

# 企業資安防禦的生存奧義

Birdman / chroot / 2015



# 前言



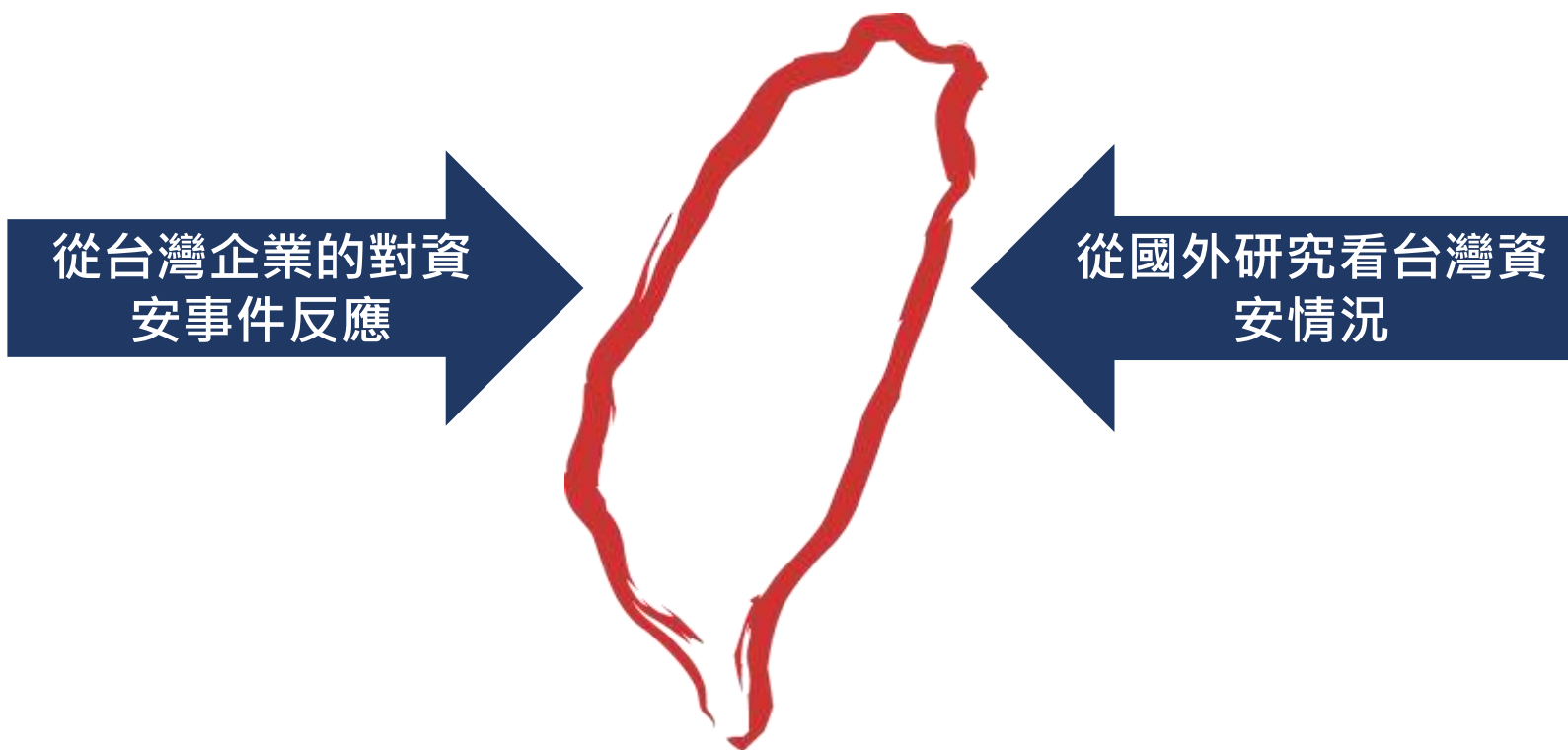
曾發表很多資安研究在 HITCON, SYSCAN, DEFCON, BLACKHAT, OWASP, AVTOKYO, HTCIA

是一個很強的男人

這場設定是給有心改革資安環境的企業資訊主管，其內容主要由是我多年的觀察，資安從業的心得，也包含幾位在資安打滾多年的朋友的意見，是茶餘飯後打屁所整理而成。

本場次技術含量不高，沒有高深駭客招式展示，但是卻是少見探討企業資安武功心法Talk，看看沒錢沒人怎麼做資安？

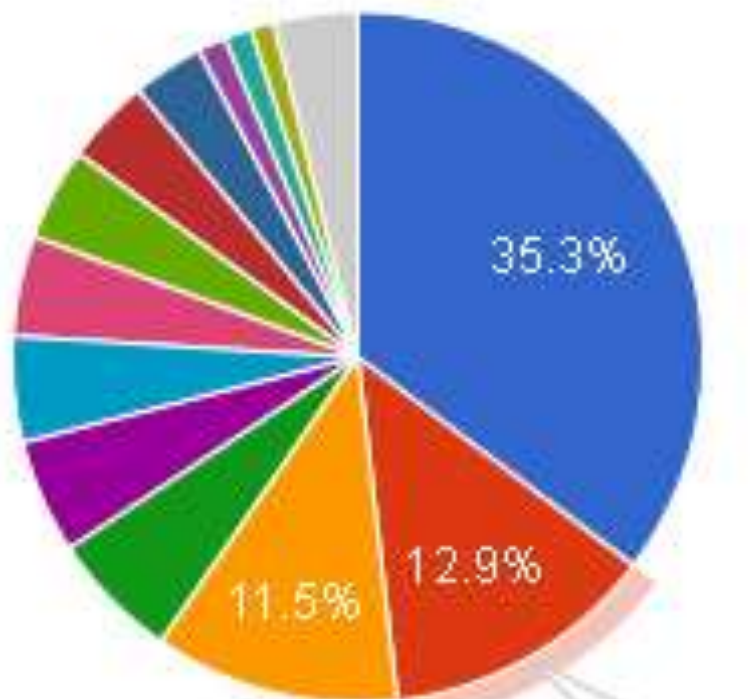
# 要怎麼看我們資安現況



# 從國外看我們資安現況

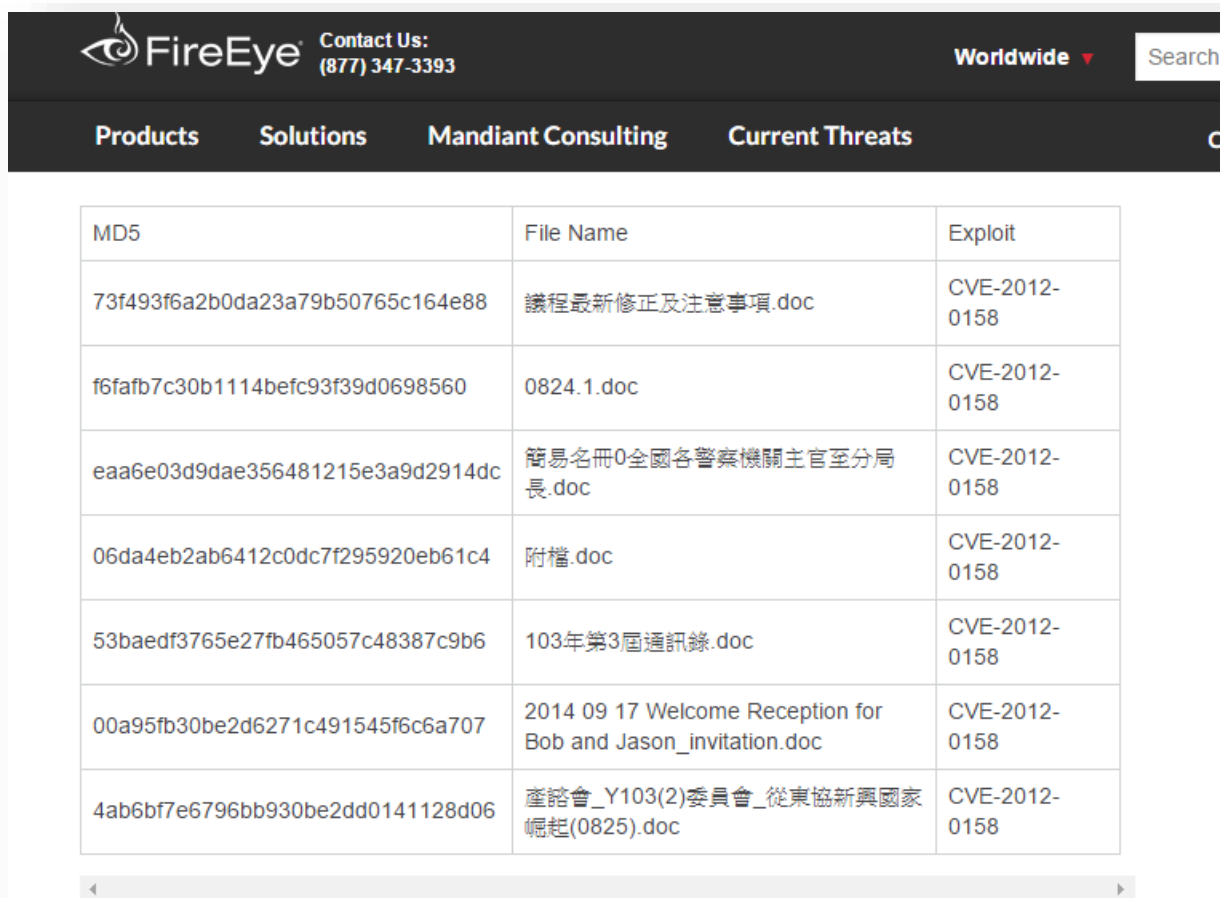
Submissions by country

VirusTotal



Taiwan (12.9%)

# 從國外看我們資安現況



The screenshot shows the FireEye website header with the logo, contact information (877) 347-3393, and a search bar. Below the header is a navigation bar with links to Products, Solutions, Mandiant Consulting, and Current Threats. The main content area displays a table of identified exploit documents for HIGHTIDE. The table has three columns: MD5, File Name, and Exploit. There are eight rows of data, each representing a different exploit document. The documents are listed in descending order of their MD5 hash values.

MD5	File Name	Exploit
73f493f6a2b0da23a79b50765c164e88	議程最新修正及注意事項.doc	CVE-2012-0158
f6fafb7c30b1114befc93f39d0698560	0824.1.doc	CVE-2012-0158
eea6e03d9dae356481215e3a9d2914dc	簡易名冊0全國各警察機關主官至分局長.doc	CVE-2012-0158
06da4eb2ab6412c0dc7f295920eb61c4	附檔.doc	CVE-2012-0158
53baedf3765e27fb465057c48387c9b6	103年第3屆通訊錄.doc	CVE-2012-0158
00a95fb30be2d6271c491545f6c6a707	2014 09 17 Welcome Reception for Bob and Jason_invitation.doc	CVE-2012-0158
4ab6bf7e6796bb930be2dd0141128d06	產諮會_Y103(2)委員會_從東協新興國家崛起(0825).doc	CVE-2012-0158

**Figure 4: Identified exploit documents for HIGHTIDE**

When the file is opened, it drops HIGHTIDE in the form of an executable file onto the infected system.

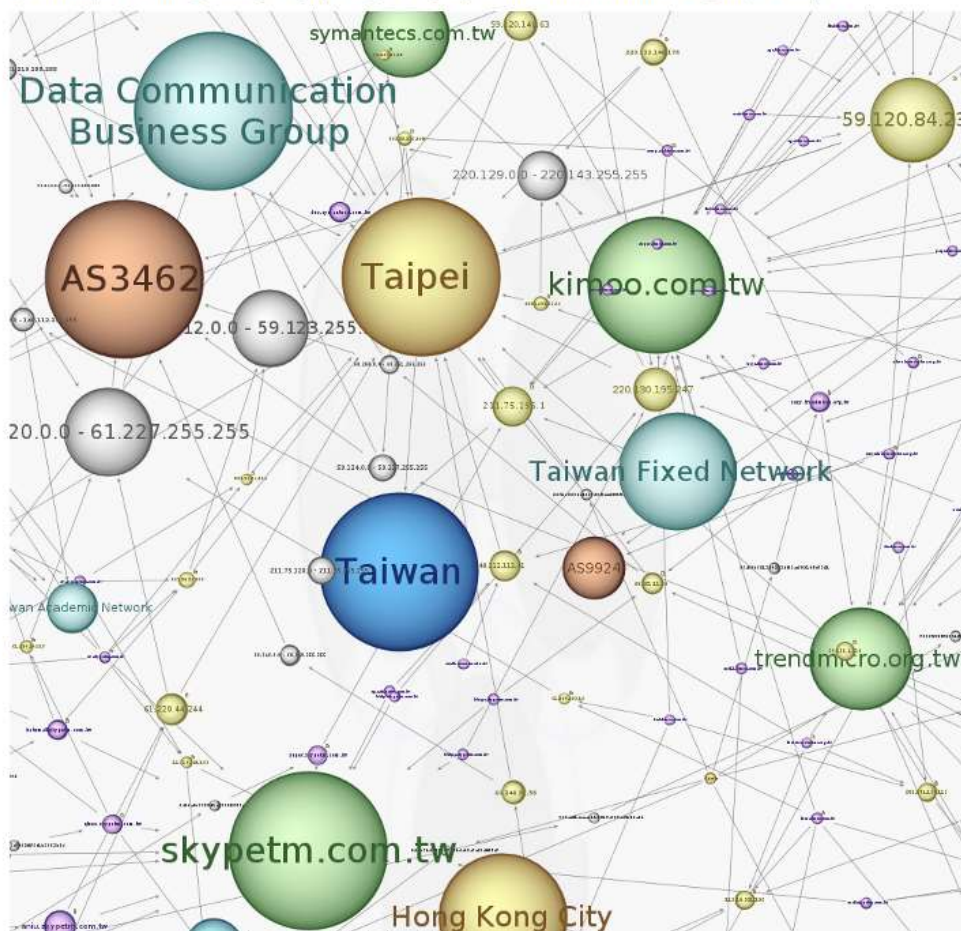
RIPTIDE and HIGHTIDE differ on several points: executable file location, image base address, the User-Agent within the GET requests, and the format of the URI. The RIPTIDE exploit document drops its executable file into the C:\Documents and Settings\{user}\Application Data\Location folder while the HIGHTIDE exploit document drops its executable file into the C:\DOCUMENTS and SETTINGS\{user}\LOCAL SETTINGS\Temp\ folder. All but one sample that we identified were written to this folder



# 從國外看我們資安現況

- Two of the used RATs have been developed by the same developers: CT RAT and PittyTiger RAT. The controllers for these RATs show Chinese language;
- Several binaries used by the attackers show either "Chinese - China" or "Chinese-Taiwan" language ID in their resources;
- A decoy Word document has been found, written in Chinese language;

The IP addresses used for the hosting of the c&c domains are mainly located in Taipei (Taiwan) and Hong Kong City (Hong Kong Special Administrative Region, PRC):



# 從國外看我們資安現況



# 從國外看我們資安現況

## 前美國五角大廈資安官：臺灣是亞洲第2大APT重災區

2014下半年臺灣遭APT威脅中，逾2成攻擊鎖定醫療和政府機構，反映出臺灣近年來已成為駭客入侵滲透的首要目標

文/ 余至浩 | 2015-04-14 發表



1.4 萬

按讚加入iThome粉絲團



分享

546



8+1

12



前美國五角大廈資安官、FireEye副總裁暨全球政府業務部門技術長Tony Cole近日來臺時表示，面對日益猖獗的網路攻擊事件頻傳，圖片來源: iThome臺灣政府應協助企業及政府單位建立一套自動通報的分享機制，加快攻擊情報的傳遞分享。



# 不能說的秘密

## The Impact Team

2015年8月20日 星期四

**The government of Taiwan is waiting**

*Waiting for us, in February 18th, announced Taiwan the corruption of 90GB*

ASH  
**MADISON**<sup>®</sup>  
Life is short. Have an affair.<sup>®</sup>

Get started by telling us your relationship status:

Please Select

**See Your Matches »**

Over **32,875,000** anonymous members!



**我們不得不承認，情況沒有比較好**

# 現在已進入紙本作業的高峰期

## 綠危機總動員 改採紙本作業

中時 電子報  
chinatimes.com

作者：管嫻媛、楊舒媚／台北報導 | 中時電子報 - 2015年6月21日 上午5:50



民進黨決定重要文件不再用網路傳遞。圖為中央黨部進行反偷拍檢測。（本報資料照片）

中國時報【管嫻媛、楊舒媚／台北報導】

民進黨2016總統參選人蔡英文訪美期間，「家裡」遭「入侵」，黨內包括祕書長吳釗燮等諸多重要幹部電子信箱、通訊軟體遭駭，甚至連黨的雲端硬碟都被入侵。為「保密防諜」，民進黨試了許多方式，但最後發現，最古老方式就是最安全的方法，因此，然處於高科技年代，但重要文件反倒要恢復土法煉鋼的「紙本」作業，且必須「面交」。

# 再談談一個現象～勒索軟體

## 加密勒索軟體散播到新地區,台灣列入歐美以外最受影響的國家

POSTED ON 2015 年 03 月 02 日 BY TREND LABS 趨勢科技全球技術支援與研發中心



個視窗要求使用者存取CryptoWall解密服務並支付贖金，首次要求的贖金為200美元，而且會隨著時間加碼，並允許使用者以比特幣支付贖金。CTU指出，他們發現有一案例是使用者支付了1萬美元來解救他的檔案。

有不少地方政府或部門的重要文件，被勒索軟體加密，為了取回加密文件，平均支付400歐元的贖金。像是，義大利地方政府的安全數位鑑識委員會諮詢小組已經在10月中，員工被迫支付400歐元（約1.4個比特幣）以取回被惡意程

在英國，則有2,300臺電腦受駭，超過3千萬檔案文件被加密，主要鎖定中小企業，而支付贖金的約有210人，平均支付400英鎊～650英鎊之間。不過，若在駭客規定的付款期限內（平均2～4天）支付贖金的話，竟然還打5折。顯



# 我們常常被廠商跟媒體恐嚇

國家級APT駭客攻擊

Banking Trojan

中間人攻擊

網站被 SQL Injection

有人踢到Server電源線

勒索軟體

零時差攻擊

員工竊取機密文件

水坑式攻擊

非授權存取

客戶個資外洩

DDoS 攻擊

帳號被盜用

公司內網被Worm 攻擊

手機惡意軟體

USB 惡意程式

# 你不是膽子大嗎？

聽完廠商的話後...

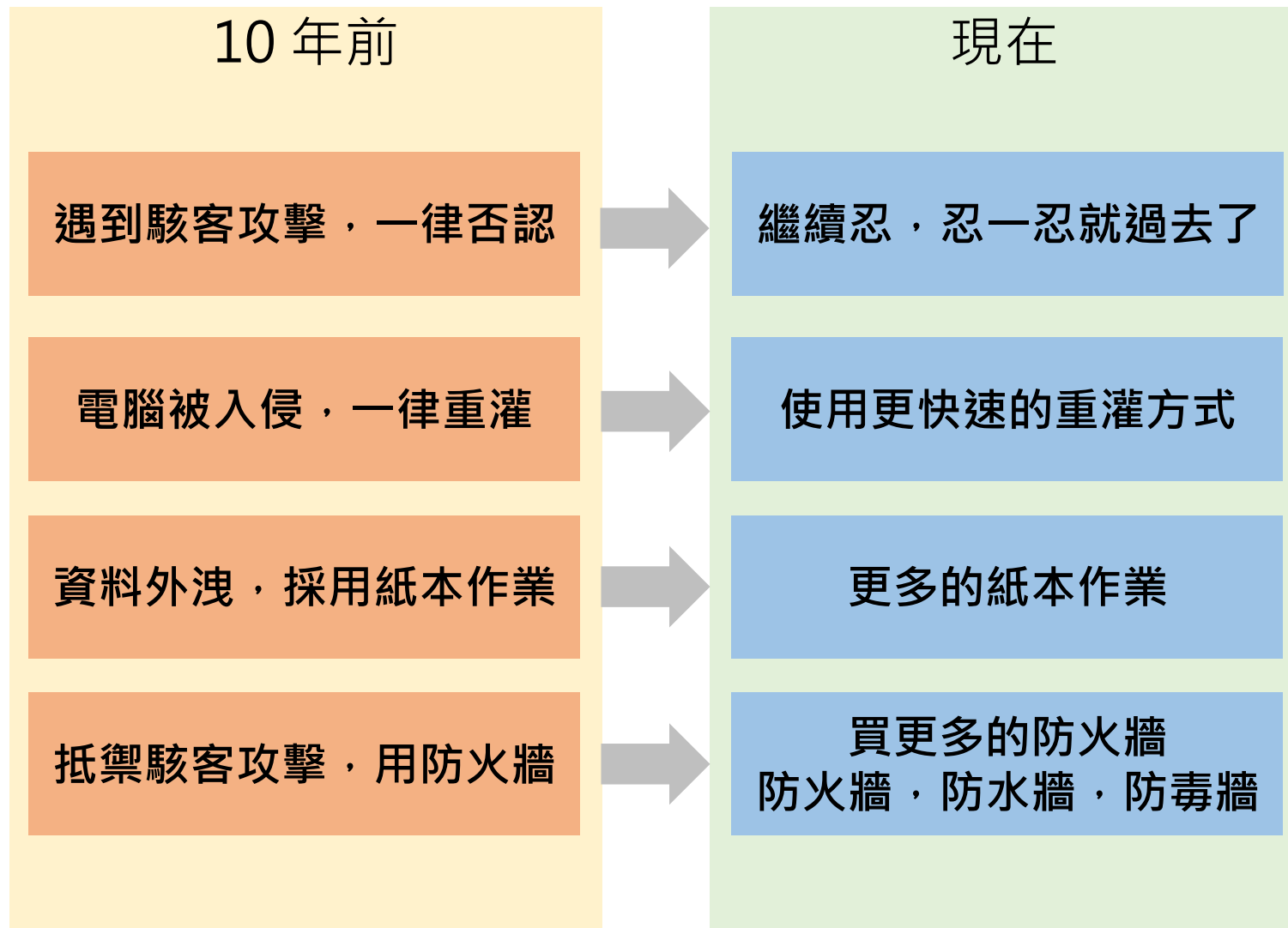
為甚麼你要處理，那摸著不邊際攻擊，看不見的敵人？

對抗外星人攻擊，交給吉姆雷諾 就好了，輪不到你



圖片來源: 暴雪娛樂, 星海爭霸

# 我們的態度真的有進步嗎？





那我們怎麼做才好



# 你的威脅來源

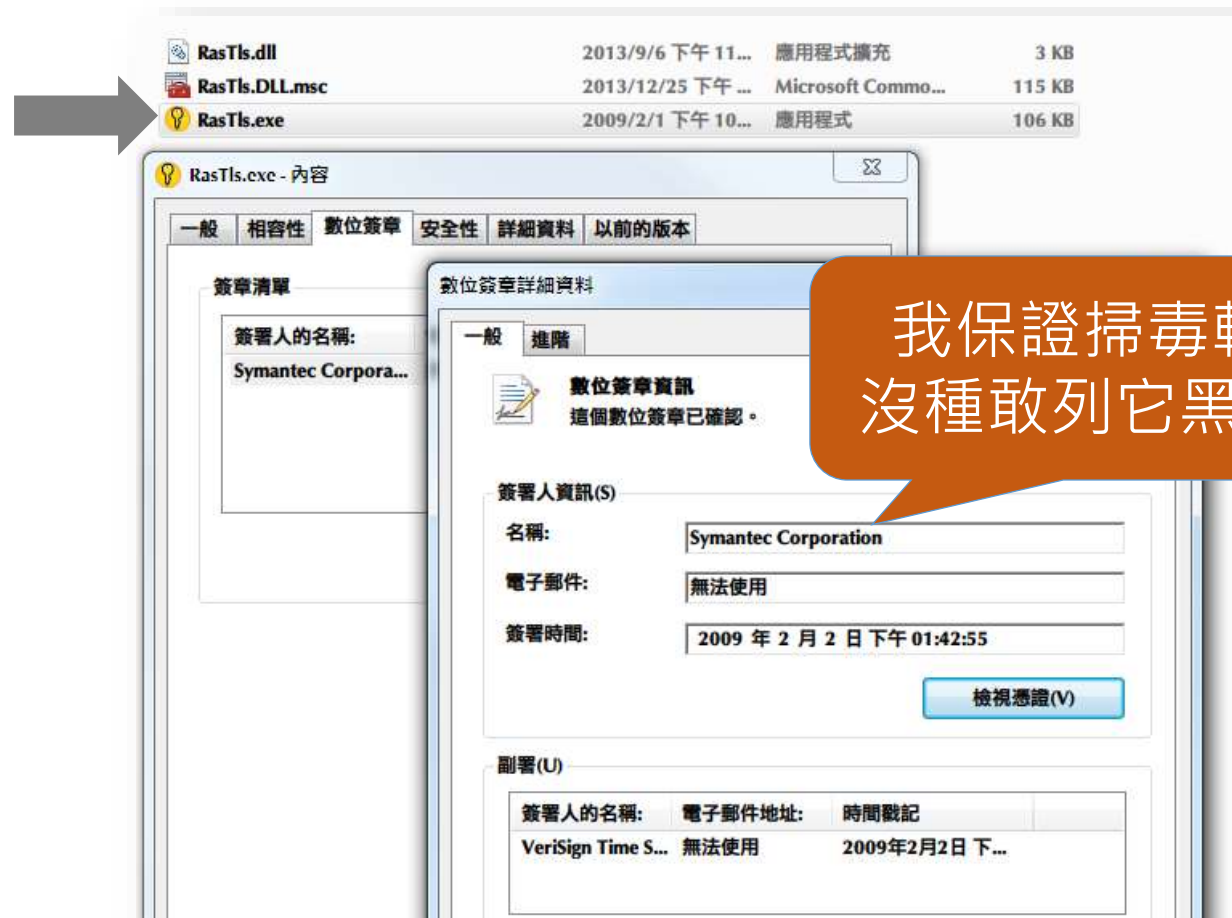


這是個改編過的真人真事...



# 怎麼會這樣？

- 我不是有裝掃毒軟體，而且每日更新 !?
- 結果惡意程式都是有數位簽章...這叫人情何以堪





# 更扯的是

- 有時候，你怎麼都找不到惡意程式的原因是...  
駭客根本不需要裝就能開後門

Index	Score	Type	File Name	Company	Type	Size (KB)	Create Time	Write Time
<input type="checkbox"/> 1	1200		C:\WINDOWS\PSEXESVC.exe	Sysinternals	EXE	185	2014-06-10 1...	2014-06-10 1...
<input type="checkbox"/> 2	1580	Suspicious	C:\WINDOWS\system32\sethc.exe	Microsoft Corporation	EXE	461	2010-07-07 0...	2007-02-17 0...
<input type="checkbox"/> 3	250		C:\WINDOWS\system32\drivers\arcsas.sys	Adaptec, Inc.	SYS	52	2009-06-15 1...	2009-06-15 1...
<input type="checkbox"/> 4	300		C:\WINDOWS\system32\sa-inspect-9556.exe	IBM Corporation	EXE	44	2009-06-15 1...	2006-02-07 1...
<input type="checkbox"/> 5	310		C:\Documents and Settings\Administrator\Local Setti...		EXE	40	2005-06-29 0...	2005-06-29 0...
<input type="checkbox"/> 6	300		C:\Documents and Settings\Administrator\Local Setti...		EXE	44	2005-06-29 0...	2005-06-29 0...
<input type="checkbox"/> 7	890		D:\TrustView\TrustServer\tomcat\bin\tomcat5.exe	Apache Software Foundation	EXE	92	2009-06-15 1...	2004-05-04 2...
<input type="checkbox"/> 8	270		C:\WINDOWS\$\NtServicePackUninstall\$\wmperfmon...	Microsoft Corporation	EXE	99	2009-06-15 1...	2005-03-24 1...
<input type="checkbox"/> 9	180		C:\Program Files\Common Files\InstallShield\engine\6\...	InstallShield Software Corp...	EXE	596	2009-06-15 1...	2009-06-15 1...



SHA256: c60009b5c0c49f055d2427099e236f9f1066666cc0f04c0a0b04b103a04b

File name: cmd

Detection ratio: 0 / 52

Analysis date: 2014-05-28 02:25:01 UTC ( 2 weeks, 8 days ago )

Analysis [File detail](#) [Additional information](#) [Comments](#) [Votes](#)

Antivirus	Result	Update
AVG		20140527
Ad-Aware		20140528
Avira		20140528
Avast		20140527
Avast-UI		20140527
Avast-UI		20140528
Avast-UI		20140528
Avast		20140528

## Copyright

© Microsoft Corporation. All rights reserved.

## Publisher

Microsoft Corporation

## Product

Microsoft® Windows® Operating System

## Original name

Cmd.Exe

## Internal name

cmd

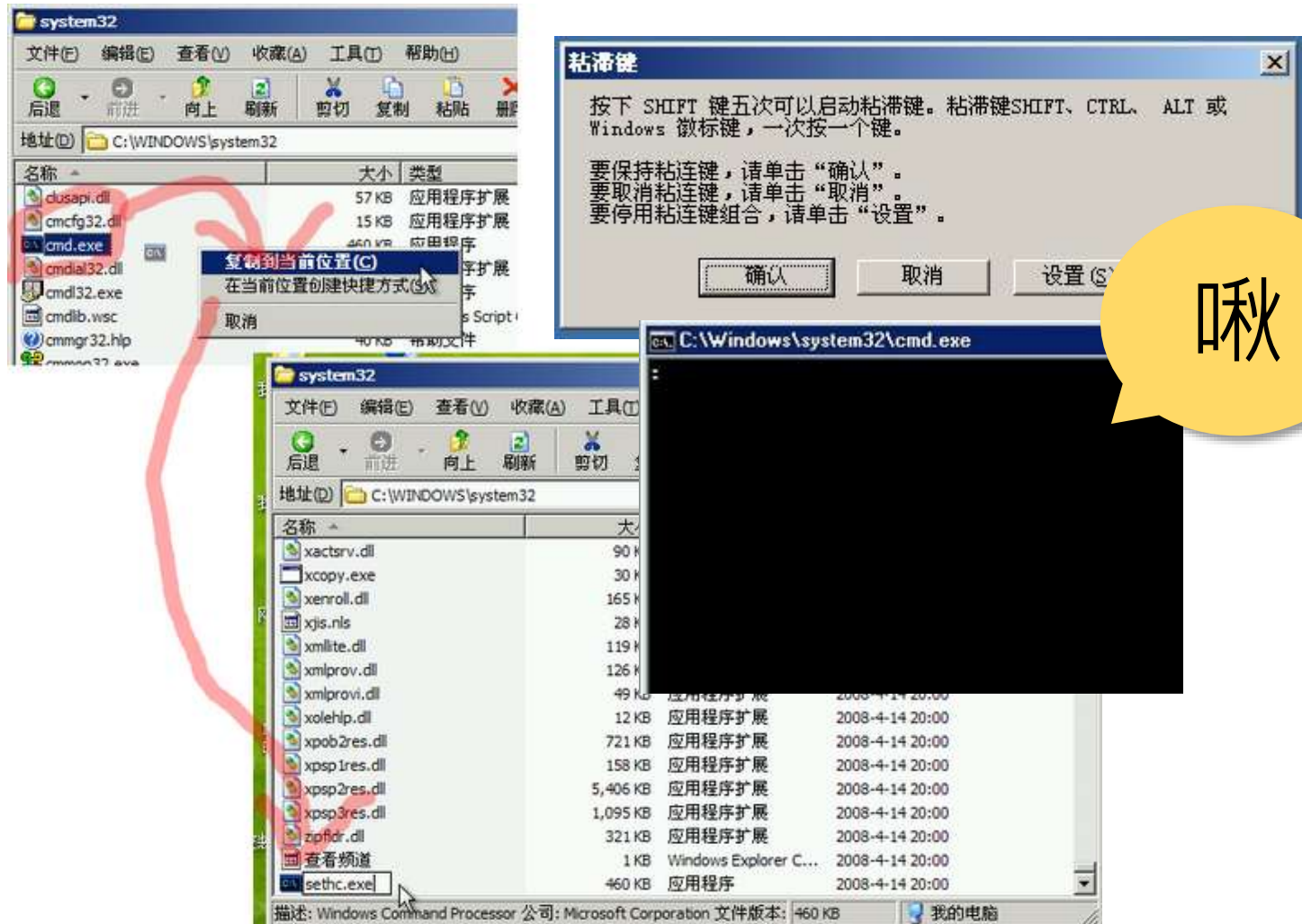
## File version

5.2.3790.3959 (srv03\_sp2\_rtm.070216-1710)

## Description

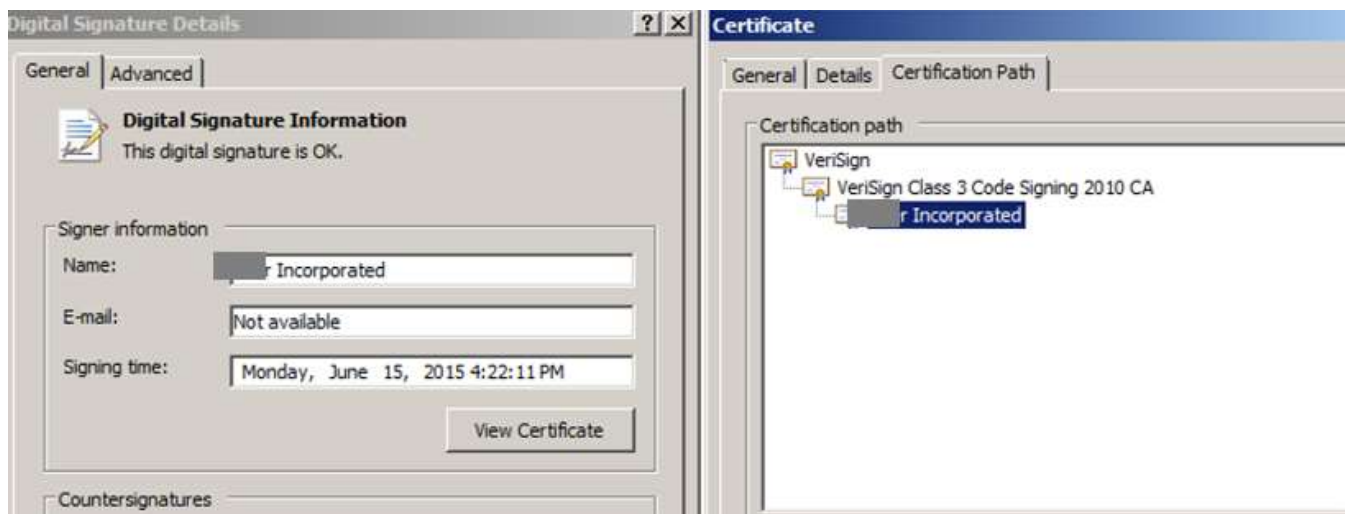
Windows Command Processor

# 簡單就可以繞過你防禦系統 (replace cmd.exe with sethc.exe)



# 有些事情很可怕，是資安廠商不敢說的秘密...

- 資安公司被APT駭客入侵的情況，比你想像中嚴重



- 資產管理系統與掃毒軟體，被駭客破解、利用的慘況比你想像中可怕...

# 小結：你該警覺的威脅趨勢

- 駭客的程式已經開始使用偷來的數位簽章
- 駭客的網路傳輸已經使用常見合法的 Cloud Service (Dropbox, Google...)，並且採用 HTTPS加密
- 在AD環境下，駭客常常使用 **PtH** 攻擊，根本就不需要暴力破解你的密碼
- 資產管理系統與掃毒軟體系統，被駭客入侵是常見



# 資安防禦思維的轉變



# 資安防禦思維的轉變

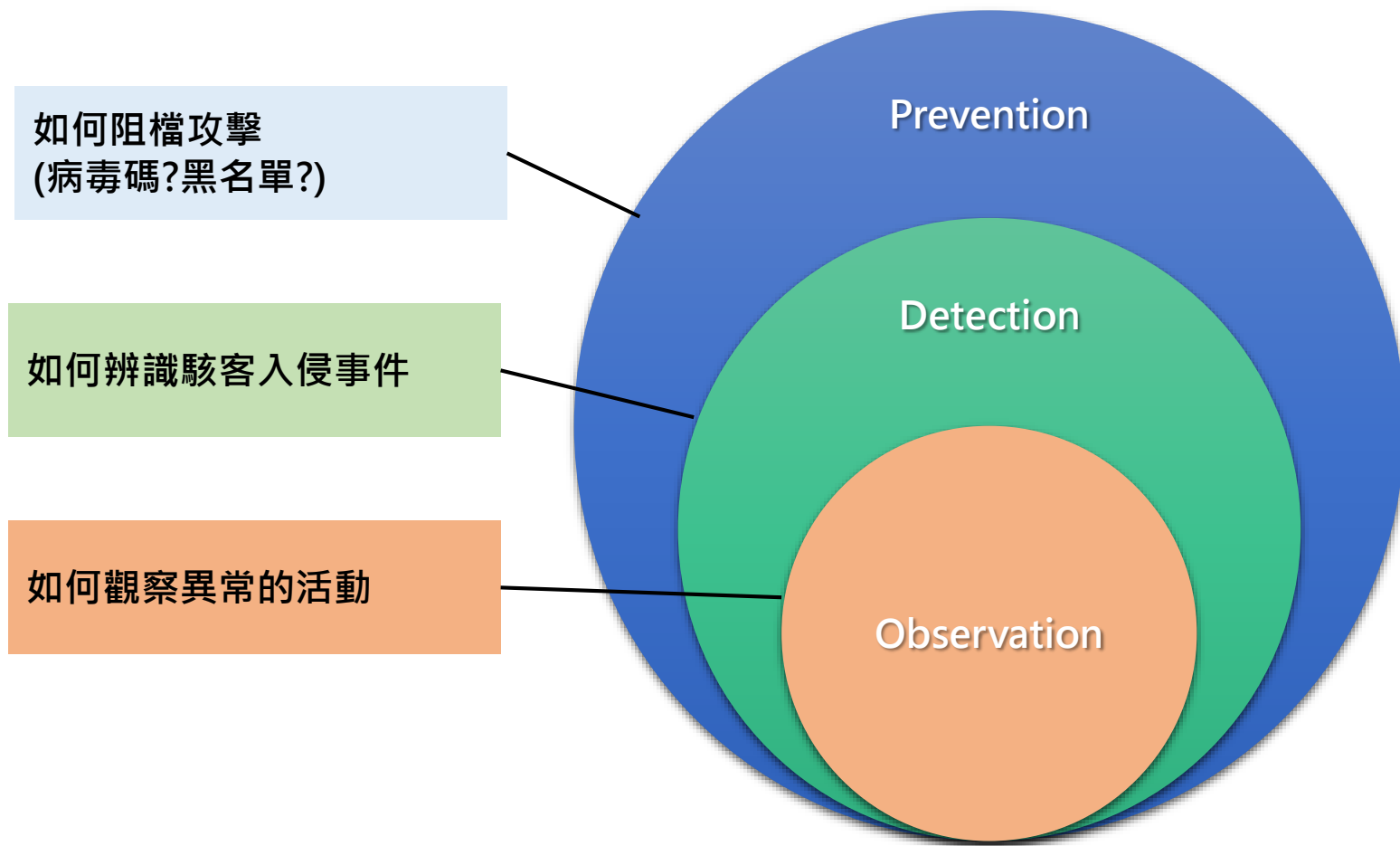
## 建構你自己的防禦體系

- 買你會用的工具，不會用的不要買，反正忍一忍就過去了
- 沒有一個廠商的防禦架構 100%適合你，思考自己的需要
- 資安/IT 委外，不表示責任委外

## 用應變取代阻擋

- 如同地震演習一樣，我們無法阻擋發生，只要有應變計劃並時常演練，還是可以降低損害
- 舉例來說：如果AD Admin權限被駭客拿下，你該怎麼辦？
- 你建立自己公司的應變團隊，積極地面對資安事件，並準備下次攻擊的到來

# 情資導向的資安防禦模型



# 檢視你自己的資安防禦能量

- 是否架構了正確的資安防禦模型

- 如何阻擋駭客攻擊
- 如何發現潛伏惡意程式
- 如何發現內網駭客活動
- 如何分析駭客的攻擊手法、武器與意圖

- 是否評估資安體系應變的時間成本

- 辨識一個已知惡意檔案，需要多久時間
- 辨識一個新的惡意檔案，需要多久時間
- 偵測駭客活動需要多久時間
- 處理被入侵電腦，需要多少時間
- 攻擊情資回進饋進防禦體系，需要多少時間



# 每個人心中都有奧義！

- 1 不急著買產品，先認識新的手法與威脅，學習識別攻擊的方式
- 2 檢討並分析單位歷年來所發生的資安事件，並蒐集識別的方法 (Indicator)
- 3 建置自動化觀察與偵測體系，並確保能夠涵蓋 [2] 的 Indicator
- 4 建立資安事件應變流程 SOP，建立團隊，處理完畢後回饋到 [1], [2], [3]
- 5 依據 [4] 報告檢討，並調整 IT 架構以因應資安需求
- 6 使用資安產品與服務，將資安事件偵測與應變自動化 [4]
- 7 最佳化 [ 3, 4, 5, 6] 反應時間，強化自動防禦能量

不要放棄治療

你還有救！