

TorrentLocker  
ransomware

# WHO ARE WE?

Harshil Patel



Ashfaq Abdullah

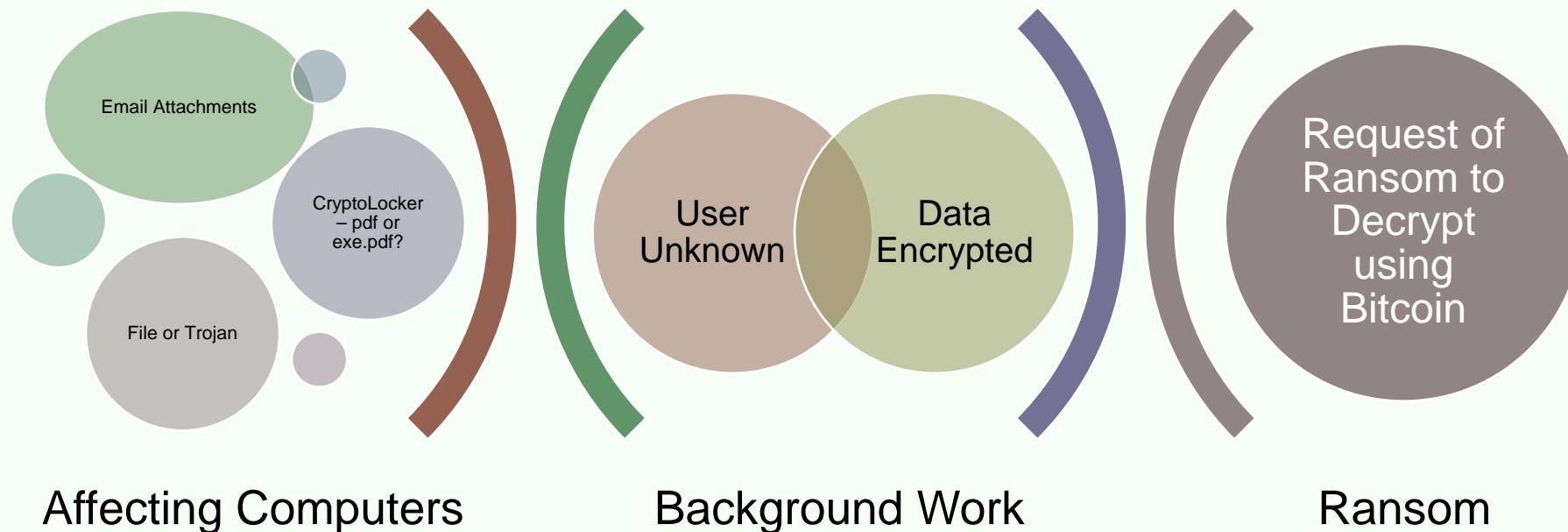


Gobisan Pathmasiri



# WHAT IS TORRENTLOCKER?

TorrentLocker is a type of ransomware that encrypts a user's data. The user then receives a message on how to get their data back: pay bitcoin. Only after the ransom is paid will the data be released to the user.



# HOW?

- Makes changes to explorer.exe after being executed
- Creates or Modifies Registry Keys – makes it able to launch at startup

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<random>

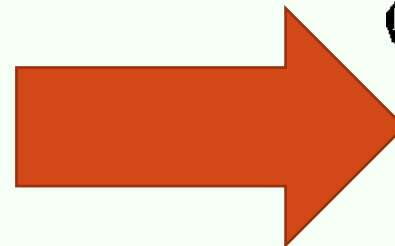
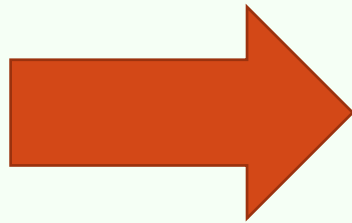
C:\ProgramData\<random>.exe

Any GUESS on how many extensions have been infected by now?



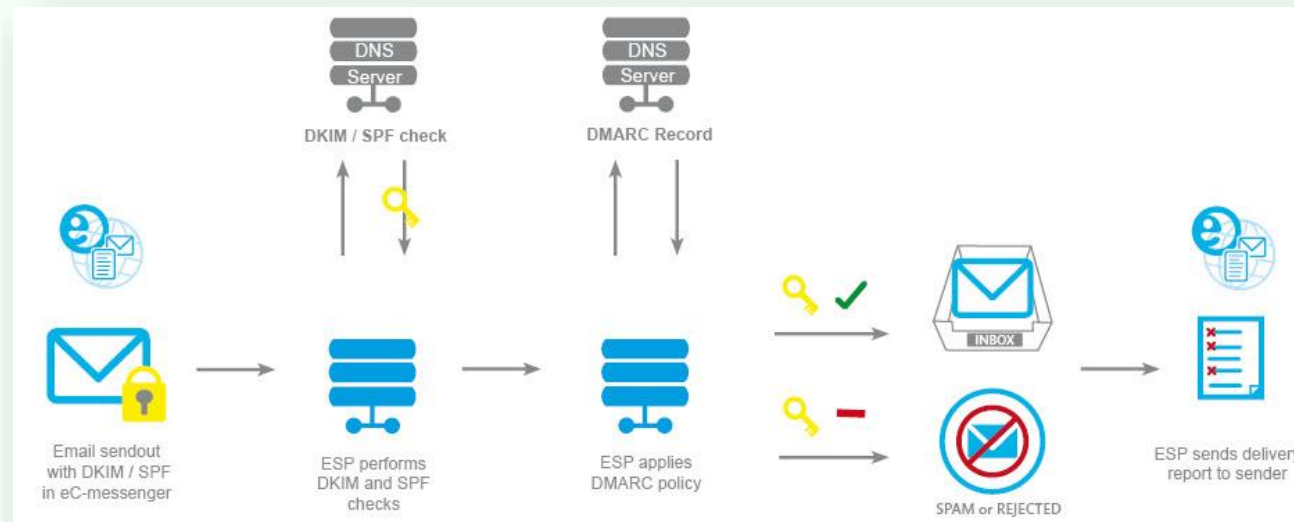
# BE AWARE! (Think before you click)

mfw,\*.mef,\*.mdc,\*.kdc,\*.kc2,\*.iiq,\*.gry,\*.grey,\*.gray,\*.fpx,\*.fff,\*.exf,\*.erf,\*.dng,\*.dcr,\*.dc2,\*.crw,\*.craw,\*.cr2,\*.cmt,\*.cib,\*.ce2,\*.ce1,\*.arw,\*.3pr,\*.3fr,\*.mpg,\*.jpeg,\*.jpg,\*.mdb,\*.sqlitedb,\*.sqlite3,\*.sqlite,\*.sql,\*.sdf,\*.sxc,\*.ots,\*.ods,\*.sxc,\*.stw,\*.sxw,\*.odm,\*.oth,\*.ott,\*.odt,\*.odb,\*.csv,\*.rtf,\*.accdr,\*.accdt,\*.accde,\*.accdb,\*.sldm,\*.sldx,\*.ppsm,\*.ppsx,\*.ppam,\*.potm,\*.potx,\*.pptm,\*.pptx,\*.pps,\*.pot,\*.ppt,\*.xlw,\*.xll,\*.xlam,\*.xla,\*.xlsb,\*.xltm,\*.xltx,\*.xlsm,\*.xlsx,\*.xlm,\*.xlt,\*.xls,\*.xml,\*.dotm,\*.dotx,\*.docm,\*.docx,\*.dot,\*.doc,\*.txt .....and many more



# INFECTION

- Initially, TorrentLocker targeted Australian victims using Australia Post themed phishing campaigns and websites.
- The emails of new TorrentLocker campaign use Domain-based Message Authentication, Reporting and Conformance (DMARC) to avoid detection and collect data.



# ANALYSIS (ISIGHT PARTNERS)

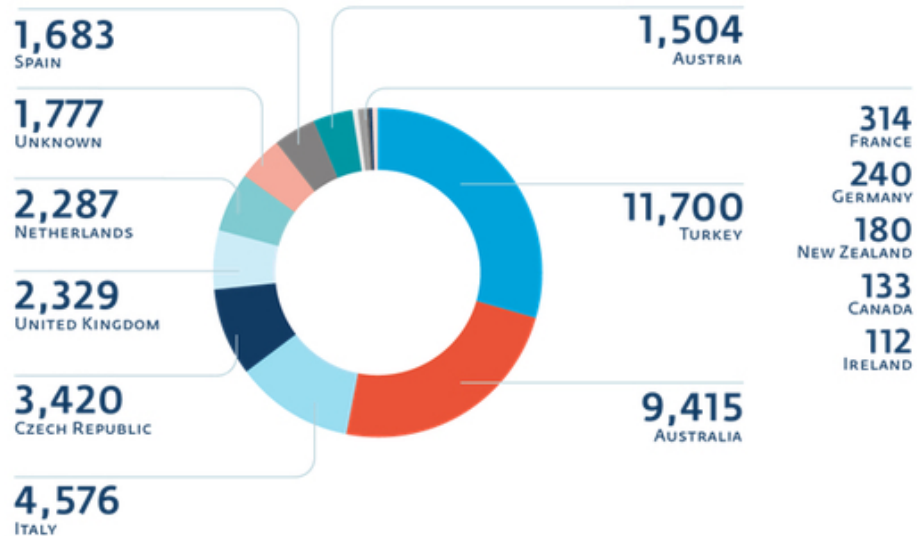
- Encryption use: AES with either 128, 192, or 256 bit keys
- Rijendael is a symmetric encryption algorithm that is best known for its use in advanced encryption standard (AES)
- Primarily encrypted all files using same key which could be decrypted using Output Feedback mode. After the disclosure, modified to use different key streams (Cipher-Block Chaining).



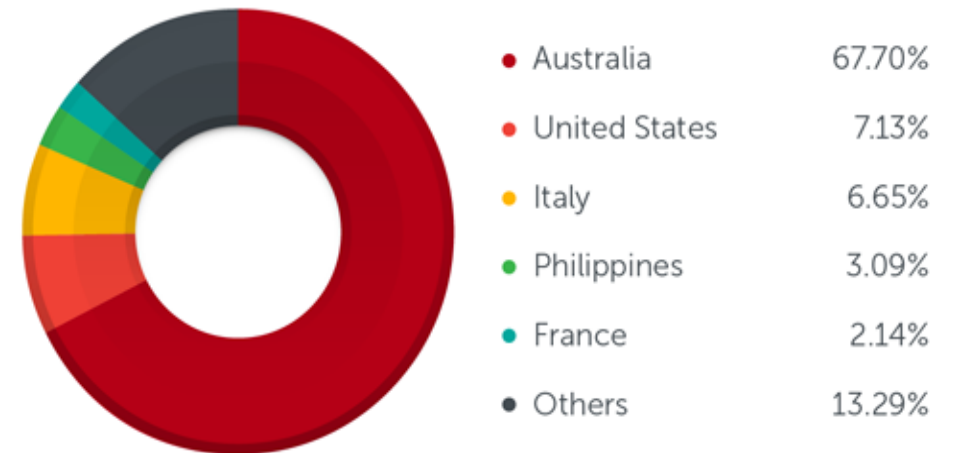


# SPREAD STATISTICS:

Before DMARC



After DMARC



- The report reveals that there are 691.5 new infected computers per day.






# LOOK AND FEEL

**Your files are encrypted.**

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **28/05/14 - 09:02** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:

**119h 48m 01s**

Your system: **Windows XP (x32)** First connect IP: **69.80.100.35** 

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We give you the opportunity to decipher 1 file free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt the files.

Please select a file to decrypt and load it to the server

Note: file should not be more than 512 kilobytes

## WARNING

**We have encrypt your files with CryptoLocker virus**



Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc. were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software.

Caution: Removing of CryptoLocker will not restore access to your encrypted files. The only way to save your files is to buy a decryption software. Otherwise, your files will be lost.

[Click here to buy decryption software](#)

Our website should also be accessible from one of these links:

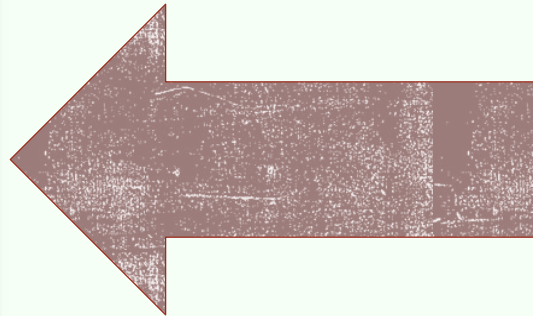
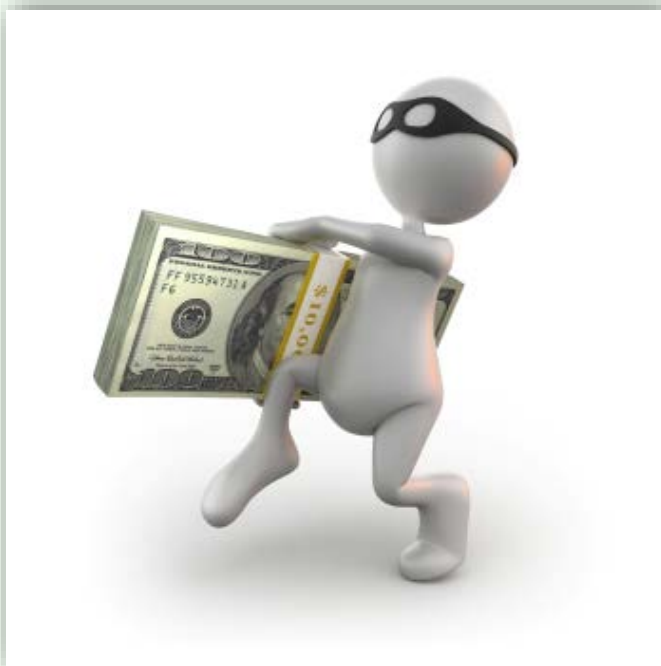
<http://erhitnwfvpgajfbu.tor4u.net/buy.php?71mndj>  
<http://erhitnwfvpgajfbu.door2tor.org/buy.php?71mndj>  
<http://erhitnwfvpgajfbu.tor2web.org/buy.php?71mndj>  
<http://erhitnwfvpgajfbu.onion.cab/buy.php?71mndj>

Frequently Asked Questions



# PAYMENTS

- According to ESET's research, only 570 out of 39,760 infected systems actually received the decryption software. In the report, L  veill   explained that only 1.44% of identified users have paid the full ransom to the criminals. Another 20 people partially paid and didn't receive their data.



# HOW TO RESCUE?

## TorrentLocker says:

```
If (ComputerInfected == TorrentLocker)
{
    Pay Bitcoin;
    if (Paid){
        Release Data; }
    else {
        No Data; }
}
```

## Simple Solution:

```
If (ComputerInfected == TorrentLocker) {
    NoPayment;
    Restart Computer;
    GoodBye TorrentLocker;
    If (ComputerInfected == TorrentLocker) {
        NoPayment;
        Format Computer; // Data Lost
        GoodBye TorrentLocker;
    }
}
```





Q&A

You have

Questions

We have

Answers

# Q AND A

## 1) What is TorrentLocker?

TorrentLocker is a type of malware known as 'ransomware'. It acts by restricting user access to personal files. Restrictions are lifted after payment (in Bitcoins) is made to the attacker(s).

## 2) How does TorrentLocker restrict access?

TorrentLocker utilizes the Rijndael algorithm, one of the five finalists chosen by the NIST to be used for the AES. Key sizes are 128, 192, or 256 bits in length.

## 3) Aside from paying, what can you do to circumvent TorrentLocker?

Unfortunately, no desirable solution exists as of now. The malware reappears upon restart of the computer. Rebooting the computer is the only known solution, however, it also results in a loss of all files on the system.



# REFERENCES:

- <http://digital-forensics.sans.org/blog/2014/09/09/torrentlocker-unlocked>
- <http://www.isightpartners.com/2014/09/torrentlocker-new-variant-observed-wild/>
- <http://insidebitcoins.com/news/torrentlocker-holds-user-data-for-bitcoin-ransom-but-only-a-fraction-of-victims-pay/27915>
- <http://www.securityweek.com/torrentlocker-malware-combines-elements-cryptolocker-cryptowall>
- <http://www.isightpartners.com/2014/09/torrentlocker-new-variant-observed-wild/>
- <http://www.welivesecurity.com/2014/12/16/torrentlocker-racketeering-ransomware-disassembled-by-eset-experts/>
- <http://securityaffairs.co/wordpress/34268/cyber-crime/new-torrentlocker-campaign.html>

