Locky Ransomware switches to the Lukitus extension for Encrypted Files

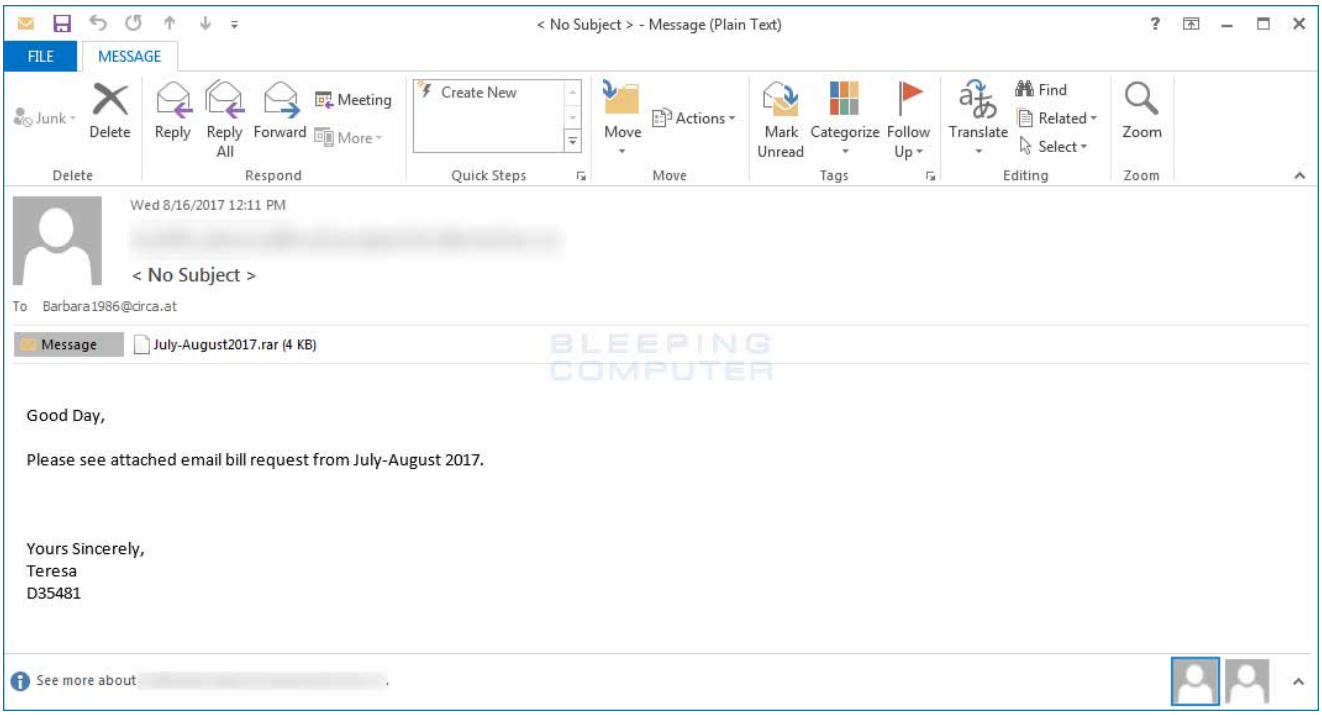
bleepingcomputer.com/news/security/locky-ransomware-switches-to-the-lukitus-extension-for-encrypted-files

By
Lawrence Abrams

- August 16, 2017
- 02:53 PM
- 0

Today a new Locky Ransomware variant was discovered by Rommel Joven that switches to the .lukitus extension for encrypted files. It is important to note that if you are infected with this ransomware, you are not infected with the Lukitus Ransomware, as some sites may call it. You are instead infected by Locky, which is using the .lukitus extension. There is a difference.

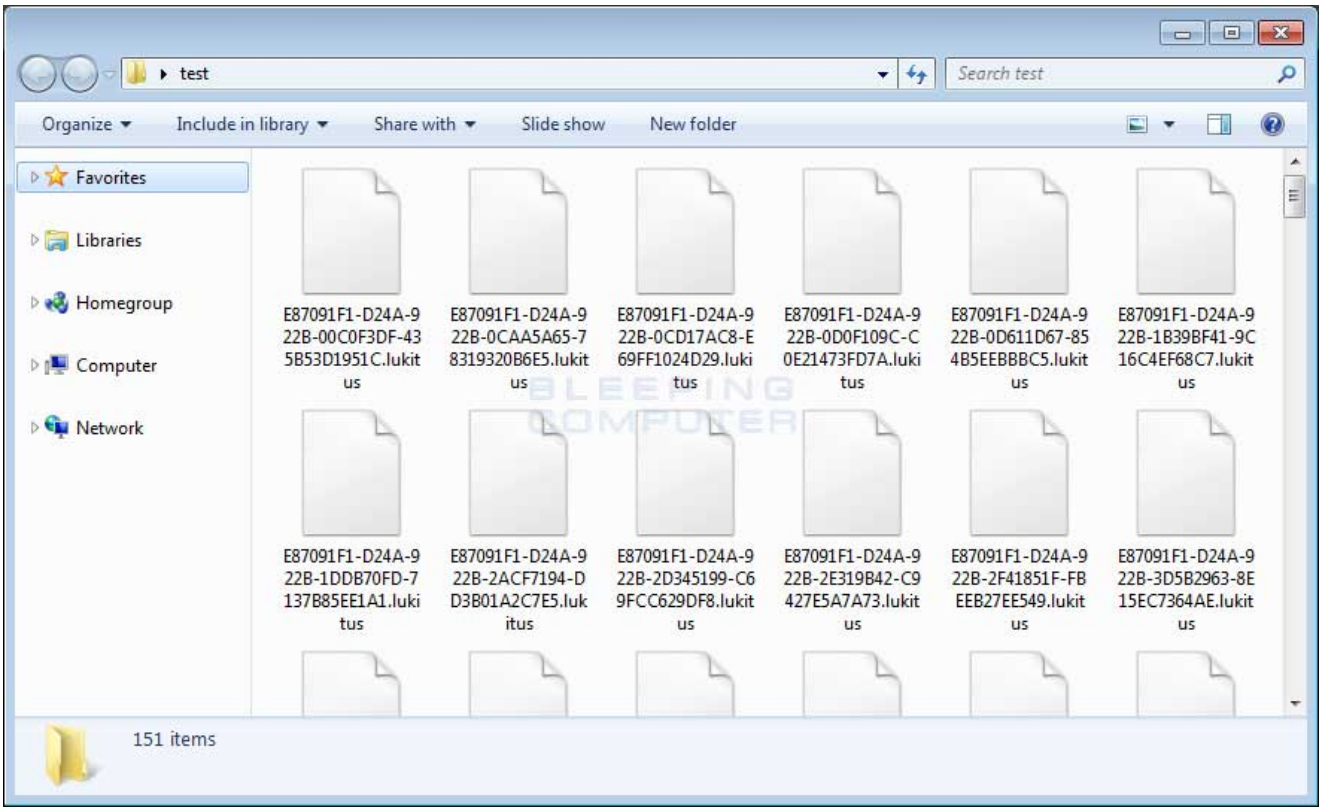
According to Derek Knight, this variant is currently being distributed via spam emails that have subject lines of **< No Subject >** or **Emailing - CSI-034183_MB_S_7727518b6bab2**, which contain zip or rar attachments with JS files. When these JS files are executed, they will download the Locky executable from a remote site.



Spam Email

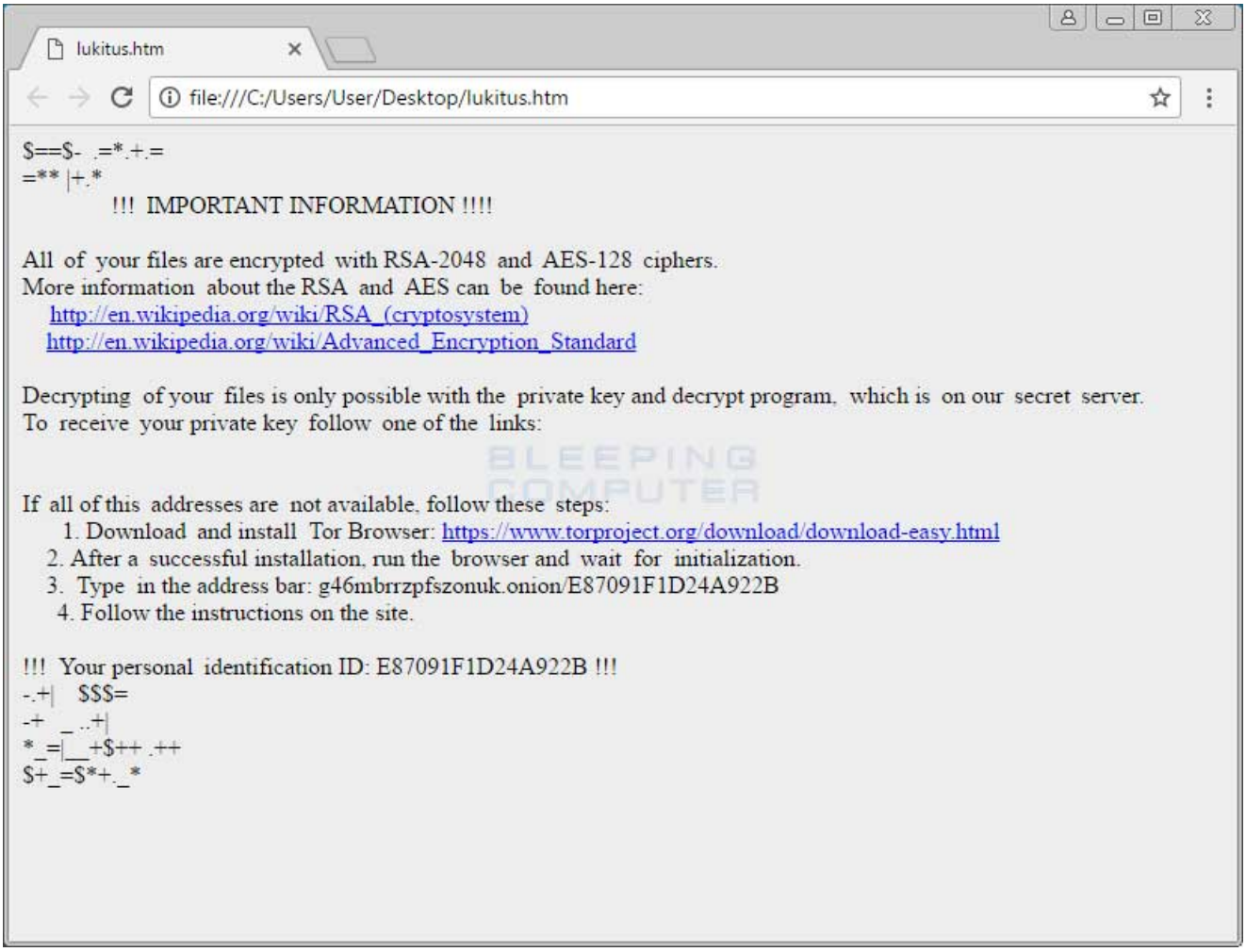
Once the file is downloaded and executed, it will scan the computer for files and encrypt them. When this Locky variant encrypts a file it will modify the file name and then append the **.**lukitus. When renaming the file, it uses the format **[first_8_hexadecimal_chars_of_id]-[next_4_hexadecimal_chars_of_id]-[next_4_hexadecimal_chars_of_id]-[4_hexadecimal_chars]-[12_hexadecimal_chars].lukitus**.

This means that a file named **1.png** would be encrypted and named something like as **E87091F1-D24A-922B-00F6B112-72BB7EA6EADF.lukitus**.



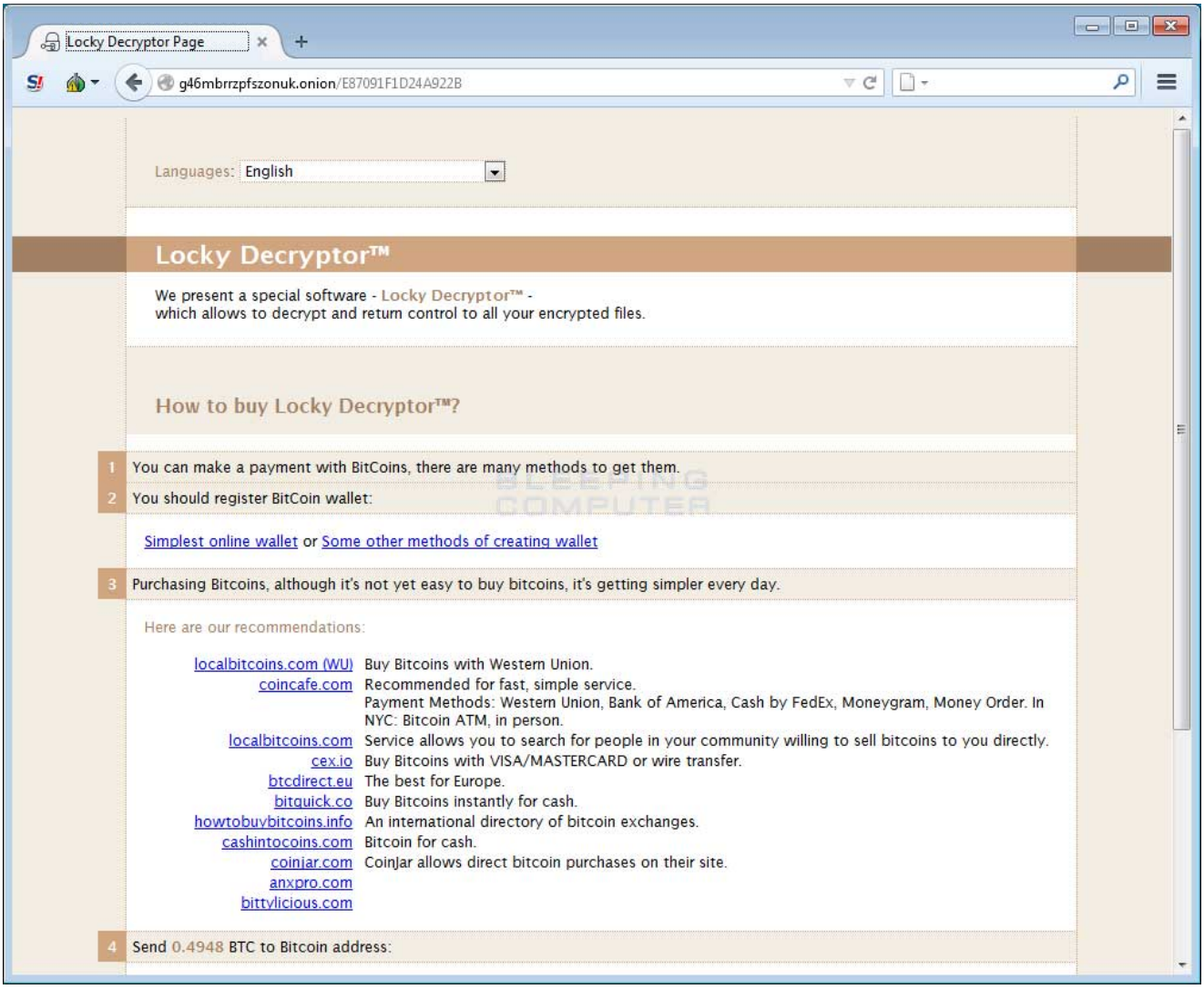
Files encrypted with the Lukitus Locky Ransomware Variant

When Locky has finished encrypting the computer, it will remove the downloaded executable and then display a ransom note that provides information on how to pay the ransom. The names of these ransom notes have changed for this version to **lukitus.htm** and **lukitus.bmp**.



Locky Lukitus Ransom Note

At the time of this writing, the Locky Decryptor TOR payment site has the ransom set to .49 BTC or approximately $2,000 USD.



Locky Decryptor Payment Site

It is not possible to decrypt the Locky Ransomware Lukitus Variant

Unfortunately, at this time it is still not possible to decrypt .lukitus files encrypted by the Locky Ransomware for free.

The only way to recover encrypted files is via a backup, or if you are incredibly lucky, through Shadow Volume Copies. Though Locky does attempt to remove Shadow Volume Copies, in rare cases ransomware infections fail to do so for whatever reason. Due to this, if you do not have a viable backup, I always suggest people try as a last resort to restore encrypted files from Shadow Volume Copies as well.

For those who wish to discuss the Locky ransomware or need support, you can use our dedicated Locky Ransomware Help & Support Topic.

How to protect yourself from the Locky Ransomware

In order to protect yourself from Locky, or from any ransomware, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

You should also have security software that contains behavioral detections such as Emsisoft Anti-Malware or Malwarebytes. I also recommend trying a dedicated ransomware protection program like RansomFree.

Last, but not least, make sure you practice the following good online security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed.
- Use hard passwords and never reuse the same password at multiple sites.

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

Update 8/16/17 7:21 PM - Updated with information about spam distribution.

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

IOCs

Hash:

```
SHA256: 29fc7875aac4e84fc6b5f76c9bb51eba9bb19eb4398cba5505050809b0f88035
```

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.