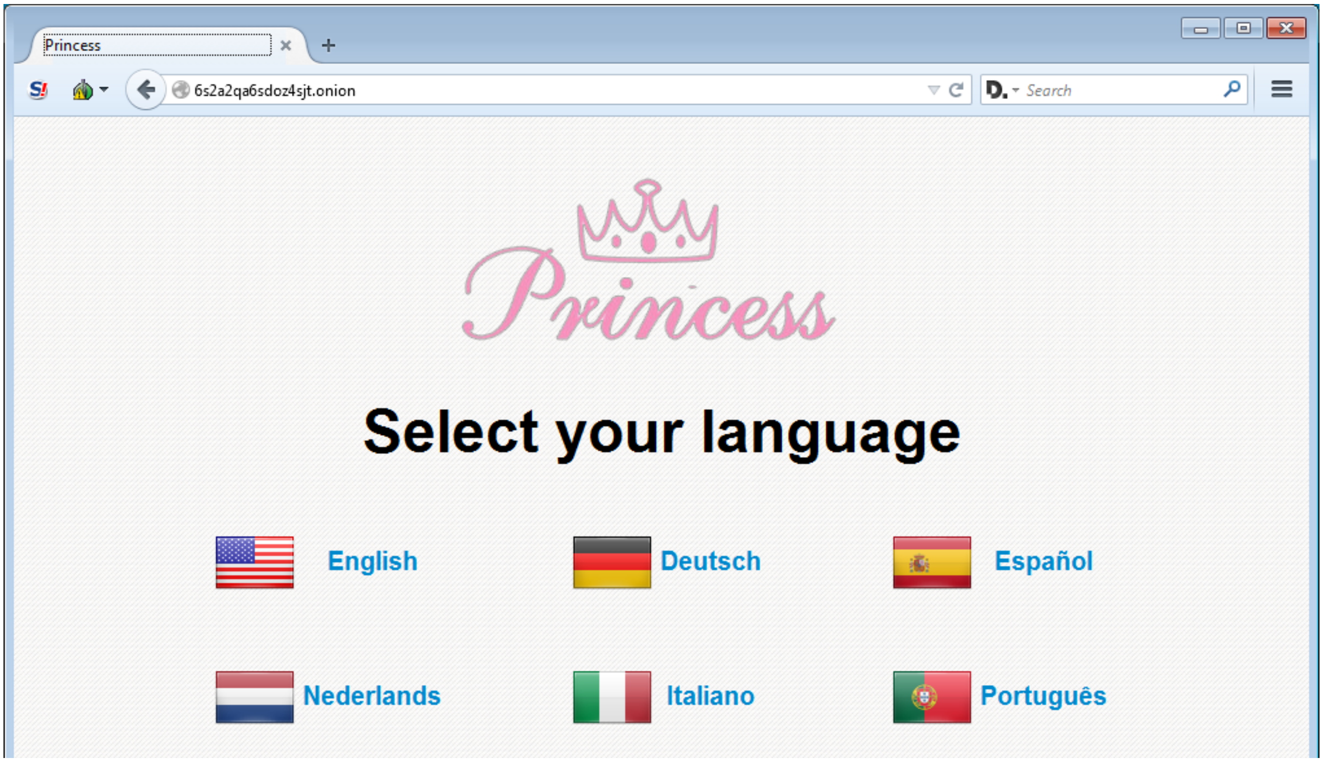
Introducing Her Royal Highness, the Princess Locker Ransomware

bleepingcomputer.com/news/security/introducing-her-royal-highness-the-princess-locker-ransomware

By
Lawrence Abrams

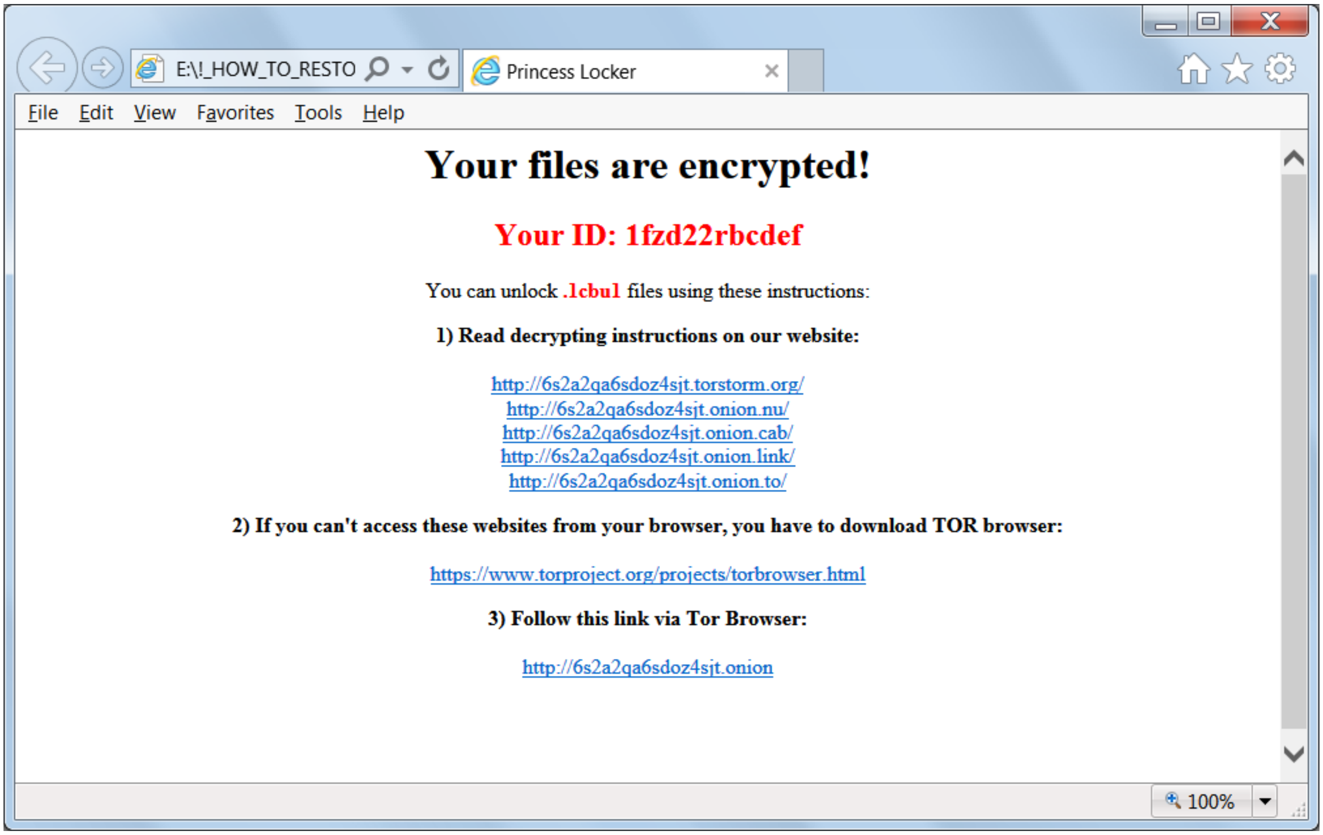
- September 28, 2016
- 06:42 PM
- 5



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.**



Your files are encrypted!

Your ID: 1fzd22rbcdef

You can unlock **.1cbu1** files using these instructions:

1) Read decrypting instructions on our website:

http://6s2a2qa6sdoz4sjt.torstorm.org/
http://6s2a2qa6sdoz4sjt.onion.nu/
http://6s2a2qa6sdoz4sjt.onion.cab/
http://6s2a2qa6sdoz4sjt.onion.link/
http://6s2a2qa6sdoz4sjt.onion.to/

2) If you can't access these websites from your browser, you have to download TOR browser:

https://www.torproject.org/projects/torbrowser.html

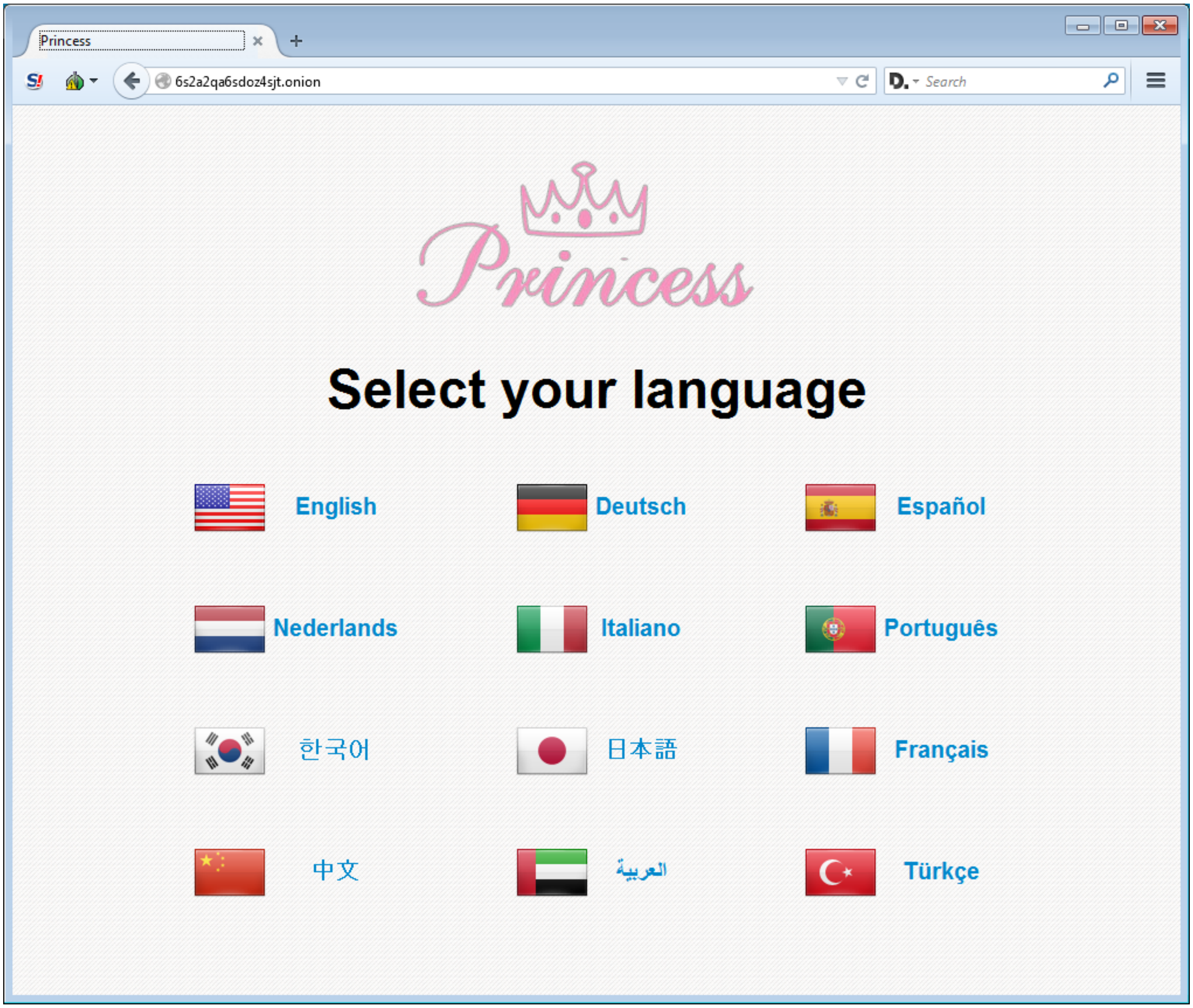
3) Follow this link via Tor Browser:

http://6s2a2qa6sdoz4sjt.onion

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.

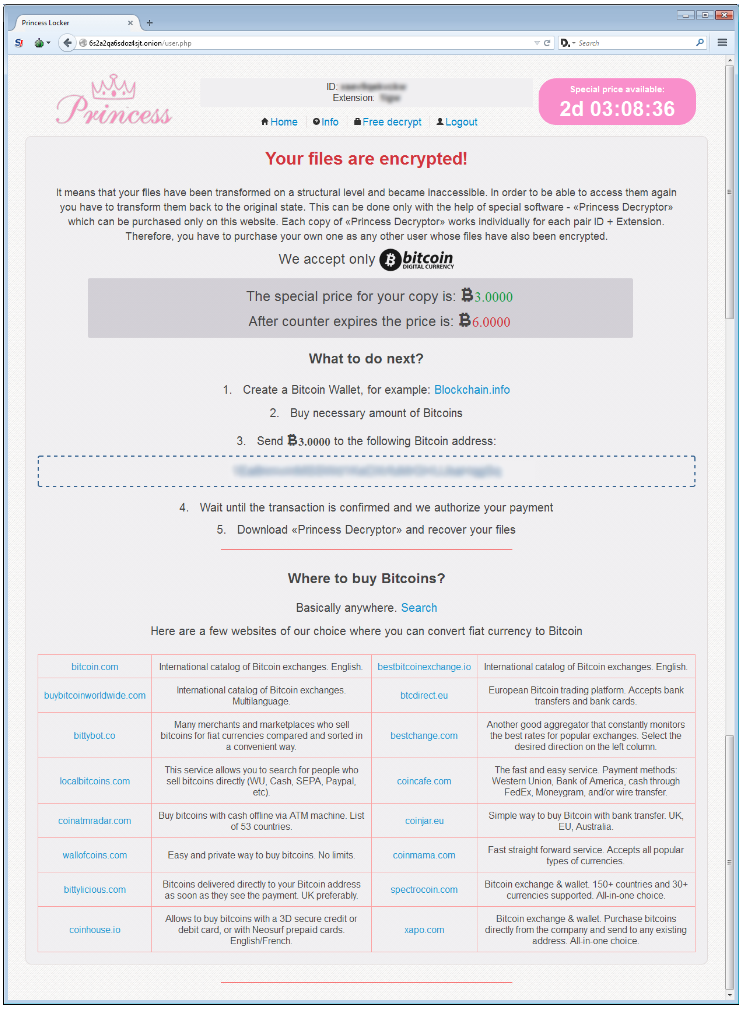


Select your language

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.

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.



6s2a2qa6sdoz4sjt.onion/user.php

ID: [redacted]
Extension: [redacted]

Home | Info | Free decrypt | Logout

Special price available:
2d 03:08:36

Your files are encrypted!

It means that your files have been transformed on a structural level and became inaccessible. In order to be able to access them again you have to transform them back to the original state. This can be done only with the help of special software - «Princess Decryptor» which can be purchased only on this website. Each copy of «Princess Decryptor» works individually for each pair ID + Extension. Therefore, you have to purchase your own one as any other user whose files have also been encrypted.

We accept only bitcoin DIGITAL CURRENCY

The special price for your copy is: Ƀ3.0000
After counter expires the price is: Ƀ6.0000

What to do next?

1. Create a Bitcoin Wallet, for example: Blockchain.info
2. Buy necessary amount of Bitcoins
3. Send Ƀ3.0000 to the following Bitcoin address:

[redacted]

4. Wait until the transaction is confirmed and we authorize your payment
5. Download «Princess Decryptor» and recover your files

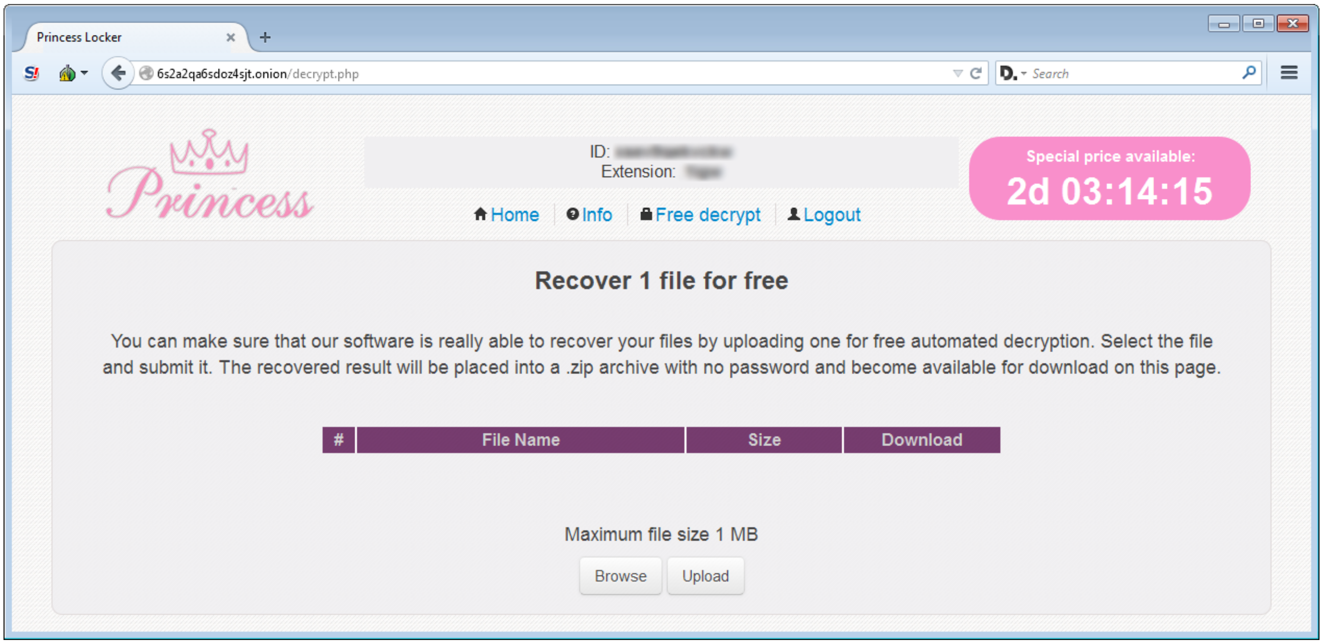
Where to buy Bitcoins?

Basically anywhere. Search

Here are a few websites of our choice where you can convert fiat currency to Bitcoin

bitcoin.com	International catalog of Bitcoin exchanges. English.	bestbitcoinexchange.io	International catalog of Bitcoin exchanges. English.
buybitcoinworldwide.com	International catalog of Bitcoin exchanges. Multilanguage.	btcdirect.eu	European Bitcoin trading platform. Accepts bank transfers and bank cards.
bittybot.co	Many merchants and marketplaces who sell bitcoins for fiat currencies compared and sorted in a convenient way.	bestchange.com	Another good aggregator that constantly monitors the best rates for popular exchanges. Select the desired direction on the left column.
localbitcoins.com	This service allows you to search for people who sell bitcoins directly (WU, Cash, SEPA, Paypal, etc).	coincafe.com	The fast and easy service. Payment methods: Western Union, Bank of America, cash through FedEx, Moneygram, and/or wire transfer.
coinatmradar.com	Buy bitcoins with cash offline via ATM machine. List of 53 countries.	coinjar.eu	Simple way to buy Bitcoin with bank transfer. UK, EU, Australia.
wallofcoins.com	Easy and private way to buy bitcoins. No limits.	coinmama.com	Fast straight forward service. Accepts all popular types of currencies.
bittylicious.com	Bitcoins delivered directly to your Bitcoin address as soon as they see the payment. UK preferably.	spectrocoin.com	Bitcoin exchange & wallet. 150+ countries and 30+ currencies supported. All-in-one choice.
coinhouse.io	Allows to buy bitcoins with a 3D secure credit or debit card, or with Neosurf prepaid cards. English/French.	xapo.com	Bitcoin exchange & wallet. Purchase bitcoins directly from the company and send to any existing address. All-in-one choice.

Princess Locker Payment Site



6s2a2qa6sdoz4sjt.onion/decrypt.php

ID: [redacted]
Extension: [redacted]

Home | Info | Free decrypt | Logout

Special price available:
2d 03:14:15

Recover 1 file for free

You can make sure that our software is really able to recover your files by uploading one for free automated decryption. Select the file and submit it. The recovered result will be placed into a .zip archive with no password and become available for download on this page.

#	File Name	Size	Download

Maximum file size 1 MB

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.

Related Articles:

Indian airline SpiceJet's flights impacted by ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

The Week in Ransomware - May 20th 2022 - Another one bites the dust

- Princess Locker
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- Viper_Security - 5 years ago

  Comment Deleted
  Reason, people will take it the wrong way, especially since this malware is irrelevant to casuals.

- GT500 - 5 years ago

  It's funny that they use the term "fiat currency" in the payment instructions. Somehow I imagine that most people don't know what that means.

-

  Lawrence Abrams - 5 years ago

  Interesting..didn't notice. Not sure if I have seen that used before in relation to ransomware.

-

  Amigo-A - 5 years ago

  Many girl-women regard themselves as princesses. Pop-gun for them. :)

- nileshbhakre - 5 years ago

  plz give me the sample of this ransomware.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: