麟雲資訊
Ring Cloud Technology

XX大學
加密勒索軟體應有的認知

大 綱

- 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

加密勒索軟體

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

2005年 由俄羅斯開始

2012年

Police Ransomeware

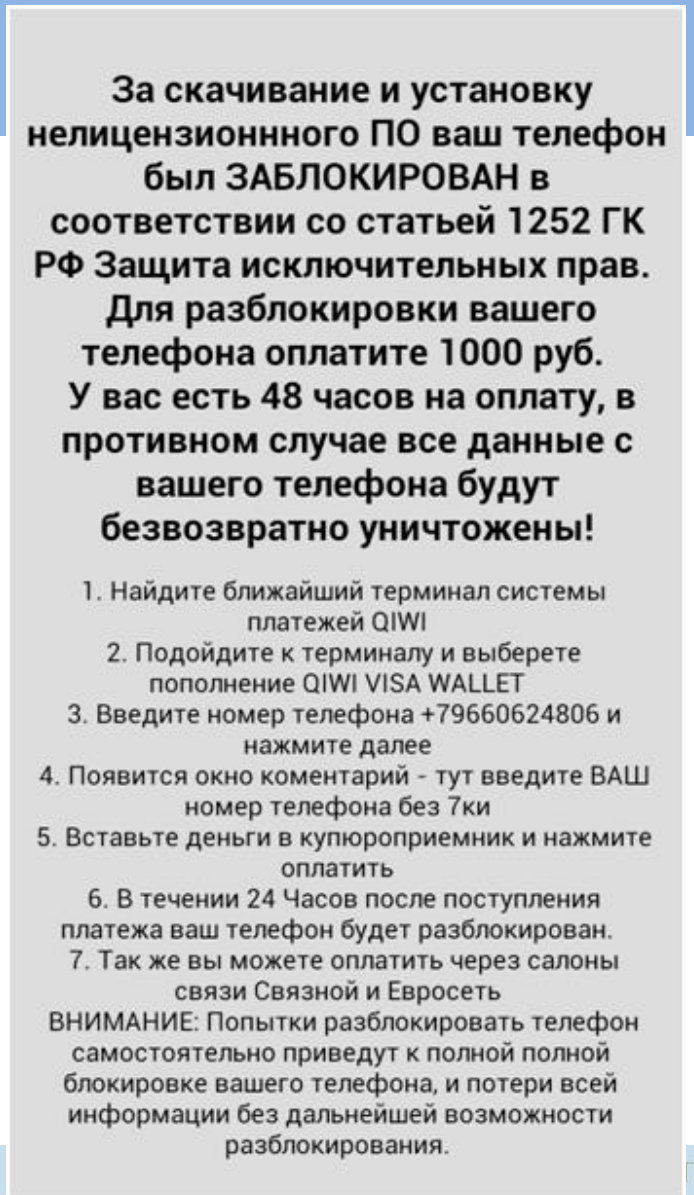
2013年

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

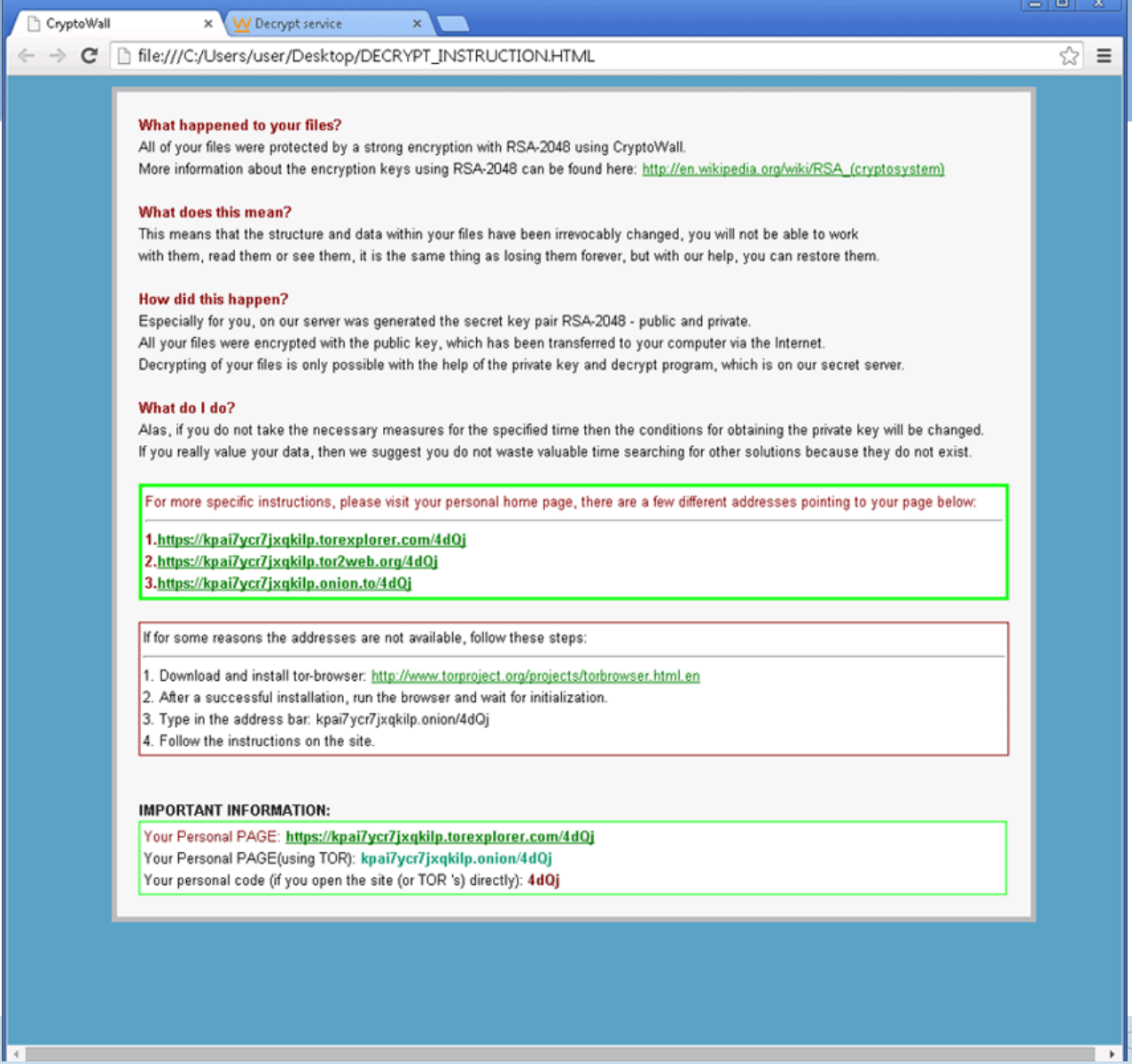
Android 勒索軟體



因為下載和安裝軟體nelitsenzionnnogo，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

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
- btcdirect.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
- bittylicious.com

4. Send - 0.5 BTC to Bitcoin address:

5. Refresh the page and download decoder.

2016

Locky

README_FOR_DECRYPT.txt

Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to [redacted](IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN THIS LINK: [redacted])
2. Use [redacted] as your ID for authentication
3. Pay 1 BTC (~410.63$) for decryption pack using bitcoins (wallet is your ID for authentication - [redacted])
4. Download decrypt pack and run

---> Also at [redacted] you can decrypt 1 file for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)

2016 KeyRanger


PETYA RANSOMWARE - St...
Search
PETYA
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 completly!
There are a lot of wrong informations online. If you are looking for reliable informations, please visit
16.12.2015
Petya launched
Today we launched the Petya Ransomware Project.

勒索

報警？

勒索

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

解密

創意的加密組合

AES + RSA

(對稱) (非對稱)

解密

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.)

解密

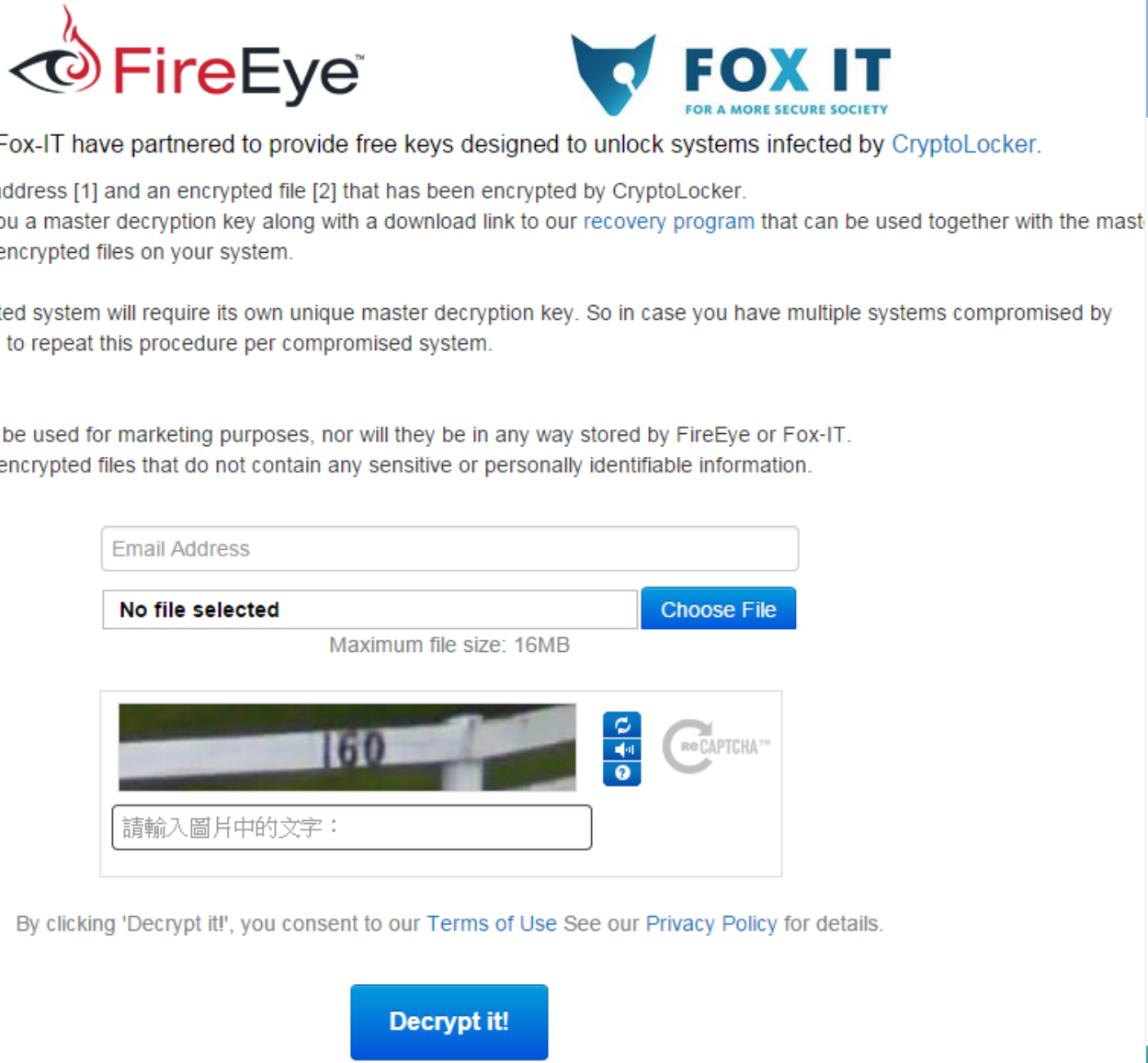

WTF! FBI Advices:
Just Pay Ransom!
If Hackers
infect your
computer with
Ransomware.

解密

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



2014年

FireEye & FOX IT

- Decrypt CryptoLocker

解密

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

解密

KASPERSKY lab

POLITIE

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

解密

2016 @leostone – Decrypt Petya

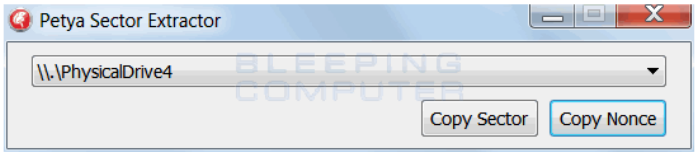
Get your petya encrypted disk back, WITHOUT paying ransom!!!

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)

Submit



Petya Sector Extractor

2016 Fabian Wosar–Petya Sector Extractor

自 我 防 護

Anti virus

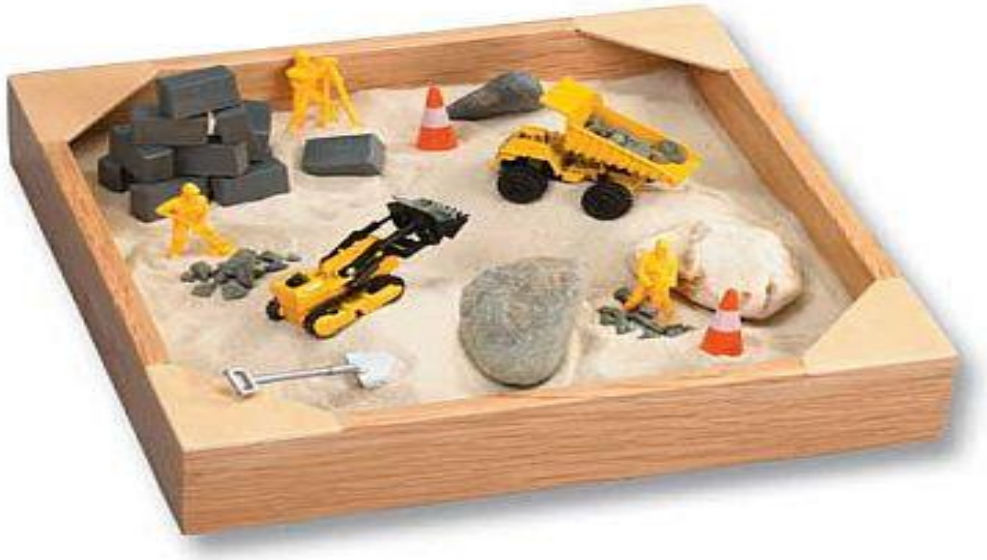
自 我 防 護

如果只有防毒

Anti virus

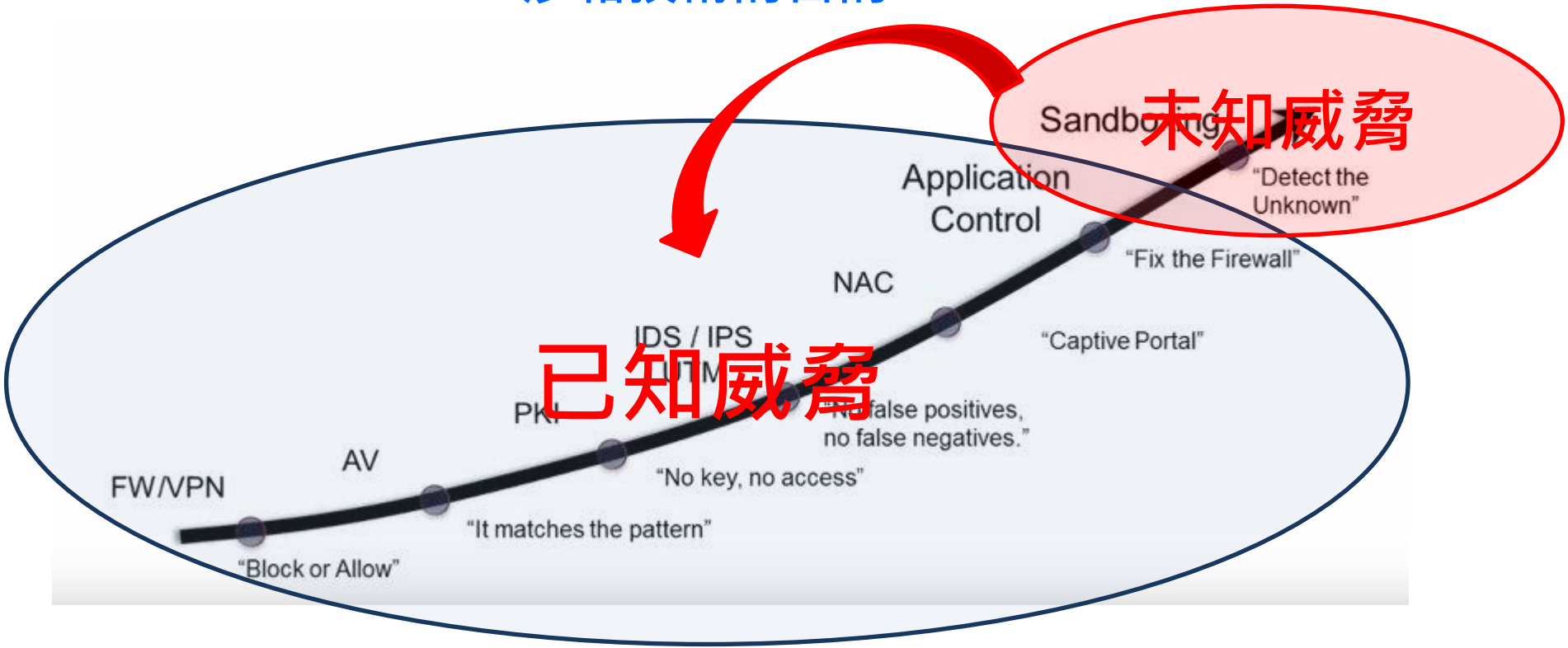
自 我 防 護

防毒廠商的秘密武器



自 我 防 護

沙箱技術的目的



備 份

黃金法則


CREATE
3
copies of your data
1 primary copy &
2 backups
STORE
2
copies of your data
on different
storage media
KEEP
1
copy of your data
offsite

Thank You

謝謝

麟雲資訊
Ring Cloud Technology