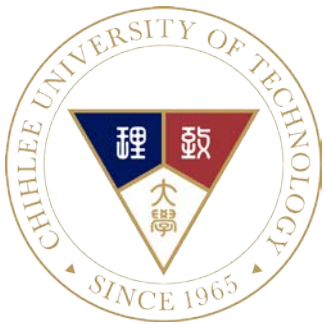




資訊安全 人人有責

主講人：康松連組長
2015年11月19日

勒索軟體病毒-中毒途徑

- ▶ 主要途徑除了透過「社交工程」或其他方式誘騙使用者執行，看起來像一般帳單、有 .exe 副檔名的 Word 或 PDF 文件、色情的照片或影片的綁架軟體之外，還會透過各種方式以病毒或木馬等方式散布這些惡意程式，甚至還會透過區網傳染給辦公室裡的電腦。

勒索軟體病毒-中毒癥兆

- ▶ 檔案、照片、文件、Word、Excel...通通都被**加密鎖起來、全部被改名**，無法開啟，如果要使用原本的檔案的話，則會跳出一個說明視窗需要中毒者付錢，方可解密、解鎖。

勒索軟體病毒-中毒畫面



勒索軟體病毒-中毒畫面

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Otherwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open [http://\[REDACTED\].onion.cab](http://[REDACTED].onion.cab) or [http://\[REDACTED\].tor2web.org](http://[REDACTED].tor2web.org) in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1. Download Tor Browser from <http://torproject.org/>
2. In the Tor Browser open the [http://\[REDACTED\].onion/](http://[REDACTED].onion/)
Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable.

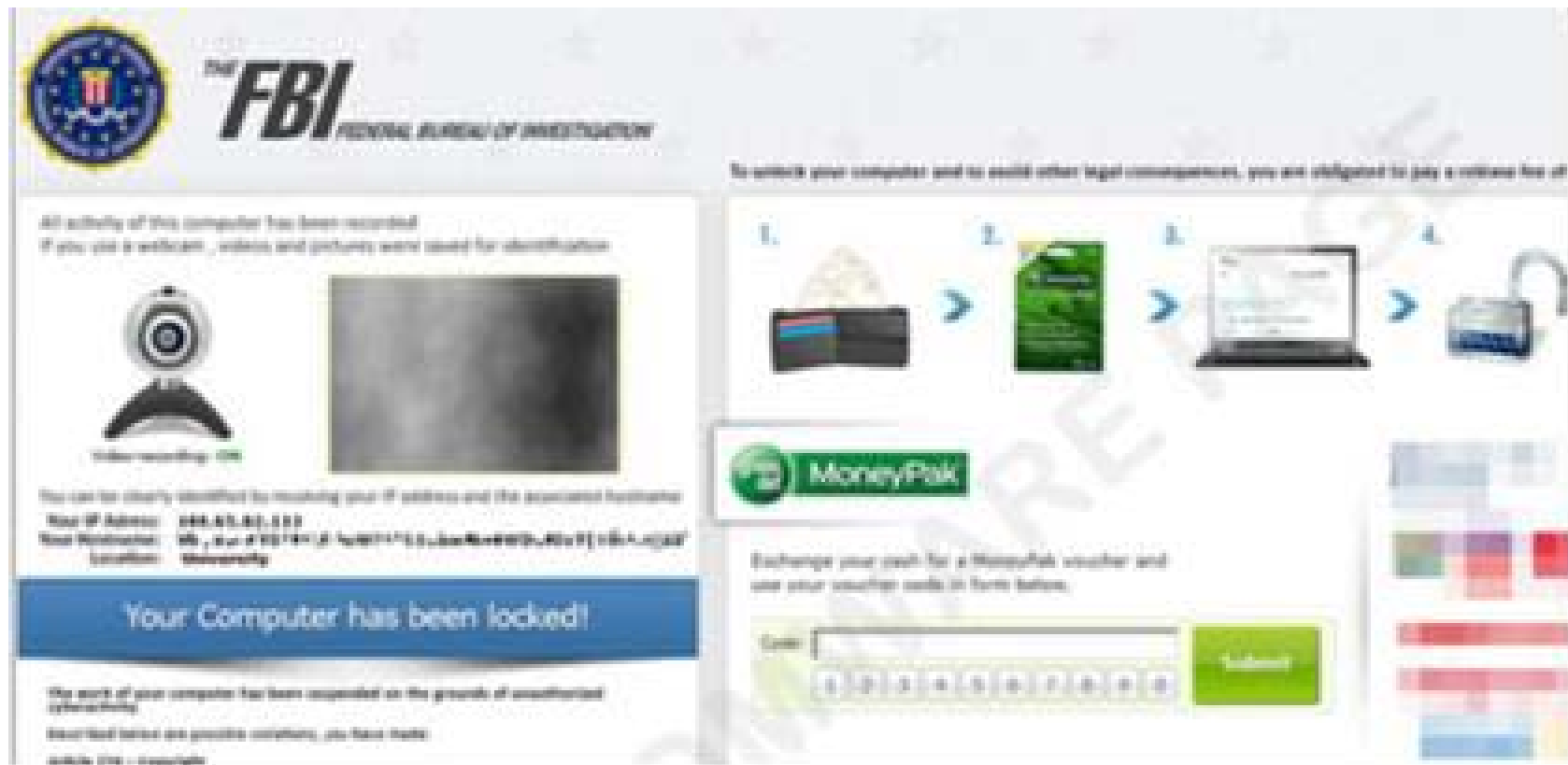
Write in the following public key in the input form on server. Avoid missprints.

[REDACTED]

Follow the instructions on the server.

These instructions are also saved to file named DecryptAllFiles.txt in Documents folder. You can open it and use copy-paste for address and key.

勒索軟體病毒-中毒畫面



勒索軟體病毒-中毒畫面

**YOUR COMPUTER
HAS BEEN BLOCKED**



THE UNITED STATES
DEPARTMENT OF JUSTICE

For information look to the *Wall of Shame* located here: [http://www.fbi.gov/wall-of-shame](#)

New Position:
New Position:
Location: United States, Dallas

The work of your computer has been suspended on the grounds of the violation of the law of the United States of America.

Penalties violations are described below:

Article - 144. Pornography involving children under 18 years
Imprisonment for the term of up to 10 (10) years
(The use of child factor of pornography file)

Article - 175. Copyright
Imprisonment for the term of up to 5 (5) years
(The use of sharing of copyrighted file)

Article - 183. The use of unknown software
Imprisonment for the term of up to 5 years
(The use of unknown software)

All stolen, activated (activated) folders your computer need data
recovered in the future technical, recovered method and restore these must
include full Payment card information. This card data transmitted in virtual
monetary/ recovered assets.

When recording 

SHOWN FILE
one of your files being stolen on the site


In connection with the decision of the Government as of October 11, 2013, all of the
violations described above could be considered as criminal. If the file has been paid,
you will become the subject of criminal prosecution. The file is applicable only to the case
of a primary violation. In the case of repeated violation you will appear before the Supreme
Court of the city.

Amount of the fee is **\$1000**. Payment must be made within 48 hours after the computer
locking. If the fee has not been paid, you will become the subject of criminal prosecution
without the right to pay the fee. The Department for the Fight Against Cyberattacks will
confiscate your computer after 48 hours.

Article 183.33. The use of unknown software
Imprisonment for the term of up to 5 years
(The use of unknown software)

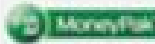
All attempt to restore the computer for monetary will, using the full capabilities of the computer system
file, the FBI, restore, restore, accordingly the work conducted with the file.

The first attempt may be made the criminal liability if the payment of the fee is
connected with the use of money to the people, on 11 December 2013. In repeated
violations of criminal responsibility is available.

To unlock your computer and to avoid other legal consequences,
you are obligated to pay a release fee of **\$1000**.

How do I unlock computer using the MoneyPak?

1. Find a local location near you.
2. Look for a MoneyPak in the proper section. Take the card without it with cash. A
service fee of up to \$400 will apply.
3. To you first, you should enter the eight MoneyPak masking code in the payment form and
press the MoneyPak.



Code:

Where you buy MoneyPak



Please note: This fee may only be paid within 48 hours, if you let 48 hours pass without
payment, the possibility of unlocking your computer expires. In this case a criminal case against
you will be initiated automatically.

勒索軟體病毒-應變之道

- ▶ 立即切斷網路連線，避免拖垮網路連線速度，繼續加密未完成的檔案
- ▶ 尋找有無備份檔案，若是沒有備份，可透過Windows內建的系統還原設定、Shadow Explorer軟體嘗試還原先前的版本
- ▶ 檔案還原完成後，利用使用微軟Safety Scanner或是防毒軟體，執行完整掃描，清除惡意程式，或是乾脆選擇重灌電腦。

勒索軟體病毒-預防方法

- ▶ 這種加密病毒來源多半是藏在網頁廣告、假網站、非法郵件、隨身碟等，所以建議在使用網路上請特別小心。
- ▶ 盡量不要瀏覽未知網站或連結，特別是大陸網站(**xxx.xxx.cn**)。不要開啟不熟悉的網頁或是不明電子郵件附件或連結，瀏覽網頁時顯現的彈出式視窗不要點選安裝，也不要安裝非公務使用或是網路流傳之破解軟體，避免感染病毒。
- ▶ 開啟電子郵件附件時小心是不是偽裝檔名的 **exe** 執行檔。
- ▶ 請勿使用「○○空間下載器」或迅雷 **P2P** 之類的下載工具程式。
- ▶ 請勿使用來源不明的隨身碟。
- ▶ 請不要再繼續使用 **Windows XP** 系統，快快升級 **Windows 7** 以上版本，持續 **Windows** 系統更新外，也請定期檢查防毒軟體是否正常更新。
- ▶ 最重要的，就是請記得定期備份你的重要資料和郵件，因為被加密後要救也都救不回來，只有全部刪除了！

社交工程演練

信件標題
【APP 推薦】超實用→台灣天氣類 App 第一名的台灣天氣資訊！！
您的 Apple ID 密碼重置確認
這個吃了會胖、那個會致癌？！揭開 5 種食物真面目
昆蟲偽裝大師
Apple 直營店來了！？
台灣公務員根本是天使！看看台灣、美國、中國、加拿大的公務員有何不同
全台熱門社區房價行情，前三社區房價下修 5～10%
回味無窮！全台十大排行必逛人氣老街！
注意！這五種飲料成分可能對孩子有害！
吸空氣會胖是真的！美研究：灰塵中的化學物質使人發胖！

教育部於104年度曾對本校實施兩次電子郵件社交工程演練，測試結果開啟惡意電子郵件者有升高趨勢（**第一次演練：「開啟信件」比率54.43%，「點選連結」比率：1.69%；第二次演練：「開啟信件」比率57.81%，「點選連結」比率：1.27%。**），經教育部評比演練結果未達標準（惡意郵件開啟率應低於10%以下；惡意連結(或檔案)點擊率應低於6%以下。），**本校被列為持續改善之機關。**

社交工程



新增聯絡人 - Internet Explorer

http://140.131.77.18/addressANM.do?uid=4353&token=from&tn

新增聯絡人 * 表示不可省略

* 名稱 IT服务台 組織 搜尋

姓名

E-mail openwebmail@fuse.net

行動電話

生日

所屬群組

性別 ☒ 男 ☐ 女

居住住址

住所電話

公司名稱

公司住址

公司電話

傳真號碼

個人網址 連結

公司網址 連結

儲存 取消

接收:4 (低危險群:0 中危險群:4 高危險群:0 威脅郵件:0)

狀態	動作	過濾名單	回報	寄信人	
垃圾郵件	接收	接收並加入白名單	回報	ADTRAN marketing@mktg.adtran.com	Important Bluesocket Access Point S
垃圾郵件	接收	接收並加入白名單	回報	Imperva Webinars webinar@imperva.com	CTO shares how to stay ahead of ha
垃圾郵件	接收	接收並加入白名單	回報	iThome產品技術報 (HTML 圖文版) epaper@msx.epaper.com.tw	提供豐富圖表, 可延伸8種網管應用功能
垃圾郵件	接收	接收並加入白名單	回報	iThome每日新聞報 (HTML 圖文版) epaper@msx.epaper.com.tw	Google語音助理更聰明了, 更複雜的「最

貼心叮嚀

- ▶ 目前，病毒感染之檔案無法救回。
- ▶ 培養良好的使用電腦習慣，來路不明的寄件者或是附件，千萬不要開啟。
- ▶ 定期備份個人重要資料，並將備份資料保存於安全地點。
- ▶ 各單位使用存放資料的學校網路空間，請不要持續連線，避免電腦中毒後，造成網路空間檔案也中毒。