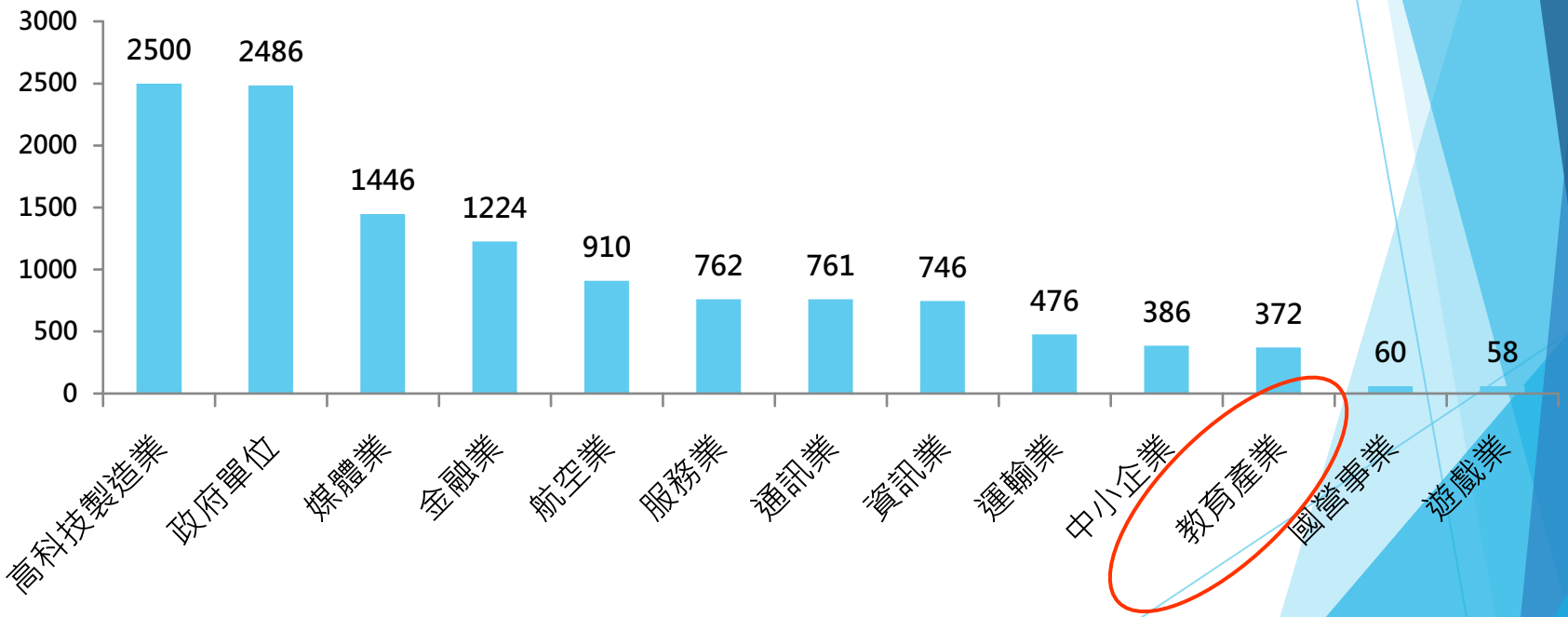
2018
挖礦勒索的興起，該如何自保

Agenda

- 引言
- 資安威脅趨勢
- 挖礦興起
- 勒索攻擊再進化
- 入侵事件的反思
- 如何因應與面對
- Q&A

台灣各產業面臨嚴峻的駭客入侵資安威脅

- 趨勢科技共調查413個駭客入侵案件，檢查2267台電腦
- 前三名受駭嚴重產業：高科技製造業、政府機關、媒體業，其中高科技製造業可能被駭客入侵後2500天才發現異常狀況，進行處理

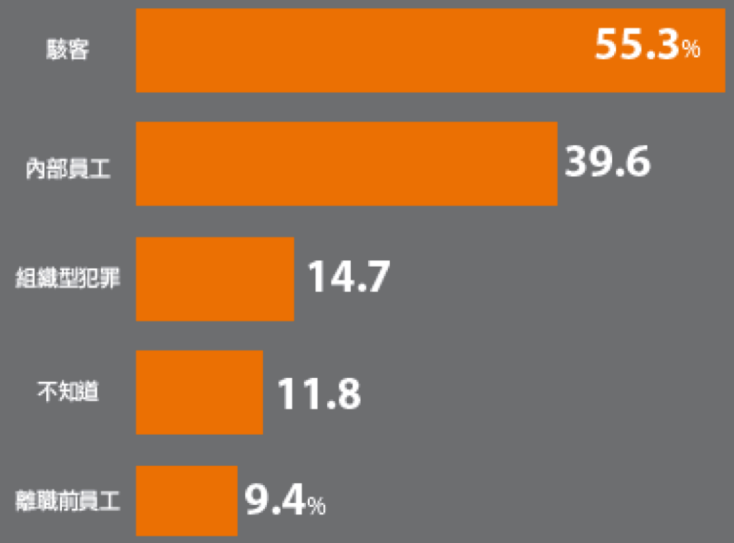


資安大調查：資安事件衝擊

員工資安意識不足的威脅，比駭客更大

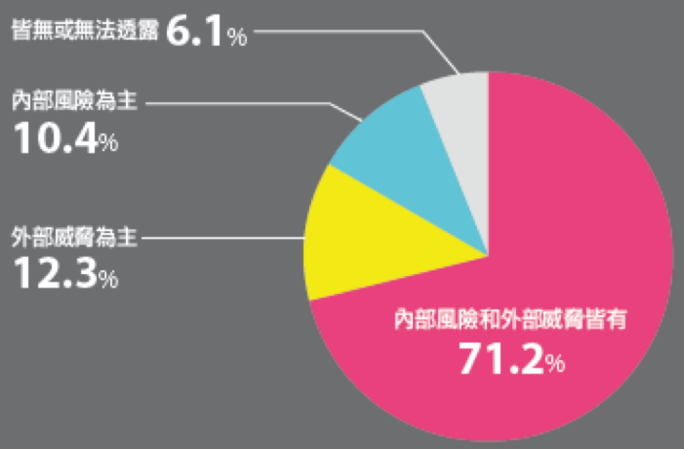
2017 年資安事件 5 大主要攻擊來源

過半數災情源自駭客，但 4 成企業也遭內部員工攻擊

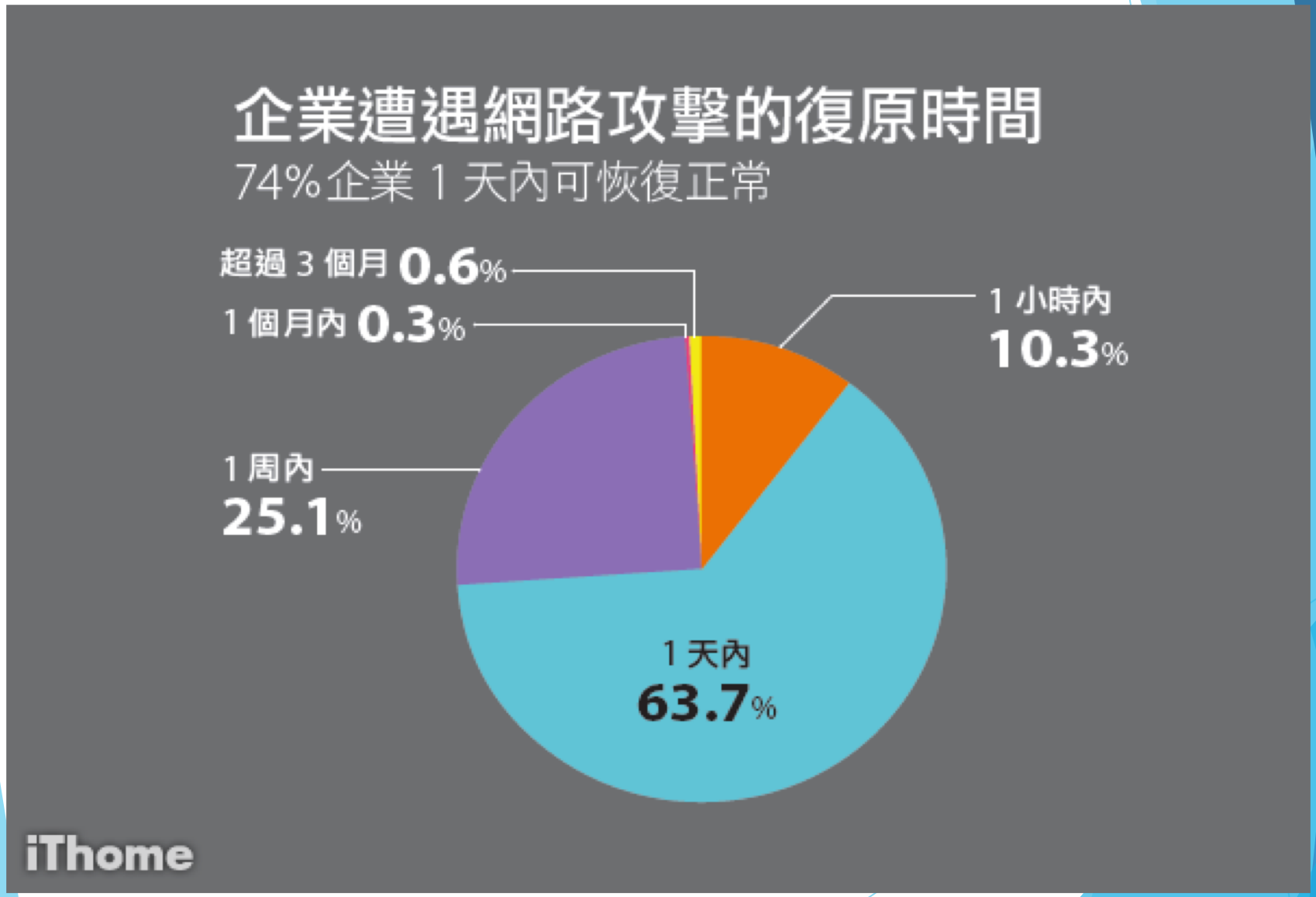


7 成企業同時面臨內部風險和外部威脅

12.3% 企業主要資安風險是外部威脅

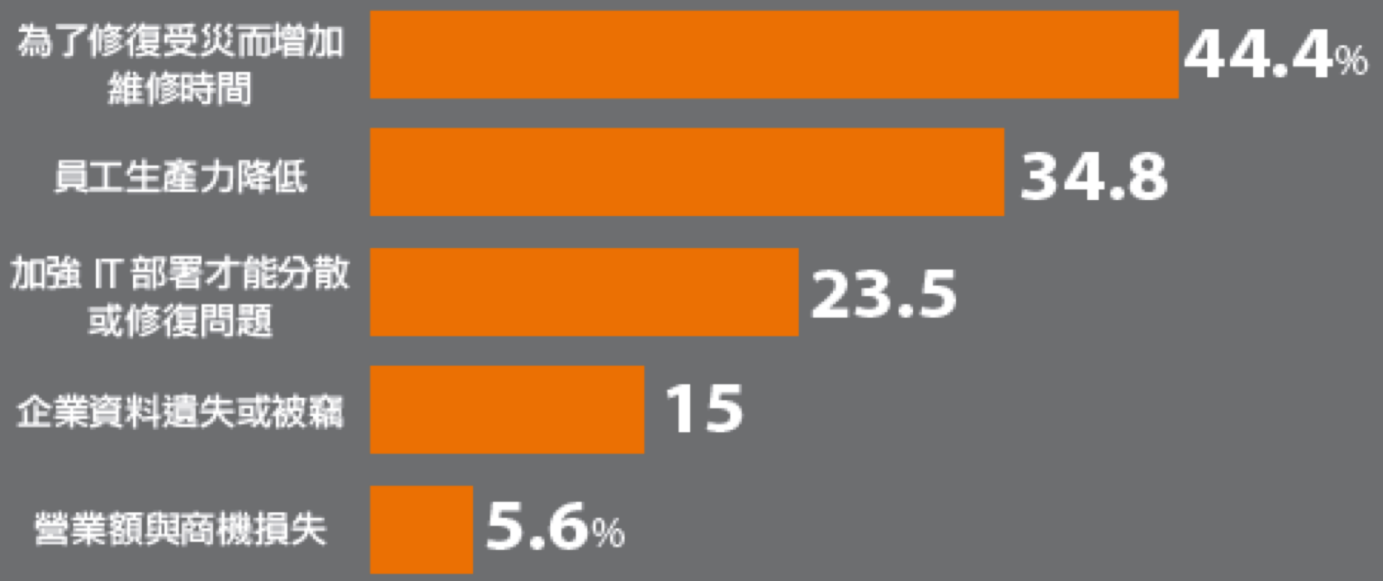


資安事件衝擊


企業遭遇網路攻擊的復原時間
74%企業 1 天內可恢復正常
超過 3 個月 0.6%
1 個月內 0.3%
1 小時內
10.3%
1 周內
25.1%
1 天內
63.7%
iThome

2017 年資安事件 5 大企業損失

4 成企業增加維修時間，3 成企業員工生產力降低



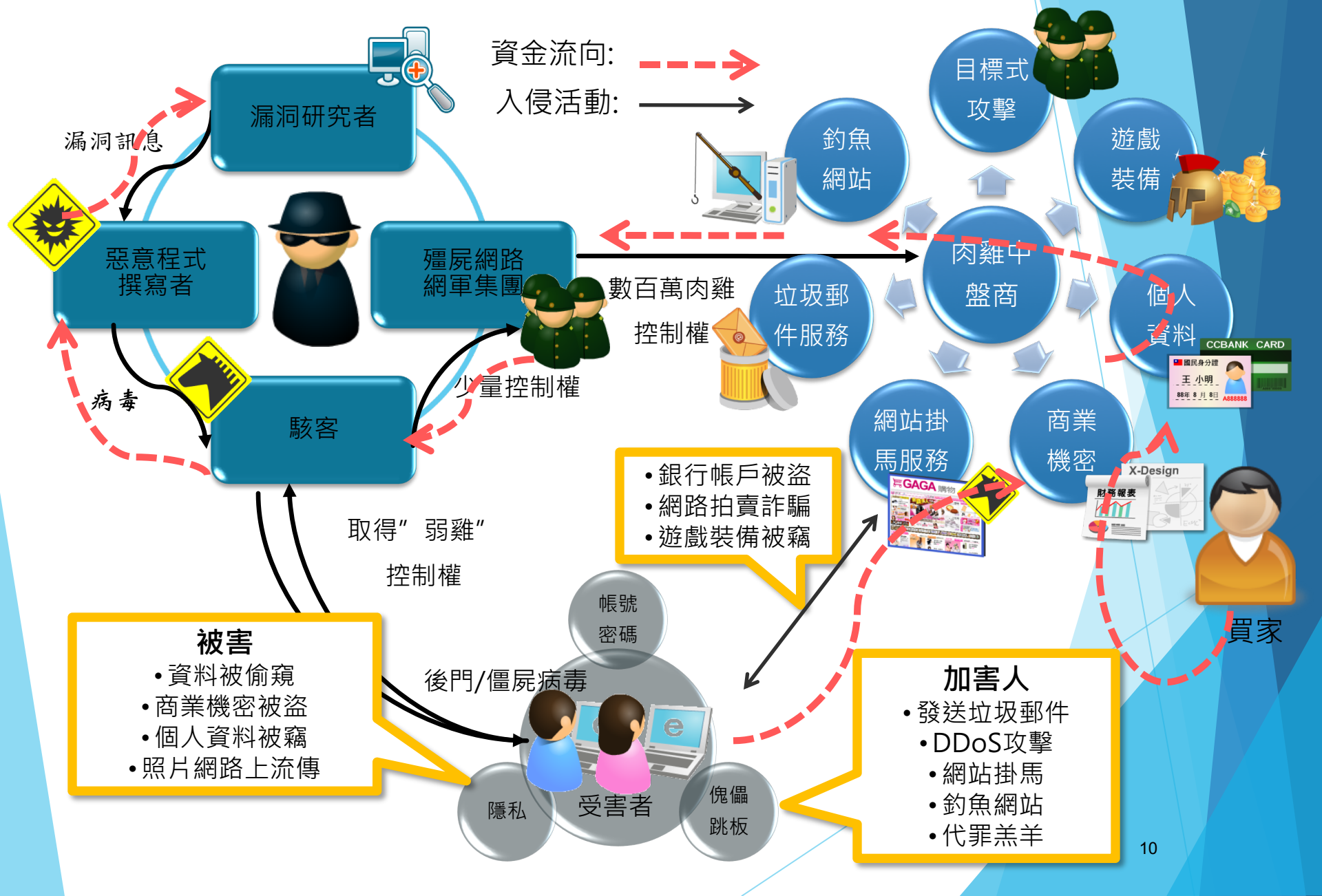
iThome


2018 臺灣企業面臨的十大資安風險
員工疏忽、缺乏資安意識是多數企業最在意的資安風險
員工疏忽、欠缺資安意識
56.7%
釣魚郵件
50.8
惡意程式
46.3
勒索軟體
45.2
垃圾郵件
35.0
使用行動裝置
23.0
過時的資安控管與架構
19.0
可能遭攻擊或破壞的潛在弱點
18.7
軟體更新
17.6
IT 人員的安全開發能力不足
15.5%
iThome

Agenda

- 引言
- 資安威脅趨勢
- 挖礦興起
- 勒索攻擊再進化
- 入侵事件的反思
- 如何因應與面對
- Q&A

黑色產業鏈


資金流向:
入侵活動:
漏洞研究者
漏洞訊息
惡意程式撰寫者
殭屍網路網軍集團
駭客
病毒
數百萬肉雞控制權
少量控制權
取得”弱雞”控制權
釣魚網站
目標式攻擊
遊戲裝備
肉雞中盤商
垃圾郵件服務
個人資料
網站掛馬服務
商業機密
買家
帳號密碼
後門/僵屍病毒
隱私
受害者
傀儡跳板
• 銀行帳戶被盜
• 網路拍賣詐騙
• 遊戲裝備被竊
被害
• 資料被偷窺
• 商業機密被盜
• 個人資料被竊
• 照片網路上流傳
加害人
• 發送垃圾郵件
• DDoS攻擊
• 網站掛馬
• 釣魚網站
• 代罪羔羊

資安威脅趨勢

Business Email Compromise

- 網路犯罪手法已由間接誘騙使用者的帳號密碼，轉向直接勒索錢財的「數位勒索」為主，駭客利用勒索病毒威脅受害者付錢贖回資料或透過**變臉詐騙攻擊或稱為商務電子郵件入侵（Business Email Compromise，簡稱 BEC）**手法進行商業詐騙，以獲得高利潤報酬。

資安趨勢部落格 > 報告數據 > 變臉詐騙 (BEC) > FBI 報告：2018 年全球變臉詐騙 (BEC) 損失金額已超過 120 億美元

FBI 報告：2018 年全球變臉詐騙 (BEC) 損失金額已超過 120 億美元

POSTED ON 2018 年 07 月 31 日 BY TREND LABS 趨勢科技全球技術支援與研發中心


您有收到類似這樣的信件嗎？
寄件人：資訊系統部門
收件人：Bob
信件名：系統部門的緊急通知
茲因信件系統不正常運作，
請進行重新登入
沒有啊

Business Email Compromise

※ 專門針對那些經常需要
匯款給外部供應商的企業機構

偽冒報價單及匯款帳戶騙
取客戶匯款

拋棄式郵件信箱

客戶接收駭客通知
匯款被騙

業務郵件遭鎖定

買家

出口商

變臉詐騙BEC(Business E-mail Compromise）運作的三種手法

- **透過偽造的郵件、電話或傳真要求匯款給另一個詐騙用帳戶**
  - 也被稱為「偽造發票騙局」、「供應商詐騙」和「發票變造騙局」
  - 透過偽造的郵件、電話或傳真要求匯款給另一個詐騙用帳戶。
- **詐騙者自稱為高階主管（CFO、CEO、CTO等）、律師或其他類型的法定代表**
  - 也被稱為「CEO詐騙」、「企業高階主管詐騙」、「偽造身分」和「金融企業匯款詐騙」
  - 聲稱要處理機密或有時效性的事情，要求匯款至他們所控制的帳戶
- **駭客入侵員工的電子郵件帳號**

預防BEC詐騙，從郵件安全做起

A. 養成安全的郵件使用習慣
   a) 不要用免費信箱與共用帳號
   b) 做好基本密碼安全與端點防護
   c) 培養員工資訊安全意識
B. 透過郵件安全產品的進階防護功能，加強企業本身的資安保護
   a) 應用郵件加密方式確保內容安全
   b) 發送BEC測試信，提升員工資安意識
   c) 可啟用專屬的BEC防護功能
   d) 自行設定郵件管控原則
   e) 強化郵件帳號登入安全
   f) 採用郵件身分驗證等機制
C. 強化企業匯款確認流程

BPC, BEC, APT

* 雖然有些目標式攻擊可能會修改商業流程，但通常是悄悄觀察敏感資料的儲存位置。

TREND MICRO 趨勢科技

大量寄發勒索病毒信件

- 駭客將**持續大量寄發勒索病毒信件**，並進一步鎖定特定可帶來最高報酬的對象攻擊，例如單一企業機構**以中斷營運為威脅**，試圖從中盈利。由於勒索病毒手法趨向純熟，促使其他類型的數位勒索攻擊也更加猖獗、從而發展出多樣且龐大的詐騙手法。

Agenda

- 引言
- 資安威脅趨勢
- 挖礦興起
- 勒索攻擊再進化
- 入侵事件的反思
- 如何因應與面對
- Q&A

資安趨勢部落格 > 挖礦/採礦程式 > 新Underminer漏洞攻擊套件, 散播Bootkit和挖礦病毒, 影響 50 萬台電腦,鎖定日本,台灣居第二

新Underminer漏洞攻擊套件, 散播Bootkit和挖礦病毒,影響 50 萬台電腦,鎖定日本,台灣居第二

POSTED ON 2018 年 07 月 30 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

趨勢科技發現一個新的漏洞攻擊套件（命名為Underminer），它會使用其他漏洞攻擊套件出現過的功能來阻止研究人員追蹤其活動或逆向工程其送入的病毒。Underminer會傳送感染系統開機磁區的bootkit及名為Hidden Mellifera的虛擬貨幣挖礦病毒。Underminer透過加密TCP通道來派送這些惡意軟體，並且用類似ROM檔案格式（romfs）的客製化格式來封裝惡意檔案。這些作法讓漏洞攻擊套件及有效載荷（payload）難以被分析。Underminer似乎是在2017年11月所開發。不過在此次案例中，使用了包括Flash漏洞攻擊碼，並且會用無檔案攻擊手法來安裝惡意軟體。

IOT 與 挖礦

- 網路犯罪集團正嘗試利用家用裝置來挖礦
- 家用裝置被用來挖礦，除了 PC 以外，就連運算能力有限的 IoT 裝置也出現挖礦活動
- 使用預設密碼登入家用裝置或暴力破解裝置密碼

十大對內攻擊 (2017 年)

對內的攻擊	活動數量
MS17-010 SMB 漏洞攻擊	2,441,996
暴力破解 RDP 登入密碼	1,464,012
可疑的 HTML Iframe 標籤	926,065
暴力破解 Microsoft SQL 系統管理員密碼	431,630
暴力破解 POP3 登入密碼	373,782
暴力破解 SMTP 登入密碼	289,746
利用指令列腳本 (Shell Script) 執行遠端指令	241,498
CoinHive 挖礦作業	194,665
利用 Apache Struts 動態方法呼叫從遠端執行程式碼	175,019
Netcore 路由器後門漏洞攻擊	142,902

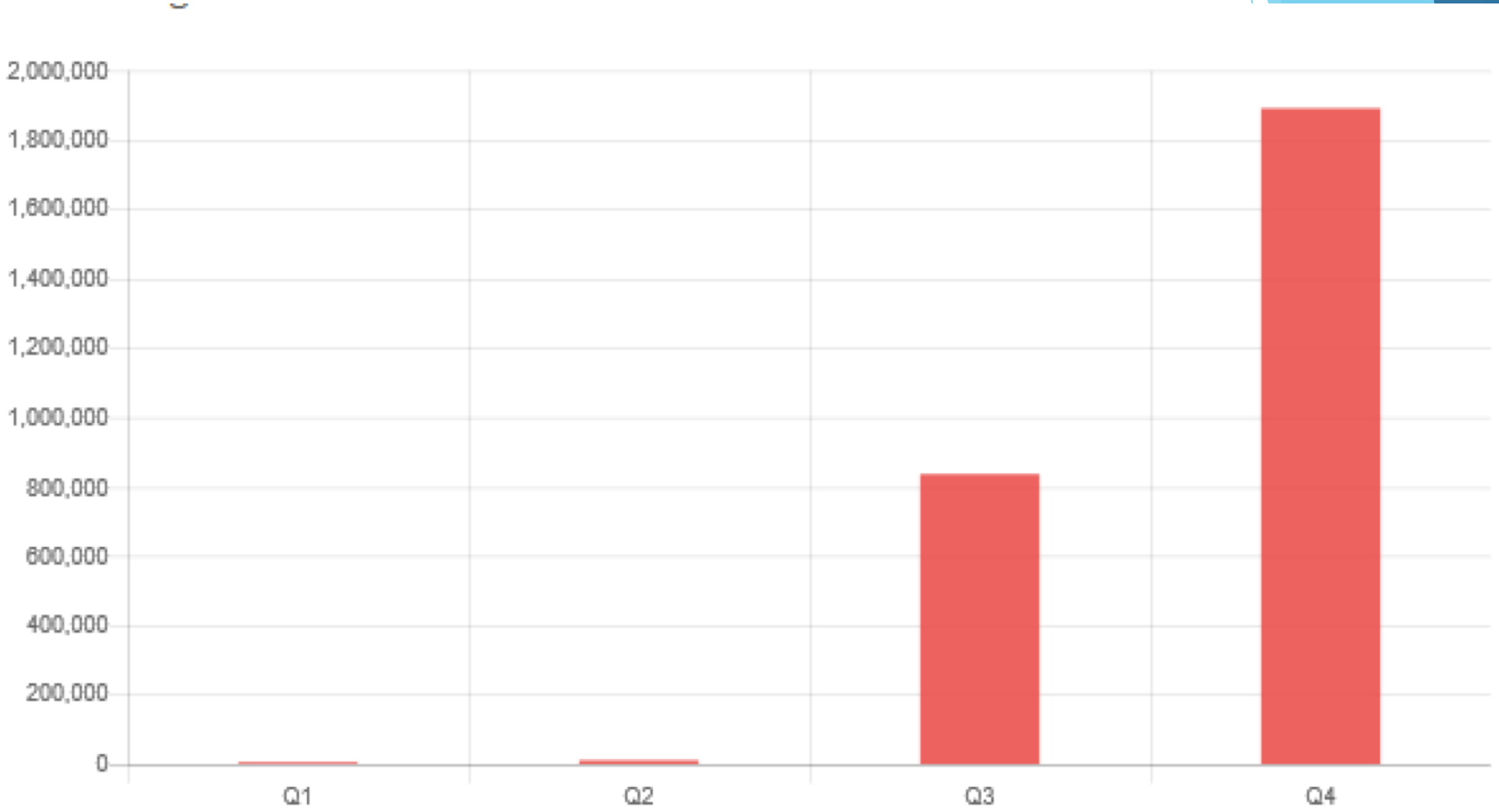
十大對外攻擊 (2017 年)

對外攻擊	活動數量
MS17-010 SMB 漏洞攻擊	9,716,094
ICMP BlackNurse 阻斷服務攻擊	1,786,694
DNS 放大攻擊	1,615,122
暴力破解 RDP 登入密碼	1,067,895
TCP SYN 洪水攻擊	777,218
IIS HTTP.sys 阻斷服務攻擊	544,883
IMAP SUBSCRIBE 指令緩衝區溢位	457,158
HTTP 內容長度負值緩衝區溢位	451,049
NULL 位元組注入	356,359
Apache Http2 無效參照解析	303,442

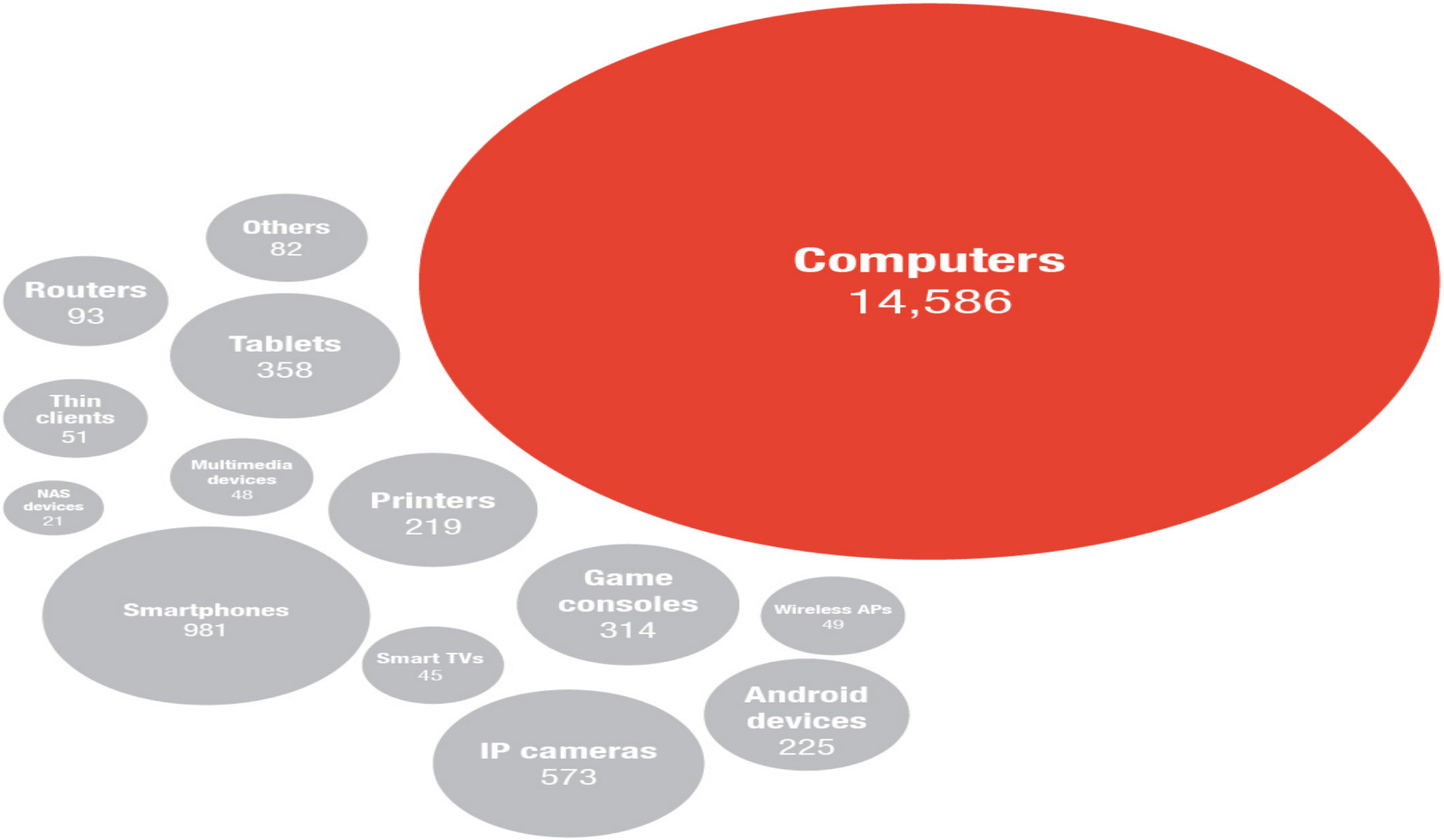
對內與對外的網路攻擊活動 (2017 年)

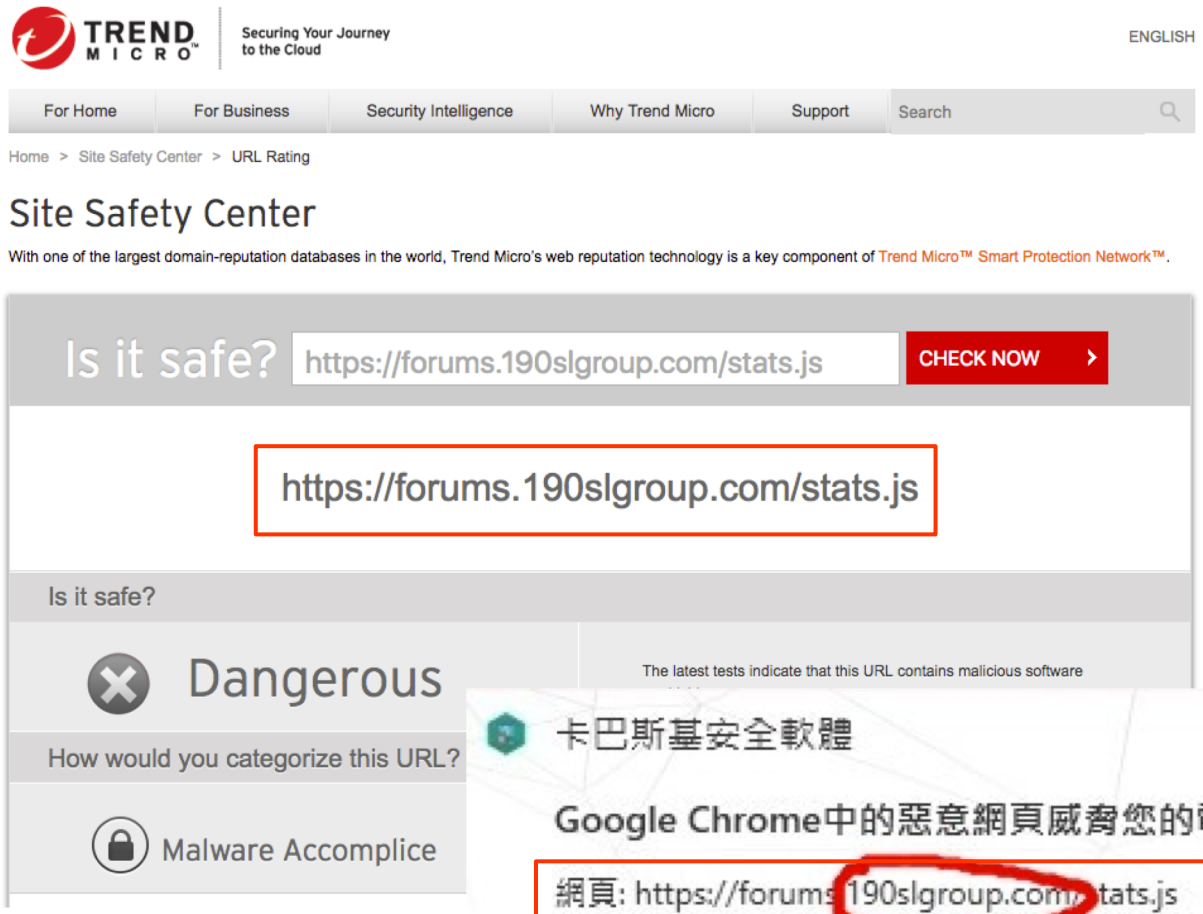
值得注意的活動	活動數量
加密虛擬貨幣挖礦	45,630,097
TELNET 預設密碼登入	30,116,181
MS17-010 SMB 漏洞攻擊	12,164,033
暴力破解登入密碼	3,695,143
ICMP BlackNurse 阻斷服務攻擊	1,792,854
DNS 放大攻擊	1,602,448
Android Stagefright 攻擊	1,170,348
可疑的 HTML Iframe 標籤	946,832
TCP SYN 洪水攻擊	855,185
IIS HTTP.sys 阻斷服務攻擊	547,570

加密虛擬貨幣挖礦活動 (2017 年)



遭到入侵的裝置被用於加密虛擬貨幣挖礦




TREND MICRO
Securing Your Journey to the Cloud
ENGLISH
For Home
For Business
Security Intelligence
Why Trend Micro
Support
Search
Home > Site Safety Center > URL Rating
Site Safety Center
With one of the largest domain-reputation databases in the world, Trend Micro's web reputation technology is a key component of Trend Micro™ Smart Protection Network™.
Is it safe?
https://forums.190slgroup.com/stats.js
CHECK NOW
https://forums.190slgroup.com/stats.js
Is it safe?
Dangerous
The latest tests indicate that this URL contains malicious software
How would you categorize this URL?
Malware Accomplice


卡巴斯基安全軟體
Google Chrome中的惡意網頁威脅您的電腦安全
網頁: https://forums.190slgroup.com/stats.js
我們建議您關閉此網頁。
詳細資訊

Agenda

- 引言
- 資安威脅趨勢
- 挖礦興起
- 勒索攻擊再進化
- 入侵事件的反思
- 如何因應與面對
- Q&A

Ransomware

- 勒索病毒攻擊活動的成功會讓網路犯罪分子想辦法從目標群獲取最大的回報。
- 攻擊者將會繼續利用**網路釣魚活動來透過郵件大量散播勒索病毒**，以確保影響一定數量的使用者。
- 還可能會針對單一組織（可能是工業物聯網IIoT的環境）來**進行破壞運作**、影響生產線的勒索病毒攻擊。

三個勒索病毒在未來數年仍將持續肆虐的理由

1）勒索病毒持續進化中

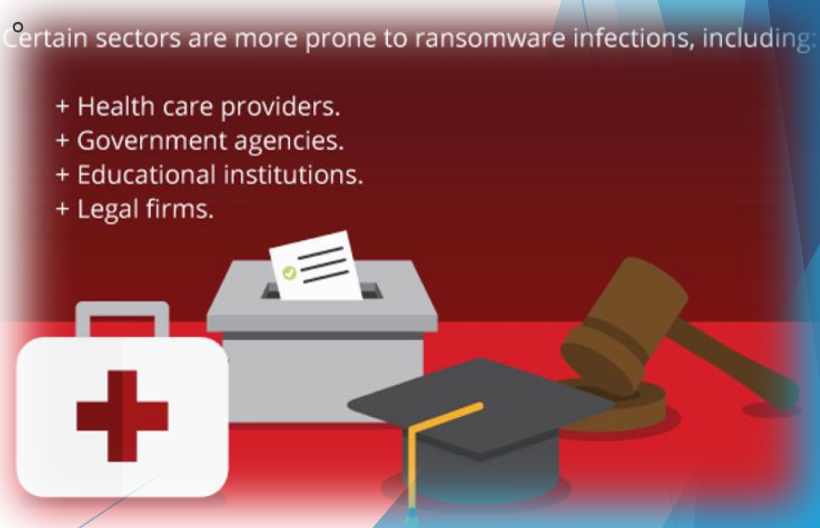
- 大多數的勒索病毒都屬於檔案加密型或上鎖型
- 另一種的上鎖型勒索病毒則是會鎖住中毒設備的作業系統

2）勒索病毒對駭客來說是個金雞母

- 駭客不需要經過中間人就可以直接獲取金錢回報
- 勒索病毒的威脅無處不在，而且某些產業會更被針對。

3）不缺乏目標: 從個人用戶到大企業都會被攻擊

- 資料的重要性以及依賴資料來進行日常運作，讓某些產業更加容易遭受勒索病毒。這包括：
  - 醫療機構
  - 政府機構
  - 教育機構
  - 法律事務所



”為什麼不關注在複雜的攻擊上？為什麼新漏洞出現時沒有發表深入地探討？”

“**因為舊的攻擊仍然造成較大的傷害**“。我們不曾回頭去檢視這些舊協定跟程式碼有多脆弱，因為“我們一直在用它們，什麼事都沒有發生，所以我們一定是安全的”如果我們不花時間來建立良好的網路習慣，不管是組織或個人，就會讓攻擊可以很容易的一再發生。

作者：**Natasha Hellberg（趨勢科技資深威脅研究員）**

Vulnerability?

Heartbleed

Struts2

Shellshock

有那麼嚴重嗎？

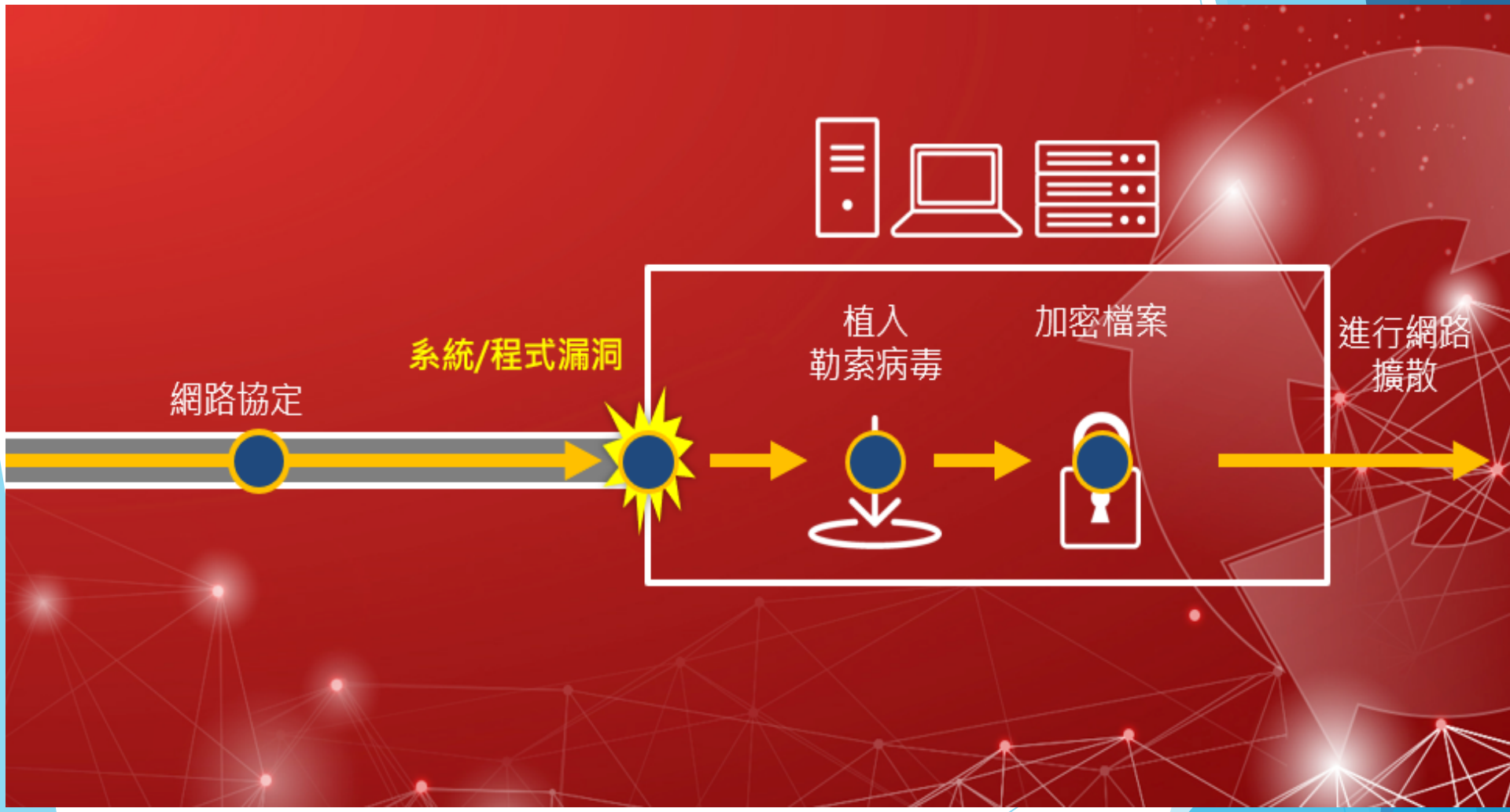
Struts 2

CVE-2017-5638：Apache Struts 2 漏洞可能讓駭客從遠端執行程式

POSTED ON 2017 年 03 月 15 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

Apache Struts 是一個免費的開放原始碼程式開發架構，用來開發 Java 網站應用程式。我們仔細研究了過去 Apache Struts 被發現的幾個遠端程式碼執行 (Remote Code Execution，簡稱 RCE) 漏洞之後發現，歹徒大多使用 Object Graph Navigation Language (OGNL) 這個程式語言。OGNL 之所以很容易讓駭客從遠端執行任意的程式碼，是因為 Apache Struts 在大多數的流程當中都用到這個語言。

最近常見攻擊企業手法



收到駭客勒索：要臉還是要錢？

Agenda

- 引言
- 資安威脅趨勢
- 挖礦興起
- 勒索攻擊再進化
- 入侵事件的反思
- 如何因應與面對
- Q&A

單位為何受駭

1) 資安人力不足
2) 缺乏防護措施
3) 缺乏預警能力
4) 缺乏處理經驗

為何駭客能一再突破

① 主機存在漏洞缺乏保護

② 網路區隔設計不佳

③ 缺乏威脅監控機制

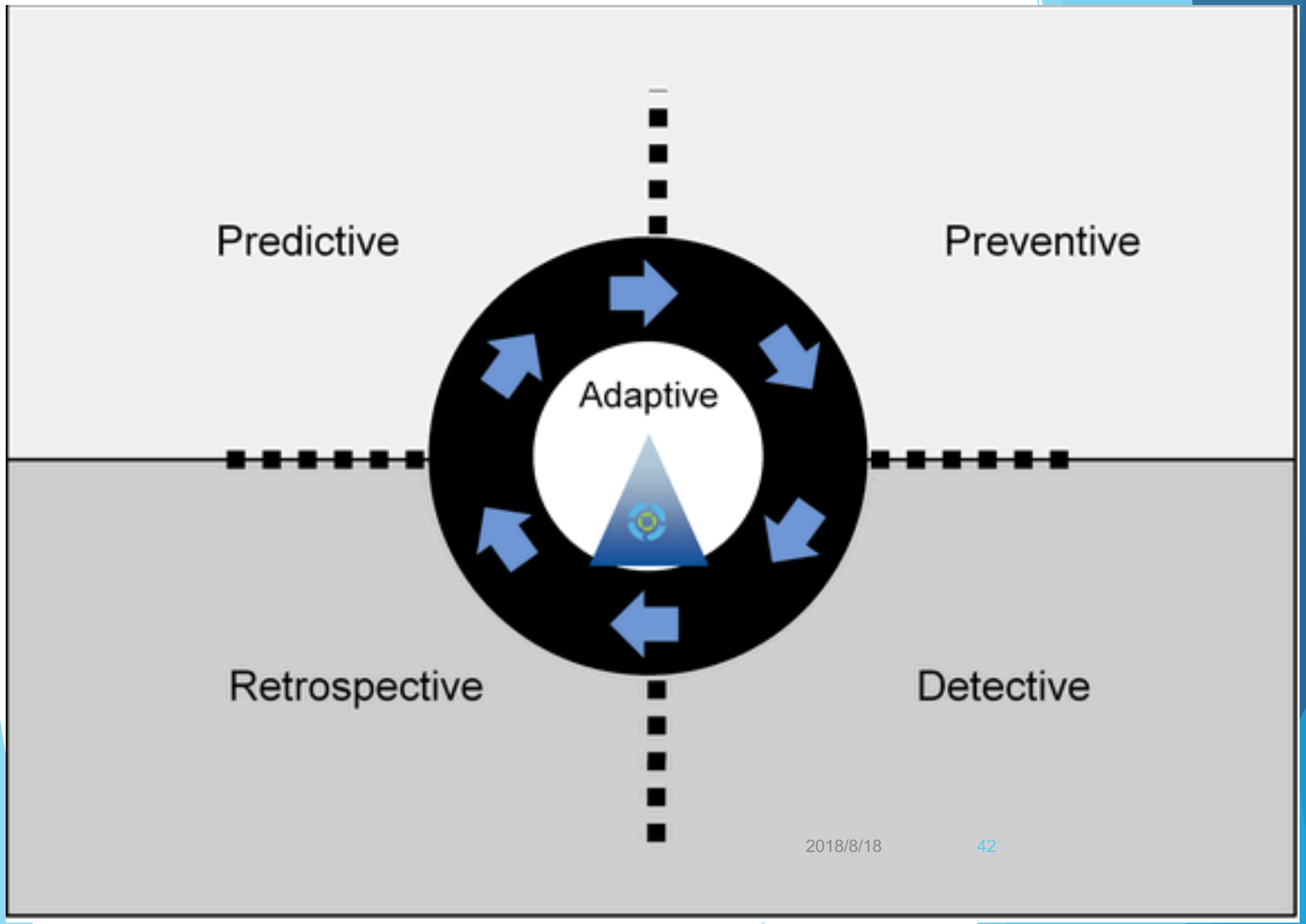
缺乏威脅監控機制

- 主機異常行為監控
  - 帳號的異動
  - 系統設定的異動
  - CPU、磁碟、記憶體等使用率的異常變化
  - LOG異常清除
- 內部網路異常流量監控
  - 遠端指令或排程
  - 針對性能問題影響業務的流量監控

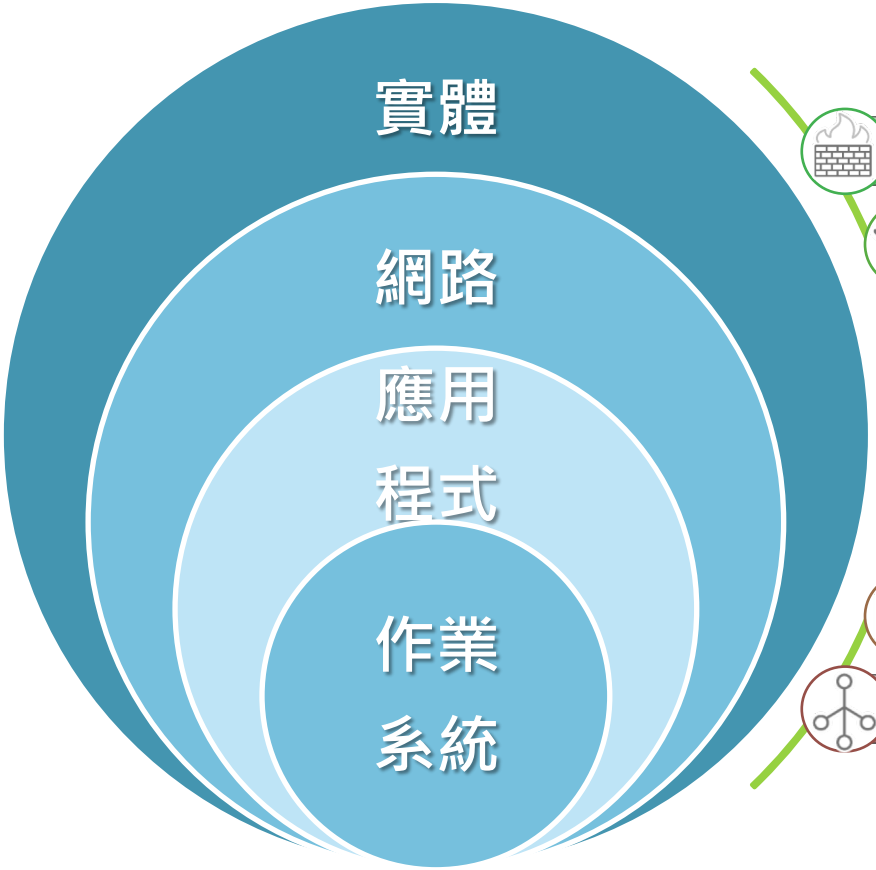
Agenda

- 引言
- 資安威脅趨勢
- 挖礦興起
- 勒索攻擊再進化
- 入侵事件的反思
- 如何因應與面對
- Q&A

面對 接受 處理

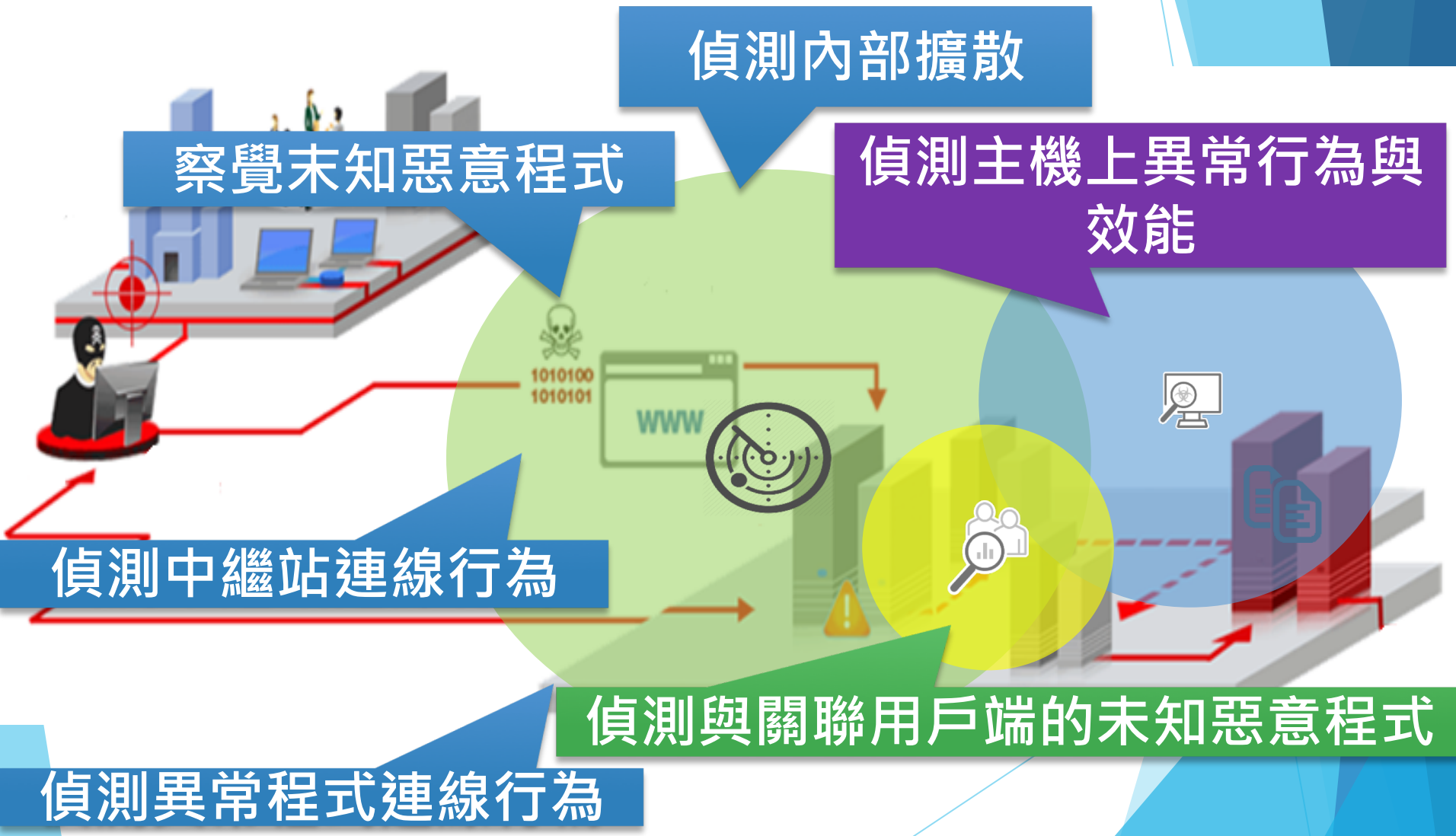

Predictive
Preventive
Adaptive
Retrospective
Detective

適應性安全架構



- 防火牆
- 深層封包解析
- 虛擬補丁
- 應用程式防護
- 惡意程式防禦
- 系統異動監控
- 紀錄集中管理

適應性安全架構


偵測內部擴散
察覺未知惡意程式
偵測主機上異常行為與效能
1010100
1010101
WWW
偵測中繼站連線行為
偵測與關聯用戶端的未知惡意程式
偵測異常程式連線行為

- 不要懷疑單位是否會成為駭客的目標

- 「世界上大型企業分兩種：一種是已經被駭客入侵，另一種則是被入侵卻渾然不知的公司。」 --- FBI 局長 James Comey

- **檢視資安事件對可能造成的風險程度**
- **檢視單位的資安現況，並採相對應的強化措施**

Agenda

- 引言
- 資安威脅趨勢
- 挖礦興起
- 勒索攻擊再進化
- 入侵事件的反思
- 如何因應與面對
- Q&A

~ Thank You ~