

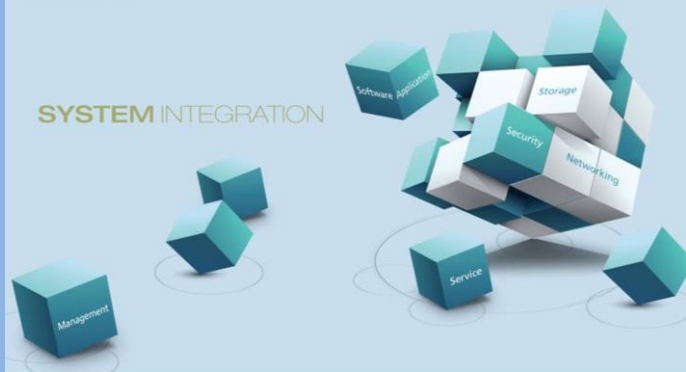


麟雲資訊

Ring Cloud Technology

XX大學

加密勒索軟體應有的認知



- 關於加密勒索軟體
- 它的發展
- 面對勒索
- 該有的意識
- 解密
- 自我防護
- 備份

特色



1. 悄悄地將檔案加密
2. 無法開啟檔案
無法解密
3. 勒索贖金



ransomware

2005年 由俄羅斯開始



Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)

18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to \$250,000.

Technical details:

Involved IP address: [REDACTED]

Involved host name: [REDACTED]

Source or intermediary sites: <http://pornerbros.com>

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of \$300.

HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:

Walmart CVS pharmacy Walgreens

2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

1	2	3
4	5	6
7	8	9
Delete	0	Enter

2012年

Police Ransomware

Permanent lock on 05/01/2013 5:20 p.m. EST



Your personal files are encrypted!



Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

2013年

CryptoLocker



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.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

2014年 CTB-Locker

View

95 50 03

Next >>

2014年

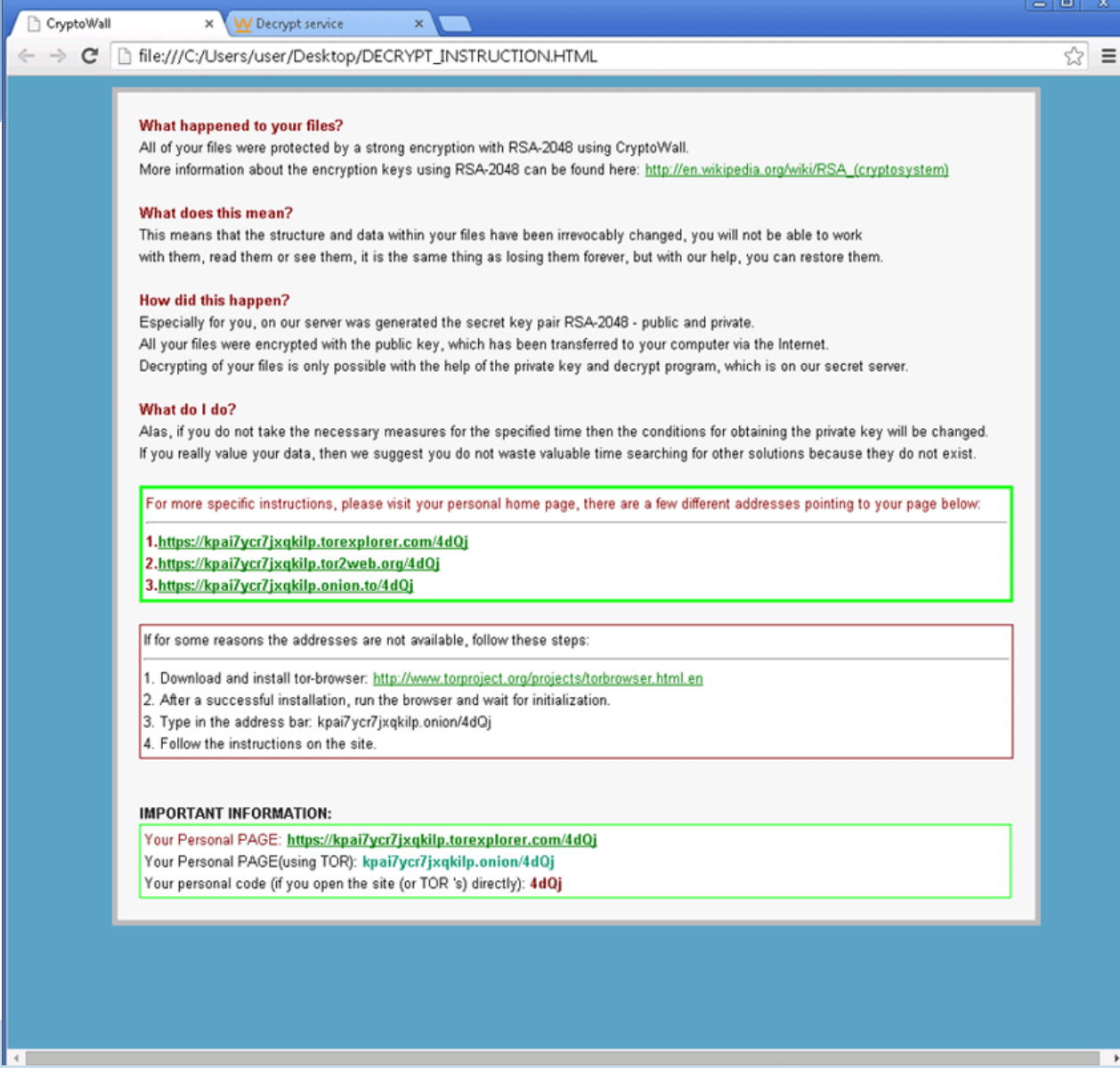
Android 勒索軟體

**За скачивание и установку
нелицензионного ПО ваш телефон
был ЗАБЛОКИРОВАН в
соответствии со статьей 1252 ГК
РФ Защита исключительных прав.
Для разблокировки вашего
телефона оплатите 1000 руб.
У вас есть 48 часов на оплату, в
противном случае все данные с
вашего телефона будут
безвозвратно уничтожены!**

1. Найдите ближайший терминал системы платежей QIWI
 2. Подойдите к терминалу и выберете пополнение QIWI VISA WALLET
 3. Введите номер телефона +79660624806 и нажмите далее
 4. Появится окно комментариев - тут введите ВАШ номер телефона без 7ки
 5. Вставьте деньги в купюроприемник и нажмите оплатить
 6. В течении 24 Часов после поступления платежа ваш телефон будет разблокирован.
 7. Так же вы можете оплатить через салоны связи Связной и Евросеть
- ВНИМАНИЕ:** Попытки разблокировать телефон самостоятельно приведут к полной блокировке вашего телефона, и потери всей информации без дальнейшей возможности разблокирования.

因為下載和安裝軟體
nelitsenzionnogo，你的手機已
經依照俄羅斯聯邦軍事準則民法第
1252條加以鎖住。
要解鎖你的手機需支付1000盧布。
你有48小時的時間支付，否則你手
機上的所有資料將永久被破壞！

1. 找到最近的QIWI終端支付系統
 2. 使用該終端機器，並選擇補充
QIWI VISA WALLET
 3. 輸入號碼79660624806，然後
按下一步
 4. 會出現留言視窗 – 輸入你的號
碼去掉7ki
 5. 將錢放入終端機，然後按支付
 6. 收到付款後的24小時內，你的
手機將會被解鎖。
 7. 你可以透過行動商店和
Messenger Euronetwork支付
- 注意：試圖自己解開手機會導致手
機完全被鎖住，所有消失的資料沒
有機會回復。



2015年

CryptoWall 3.0

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below.

1. <https://kpai7ycr7jxqkpl.torexplorer.com/4dQj>
2. <https://kpai7ycr7jxqkpl.tor2web.org/4dQj>
3. <https://kpai7ycr7jxqkpl.onion.to/4dQj>

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: `kpai7ycr7jxqkpl.onion/4dQj`
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGE: <https://kpai7ycr7jxqkpl.torexplorer.com/4dQj>
Your Personal PAGE(using TOR): `kpai7ycr7jxqkpl.onion/4dQj`
Your personal code (if you open the site (or TOR 's) directly): **4dQj**

Chimera® Ransomware

2015年



Chimera

You are victim of the Chimera® malware. Your private files are encrypted and can not be restored without a special key file. Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get your unique key file.

Address: **1HqoNfpAJFMy9E36DBSk1ktPQ9o9fn2RxX**

Amount: **0,93945085 Bitcoins**

For the decryption programm and additional informations, please visit:

<https://mega.nz/ChimeraDecrypter>

If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name.

Take advantage of our affiliate-program!

More information in the source code of this file.

We present a special software - **Locky Decrypter** - which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.



2. You should register BitCoin wallet ([simplest online wallet](#) OR [some other methods of creating wallet](#))
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [Coincafe.com](#) - Recommended for fast, simple service.
Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
- [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- [CEX.IO](#) - Buy Bitcoins with VISA/MASTERCARD or Wire Transfer
- [btodirect.eu](#) - THE BEST FOR EUROPE
- [bitquick.co](#) - Buy Bitcoins Instantly for Cash
- [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
- [Cash Into Coins](#) - Bitcoin for cash.
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
- [anxpro.com](#)
- [bitlyidous.com](#)

4. Send - 0.5 BTC to Bitcoin address:



5. Refresh the page and download decoder.

2016

Locky





Start

Payment

FAQ

Support

English

Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

⌚ The price will be doubled in:

6 days 6 hours 23 minutes 55 seconds

🔑 Start the decryption process

News

24.03.2015

WARNING

Do not restore the MBR with the Windows Recovery Tools. This could destroy your data completely!

There are a lot of wrong informations online. If you are looking for reliable informations, please visit [our website](#).

16.12.2015

Petya launched

Today we launched the Petya Ransomware Project.

勒索



Your money
or your data

報警 ?

網路犯罪檢舉專線: 02-2764-4490·02-2764-4434

電信警察各中隊傳真電話

第一中隊 02-26716892 台北縣三峽鎮中正路184巷11號

第二中隊 04-3954281 台中縣太平市振武路51-1號

第三中隊 07-3540927 高雄市楠梓區常德路242號

刑事警察局 <http://www.cib.gov.tw/>

電腦犯罪小組報案電話：02-27697403

檢舉電子信箱：Cybercop@cib.gov.tw

意識

不收不明信

不開可疑檔

不隨意點連結

保持更新

即時回報



創意的加密組合

AES + RSA
(對稱) (非對稱)



FBI Boston's Joseph Bonavolonta address the [Cyber Security Summit](#) on October 21st. Bonavolonta said that **paying the ransom is often the easiest path out of ransomware infections.** (Photo courtesy of FBI.)

WTF! FBI Advices:

Just Pay Ransom!

If Hackers
infect your
computer with
Ransomware.





HMC 好萊塢長老教會醫療中心

1. 病例被加密無法作業
2. 醫療系統停止一個多星期
3. 手動作業、掛號、看診
4. 危急病患被迫轉院
5. 贖金9000比特幣(360萬美元)

2016.2.18 執行長Allen Stefanek說明，支付贖金解決問題，並修正僅支付17,000美元



FireEye and Fox-IT have partnered to provide free keys designed to unlock systems infected by [CryptoLocker](#).

Please provide your email address [1] and an encrypted file [2] that has been encrypted by CryptoLocker.

This portal will then email you a master decryption key along with a download link to our [recovery program](#) that can be used together with the master decryption key to repair all encrypted files on your system.

Please note that each infected system will require its own unique master decryption key. So in case you have multiple systems compromised by CryptoLocker, you will need to repeat this procedure per compromised system.

Notes:

[1] Email addresses will not be used for marketing purposes, nor will they be in any way stored by FireEye or Fox-IT.

[2] You should only upload encrypted files that do not contain any sensitive or personally identifiable information.

Email Address

No file selected

Maximum file size: 16MB

By clicking 'Decrypt it!', you consent to our [Terms of Use](#) See our [Privacy Policy](#) for details.

2014年

FireEye &
FOX IT

-
Decrypt
CryptoLocker





DOWNLOAD THE WINDOWS BINARY



ZIP SHA256:
74F57D7F6A34440FD4E9DDB3B47B04E96
A9927199565DE5BFBC015CCEB17BCCC

DOWNLOAD THE PYTHON SCRIPT



ZIP SHA256:

TESLACRYPT DECRYPTION TOOL

The Talos TeslaCrypt Decryption Tool is an open source command line utility for decrypting TeslaCrypt ransomware encrypted files so users' files can be returned to their original state.

TeslaCrypt malware encrypts the victim's files such as photos, videos, documents, saved game files, and demands a ransom from the victim within a time limit. When the victim pays the ransom they can download a decryption key that will restore their files, otherwise they are permanently lost.

Our decryption tool gives the victim the power to decrypt their files themselves, circumventing the ransomware.

[Click here to learn more about the Talos TeslaCrypt Decryption Tool.](#)

***NOTE - ENCRYPTED FILES SHOULD BE BACKED UP BEFORE USING THIS UTILITY. THIS IS A TEST TOOL WHICH IS NOT OFFICIALLY SUPPORTED AND THE USER ASSUMES ALL LIABILITY FOR THE USE OF THE TOOL.**

2015 Cisco - Teslacrypt Decryption Tool

KASPERSKY



RANSOMWARE DECRYPTOR

Are you a [ransomware](#) victim? The National High Tech Crime Unit (NHTCU) of the Netherlands' police, the Netherlands' National Prosecutors Office and Kaspersky Lab, have been working together to fight the [CoinVault](#) and Bitcryptor ransomware campaigns. During our joint investigation we have obtained data that can help you to decrypt the files being held hostage on your PC. We are now able to share a new [decryption application](#) that will automatically decrypt all files for Coinvault and Bitcryptor victims. For more information please see this [how-to guide](#).

We are considering this case as closed. The ransomware authors are arrested and all existing keys have been added to our database.

October 28 update: ALL Coinvault and Bitcryptor keys (14k+) added to the database

April 29 update: 13 decryption keys added to the database

April 17 update: 711 decryption keys added to the database

2015 Kaspersky – CoinVault & Bitcryptor

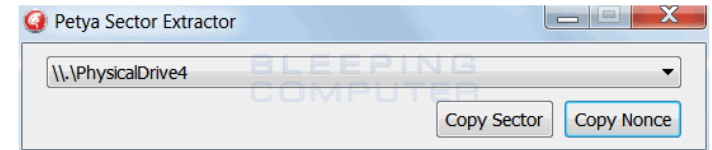
2016 @leostone – Decrypt Petya

Get your petya encrypted disk back, WITHOUT paying ransom!!!

You'll need to grab some bytes from the victim-disk, encode them in Base64 and paste the two strings in the form fields. [Tweet](#)

Base64 encoded **512 bytes** verification data
Location on victim-disk: sector 55 (0x37) offset 0(0x0)

Base64 encoded **8 bytes** nonce
Location on victim-disk: sector 54 (0x36) offset 33(0x21)



Petya Sector Extractor

2016 Fabian Wosar–Petya Sector Extractor



自我防護

如果只有防毒



自我防護

沙箱技術的目的

已知威脅

未知威脅

FW/VPN

AV

"Block or Allow"

"It matches the pattern"

PKI

IDS / IPS

UTM

"No key, no access"

NAC

Application Control

Sandboxing

"Captive Portal"

"Fix the Firewall"

"Detect the Unknown"

備份

黃金法則



Thank You

謝謝



麟雲資訊
Ring Cloud Technology