What is Ransomware?

Ransomware is a type of malware that encrypts data on your device and asks the user to pay money in order to get their data back. This particular piece of malware uses exceptionally strong encryption so there is no practical way to get the data back unless you pay the malware operators. However, even if you pay the malware operator there is no guarantee that you will get your data back. This particular variant uses infected Word (.doc, .docx) or Excel (.xls and .xlsx) files to spread the ransomware.

What is the best way to protect my personal data from Ransomware?

Chapman has updated Anti-Virus (AV) software definitions so most of the ransomware can be filtered out on University provided devices. However, updating your anti-virus may still not be enough to protect your files on your personal devices as malware operators often morph the malware to bypass defection by anti-virus. The most effective way to combat this malware is to simply avoid opening attachments from unknown senders.

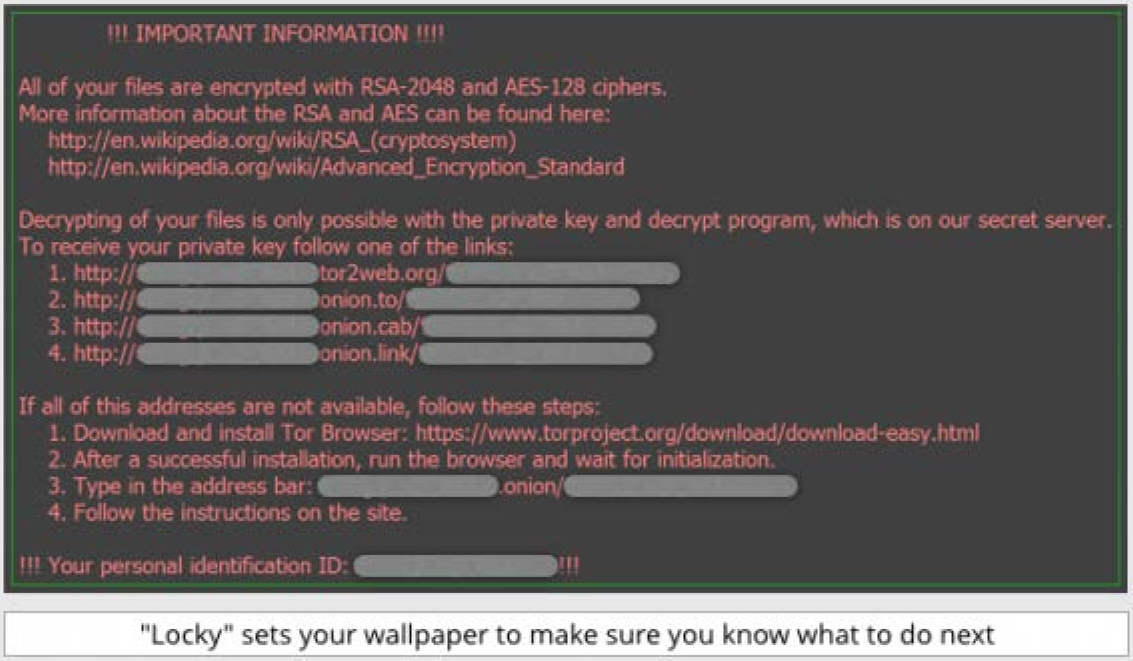
A few helpful reminders:

- Do not open any emails from senders you don’t know
- Do not open invoices, Excel, Word documents, or any other attachments from unknown sources
- Back up your critical data frequently on an external drive
- Update the Anti-Virus software on your personal computers to the latest virus definitions
- Report any suspicious email b

How do I know if my personal computer is infected?

This particular ransomware variant got it’s name from the fact it renames all your files with the extension *.locky.

Also once the ransomware finished encrypting the files it changes your desktop background with instructions on how to pay the ransom and recover your files. An example of these instructions is shown below.



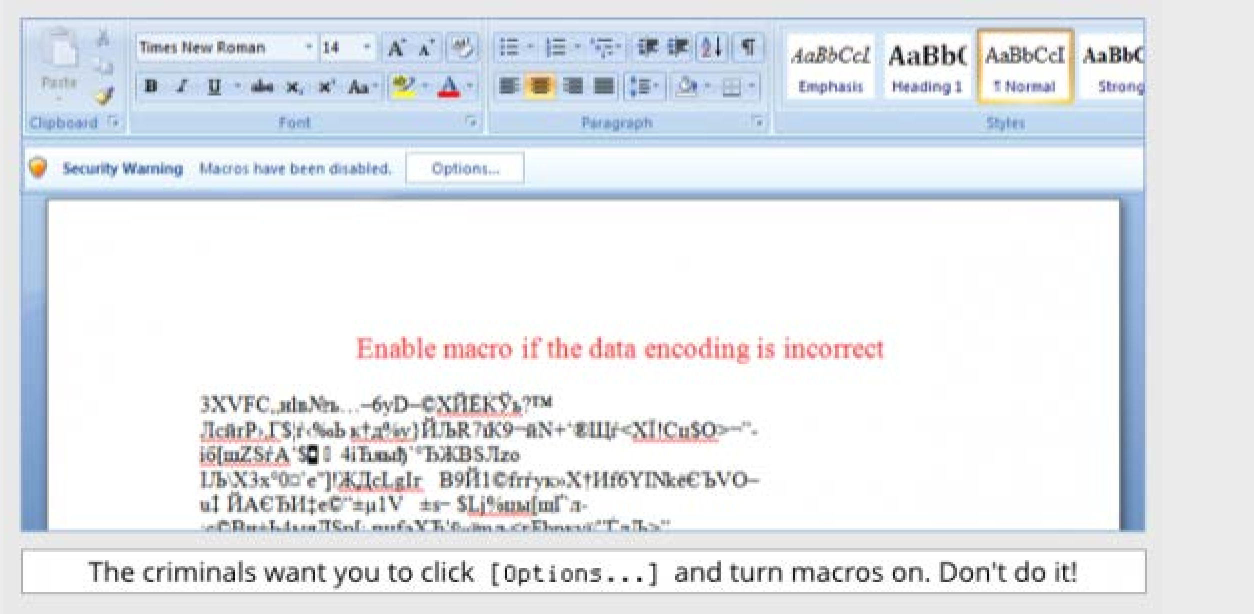
```
        !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://[redacted]tor2web.org/[redacted]
    2. http://[redacted]onion.to/[redacted]
    3. http://[redacted]onion.cab/[redacted]
    4. http://[redacted]onion.link/[redacted]

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: [redacted].onion/[redacted]
    4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted]!!!
```

"Locky" sets your wallpaper to make sure you know what to do next

Ransomware applications generally update your desktop background with an image containing instructions for paying the ransom.

The most common way that Locky arrives is as follows:

- You receive an email containing an attached document (Troj/DocDl-BCF).
- The document contents look scrambled.
- The document advises you to enable macros "if the data encoding is incorrect."
- If you enable macros, you don't actually correct the text encoding (that's a subterfuge); instead, you run code inside the document that saves a file to disk and runs it.
- The saved file (Troj/Ransom-CGX) serves as a downloader, which fetches the final malware payload from the crooks.
- The final payload could be anything, but in this case is usually the Locky Ransomware (Troj/Ransom-CGW).



Security Warning Macros have been disabled. Options...

Enable macro if the data encoding is incorrect

3XVFC„ніъNъ…–6уD–©XЙЁКЎь?™
ЛсйrР›,Г$¦ѓ‹%ьb к†д°іv}ЙЉЬR7іК9¬ãN+'®Щѓ<ХЇ!Cu$O>¬'".
іб[шZSѓA`$▮▯ 4іЋлљђ`°ЪЖBSЛzо
ЦЪ\X3x°0□'е"]!ЖДсLgIr B9Й1©frѓуќ»Х†Иf6YINkє€ЪVO–
uЈ ЙАЄЂИ‡е©"±µ1V ±s– $Lj%ыы[шГ`л-
[illegible]

The criminals want you to click [Options...] and turn macros on. Don't do it!

A ransomware infected file. Enabling macros will trigger a script to download the malware to your computer, locking you out of your own files.