Panasonic
Cyber Security Lab

Panasonic
PSIRT

狩獵網路威脅，
打造可信賴的物聯網產品

Kyo Chen, Head of Cyber Security Lab, PCSL

Freddy Ma, Senior Threat Intelligence Researcher, PCSL

Panasonic Cyber Security Lab

Kyo

網路安全實驗室負責人 / HITCON Cyber Range 總召集人

負責管理松下網路安全實驗室，並與日本松下產品安全中心共同運行全球產品安全的專案及產品安全事件響應團隊。

Freddy

資深威脅情資研究員

負責研究物聯網網路安全和惡意軟體分析，設計/開發/維運 物聯網蜜罐、沙箱和威脅情報分析系統，追蹤和分析高級持續性威脅 (APT) 的惡意軟體。

Panasonic
Cyber Security Lab

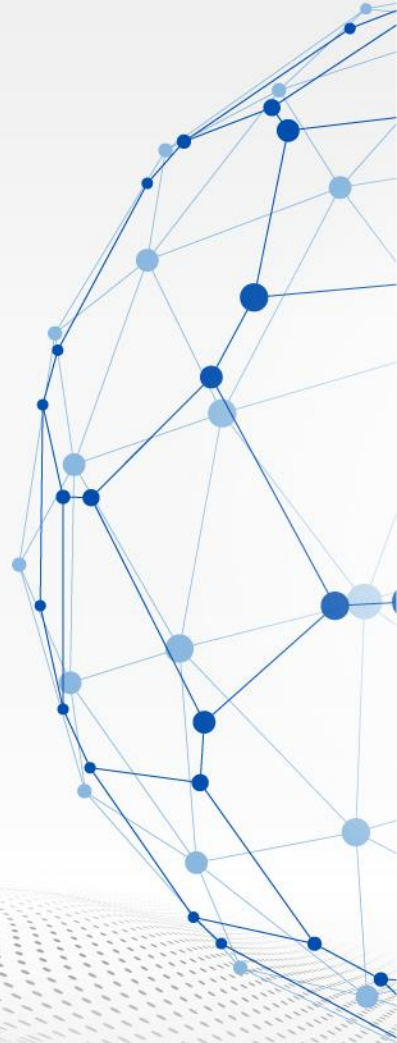
Panasonic
PSIRT

AGENDA

01 物聯網產品的資安威脅

02 Panasonic 威脅情資平台 - ASTIRA

03 Panasonic 產品安全解決方案 - THREIM



物聯網產品的資安威脅

從個人到企業面臨的挑戰

一般消費者眼中的物聯網產品威脅

iThome 新聞 產品&技術 專題 AI Cloud 醫療IT 資安 研討會 社群 IT E

高級智慧馬桶也存在安全漏洞

Satis智慧型馬桶是透過Lixil基於Android平台所開發的「My Satis」程式來控制，程式與馬桶的通訊是仰賴藍牙。該漏動讓任何人都可下載My Satis應用程式然後命令馬桶不斷沖洗，或是讓馬桶蓋突然開闔，或是啟用烘乾或盆浴功能等。

文/ 陳曉莉 | 2013-08-06 發表

讚 0 分享

智慧咖啡機「連網未加密」　成駭客入侵索財絕佳目標

免費休閒小遊戲，免下載免安裝，隨點即玩!

8 讚

實習記者陳妙津／綜合報導

現在連智慧咖啡機都可能被駭！網路安全軟體公司Avast高級研究員赫倫（Martin Hron）近日發明一項技術，可以入侵智慧咖啡機植入勒索軟體，藉以索取財物，不幸被選上的咖啡機不但無法使用，還會持續啟動、不斷噴出熱水，並發出蜂鳴聲等，迫使受害者掏錢「贖機」。

資料來源：https://www.ithome.com.tw/news/81898, https://www.ettoday.net/news/20201011/1829067.htm

物聯網產品，是能造成多大的威脅？

現實中的物聯網產品威脅

趨勢

物聯網漏洞！駭客從溫度計侵入賭場資料庫，撈出豪賭大戶名單

Mia

2018/04/16 • 資安 、 物聯網 、 IOT

隨著智慧物聯裝置普及，也為駭客打開更多入侵門戶，他舉例從智慧冰箱、溫度計、空調、音響，物聯裝置已經充滿生活，也擴展了駭客的攻擊面，而傳統的資安防護方法卻鮮少涵蓋到物聯網。

醫療IoT安全！Palo Alto Networks：75%注射幫浦存在資安風險

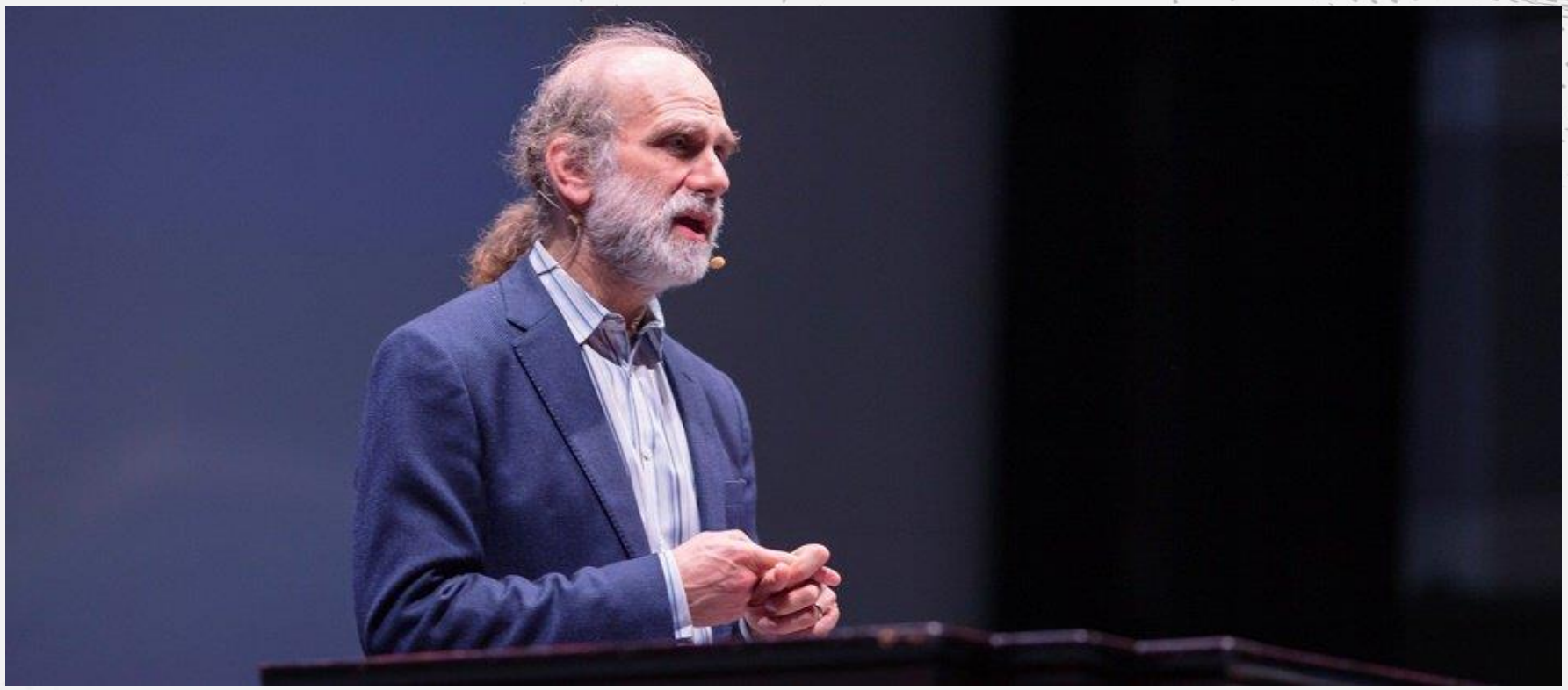
2022 / 12 / 20 - 編輯部

新增至最愛文章

19 歲駭客意外發現特斯拉漏洞，可遠距操控全球 25 輛特斯拉

作者 林 妤柔 | 發布日期 2022 年 01 月 25 日 15:40 | 分類 會員專區 , 汽車科技 , 資訊安全 分享 分享 Follow 分享

資料來源：https://www.inside.com.tw/article/12569-hackers-stole-a-casinos-high-roller-database-through-a-thermometer, https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10255, https://infosecu.technews.tw/2022/01/25/tesla-hacker-teslamate-api/



Bruce：萬物都是電腦，所有事也都變成了資安事

資料來源： https://www.ithome.com.tw/news/129804

個人、企業如何應對這些資安事?

個人及家庭消費型物聯網產品

高互動/風險聯網產品

1. 含有攝影鏡頭/麥克風，提供串流影/音功能
2. 會儲存機敏隱私資訊
3. 操作異常能造成產品本身外的重大危害
4. 使用 Linux/Android 等主流作業系統，具有較大的計算能力

低互動/風險聯網產品

1. 僅能發特定指令控制設備
2. 僅儲存使用紀錄，不含隱私資訊
3. 產品本身作動異常不會造成嚴重的擴散危害
4. 即時性作業系統，提供較小的計算資源

個人及家庭消費型物聯網產品

針對高互動/風險物聯網產品，一般消費者可以.....

1. 選擇有 PSIRT 或對於資訊安全有投資的企業/品牌的產品

2. 挑選標榜符合資安規範/標章的產品
   例如：ETSI EN 303 645, PSTI, 物聯網資安標章, CSA CLS...

3. 提升自我的安全意識
   例如：避免使用弱密碼、釣魚網站識別...

4. ~~還在用預設帳密的產品，就不要再買了~~

面向企業的物聯網產品

企業辦公室/自動化工廠

- 有線/無線網路基礎設施
- 會議室投影設備
- 辦公室影印設備
- 資料備份系統
- 門禁管制系統
- 實體安全攝影系統
- 大樓環控系統
- 自動化設備，如：機器手臂、車床、產線
- ….

面向企業的物聯網產品

企業辦公室/自動化工廠

- 有線/無線網路基礎設施
- 會議室投影設備
- 辦公室影印設備
- 資料備份系統
- 門禁管制系統
- 實體安全攝影系統
- 大樓環控系統
- 自動化設備，如：機器手臂、車床、產線
- ....

ZERO TRUST

面向企業的物聯網產品

針對物聯網產品，企業可以.....

1. 制定符合企業運作的物聯網產品安全管理辦法
   例如：建立物聯網產品採購規範、資產清單、定時更新及汰換設備

2. 建立適當的物聯網產品監管機制
   例如：流量異常監測、日誌異常管理

3. 挑選能積極符合資安需求的供應商
   例如：重大漏洞發佈時能主動告知

4. 定期進行員工資訊安全教育訓練

5. ~~還在用預設帳密的產品，就不要再買了~~

物聯網產品製造商，要如何抵抗威脅?

02

ASTIRA

Panasonic 威脅情資平台

針對 IoT 的攻擊增加

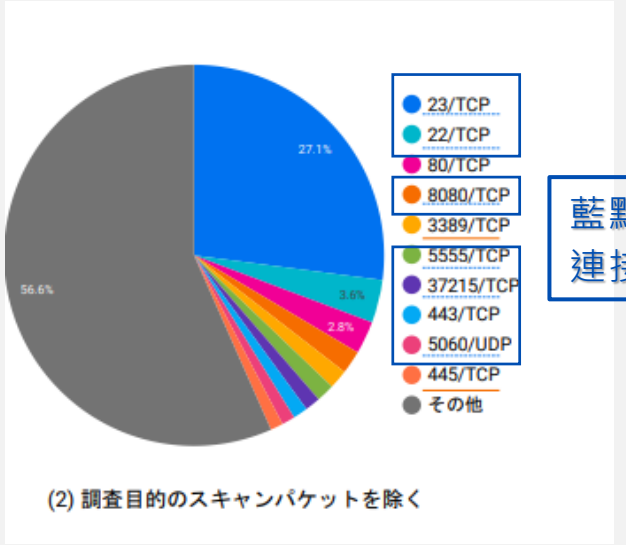
日本 NICTER 自暗網觀測到每個 IP 位址每年觀察的封包總數
(過去 10 年間)

図2.1 IPアドレス当たりの年間総観測パケット数（過去10年間）

資料來源：https://csl.nict.go.jp/report/NICTER_report_2023.pdf

按目標連接埠劃分的年度觀察到的封包百分比
(去除掃描封包)

資料來源: 日本 NICTER 自暗網觀測報告



藍點底線為 IoT 設備常見連接埠

NICTER REPORT 2023 (Japanese only)

IoT 惡意程式的現狀

- 由於物聯網惡意程式在**漏洞揭露後幾天內**就開始肆虐，且攻擊週期變得越來越快

- 日益複雜的規避偵測功能功能
  - 包含多層次執行階段的惡意程式
  - 複雜的混淆技術

武器化

ASTIRA

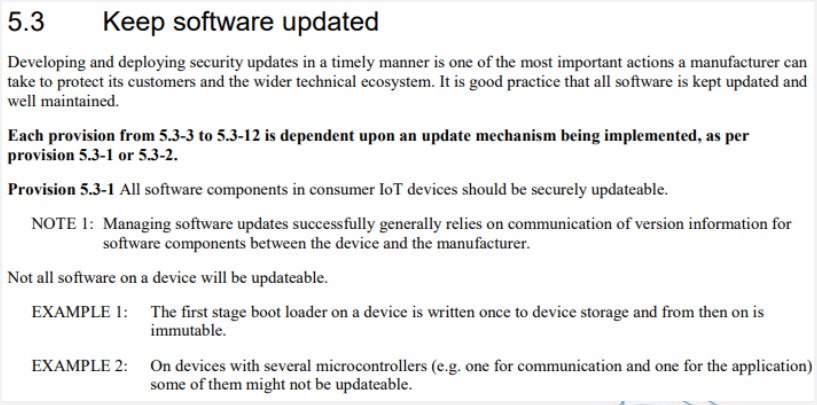
2022/12
IoT BotNet 惡意程式發布

2023/01/11
ASTIRA 捕獲到惡意程式

2023/01/18
VirusTotal 收到樣本

出貨後產品安全的重要性

- 涵蓋產品生命週期的安全活動
  - 攻擊方法不斷演變
- =>產品安全措施的**有效性隨著時間的推移而下降**
- 國際標準要求強制執行安全性更新，
  例如: ETSI EN303.645



5.3 Keep software updated

Developing and deploying security updates in a timely manner is one of the most important actions a manufacturer can take to protect its customers and the wider technical ecosystem. It is good practice that all software is kept updated and well maintained.

Each provision from 5.3-3 to 5.3-12 is dependent upon an update mechanism being implemented, as per provision 5.3-1 or 5.3-2.

Provision 5.3-1 All software components in consumer IoT devices should be securely updateable.

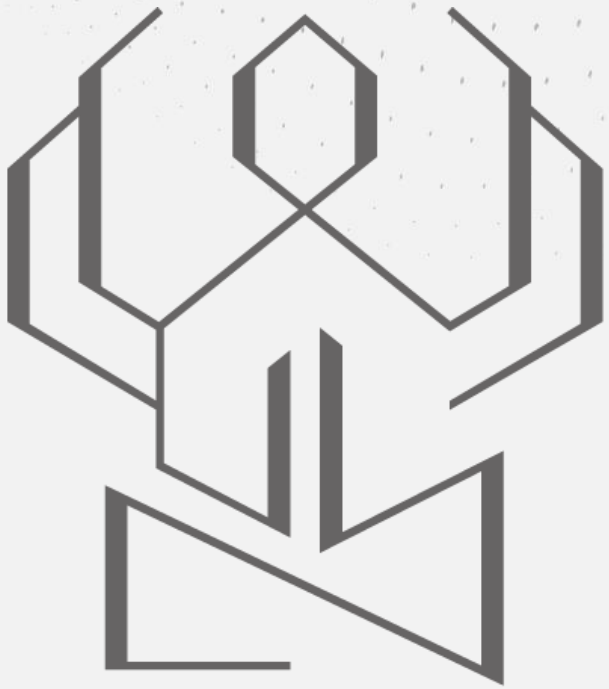
NOTE 1: Managing software updates successfully generally relies on communication of version information for software components between the device and the manufacturer.

Not all software on a device will be updateable.

EXAMPLE 1: The first stage boot loader on a device is written once to device storage and from then on is immutable.

EXAMPLE 2: On devices with several microcontrollers (e.g. one for communication and one for the application) some of them might not be updateable.

資料來源：https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf



ASTIRA

Panasonic IoT Threat Intelligence

ASTIRA 的研發動機

- 整個產品生命週期至上市後的生命週期結束，持續超過 15 年。
- **攻擊者不斷精進攻擊手段，產品的相對安全等級在出貨後隨著時間的推移而降低。**
- 持續改進產品生命週期中的每項安全活動。

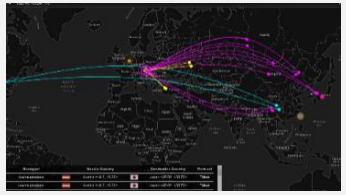
ASTIRA 如何運作

來自 HoneyPot 與網際網路的惡意情資

蒐集資料

分析情資

情資平台



視覺化

強化組織

開發 / 採取對策

從洞察至戰略

快速告警至整個團隊

分享回饋

出貨前
建立 DevSecOps

出貨後
確保服務階段安全

6年來收集的資料統計

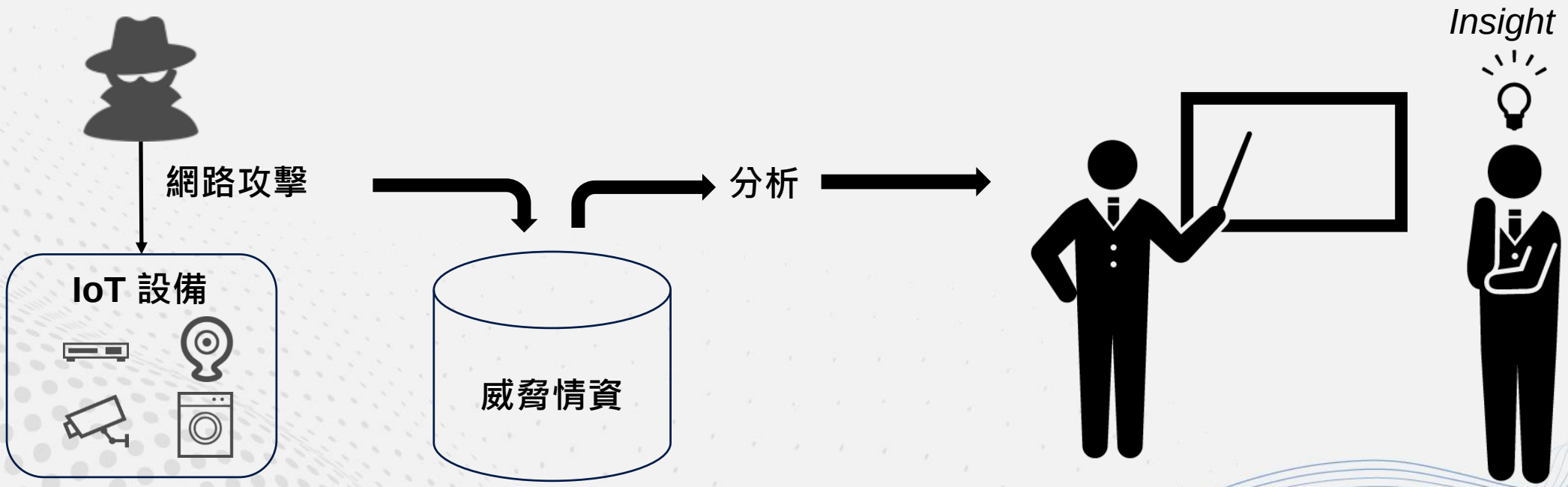
- 將 Panasonic IoT 設備，安裝成 Honeypots
- IoT 被故意設置成”鬆散的”設定，使其容易被攻擊
- IoT 惡意程式的自動捕捉、靜態和動態分析
- 對正在開發並尚未推出市場的產品進行資訊收集

[Since November 2017]

Total Attacks	2,810,981,814
Malware	439,014
IoT Malware	37,768

分析威脅的目的

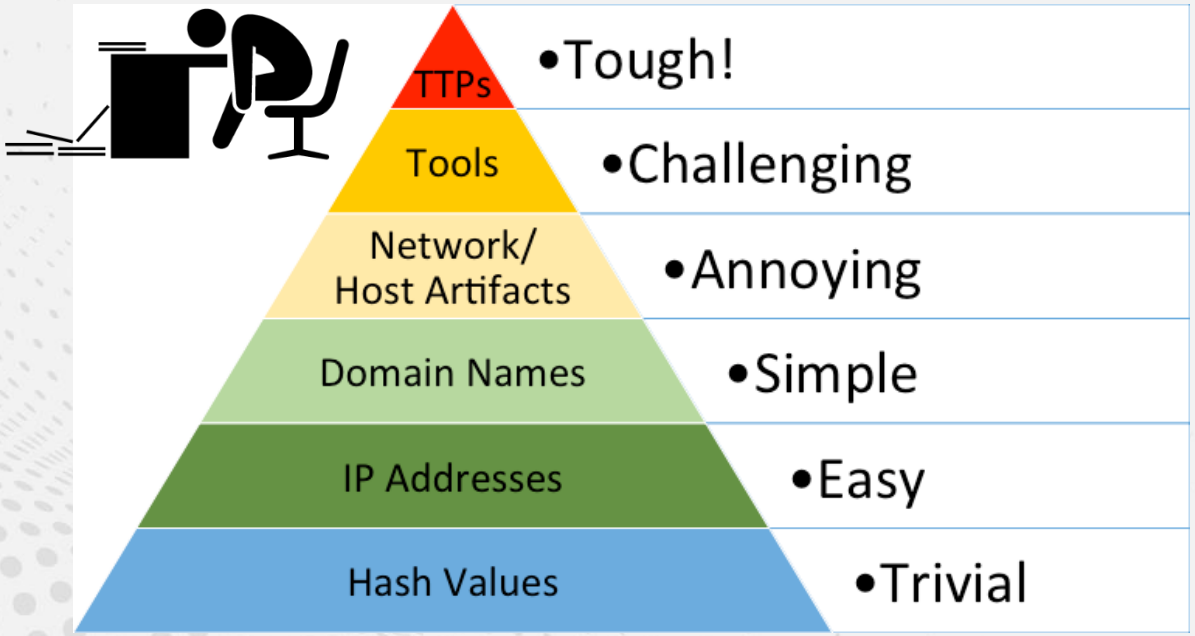
- 透過與開發人員分享針對 IoT 設備的真實威脅，使開發人員能夠掌控並提高產品安全性
- STEP1：從大量威脅情資中洞察其內容
- STEP2：與開發者分享看法 / 分析結果



分析資料的挑戰

STEP1：從大量威脅情資中洞察其內容

- 工作量亦很大
- 撰寫報告非常耗時



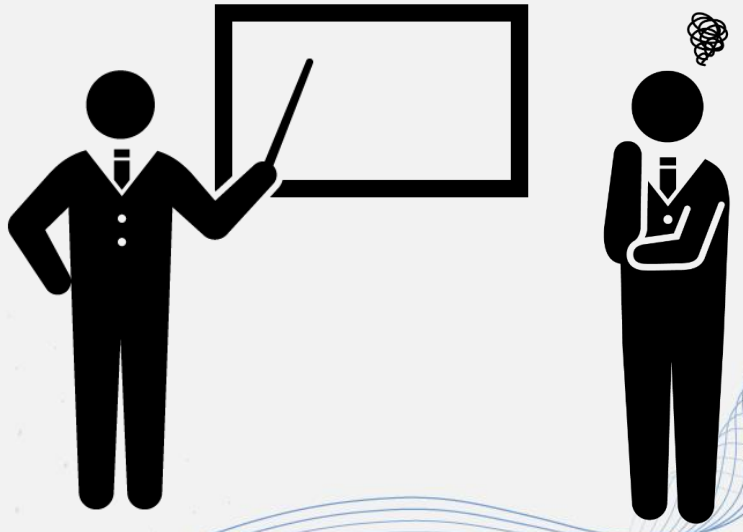
David Bianco 的痛苦金字塔

資料來源：https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

STEP2：與開發者分享看法 / 分析結果

- 產品開發人員不是資安專家
- 他們必須了解資安議題

艱深的技術術語

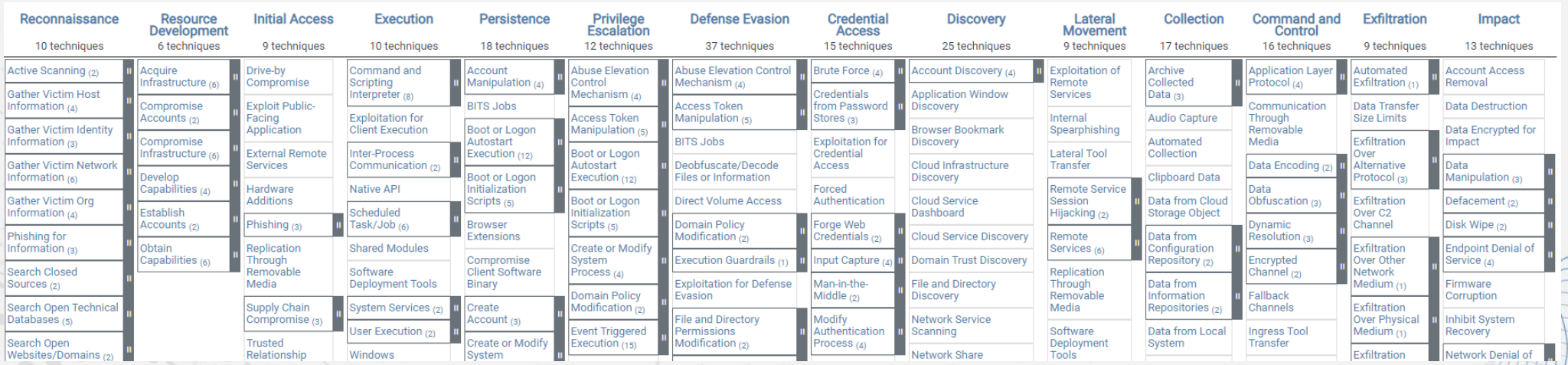


使用 MITRE ATT&CK

- 組織 TTP 的框架，廣泛應用於安全產業。
- 組織性的分析與理解。
- 從視覺上很容易理解，越向右攻擊進程就前進。

將攻擊對應到 ATT&CK 框架是有效的

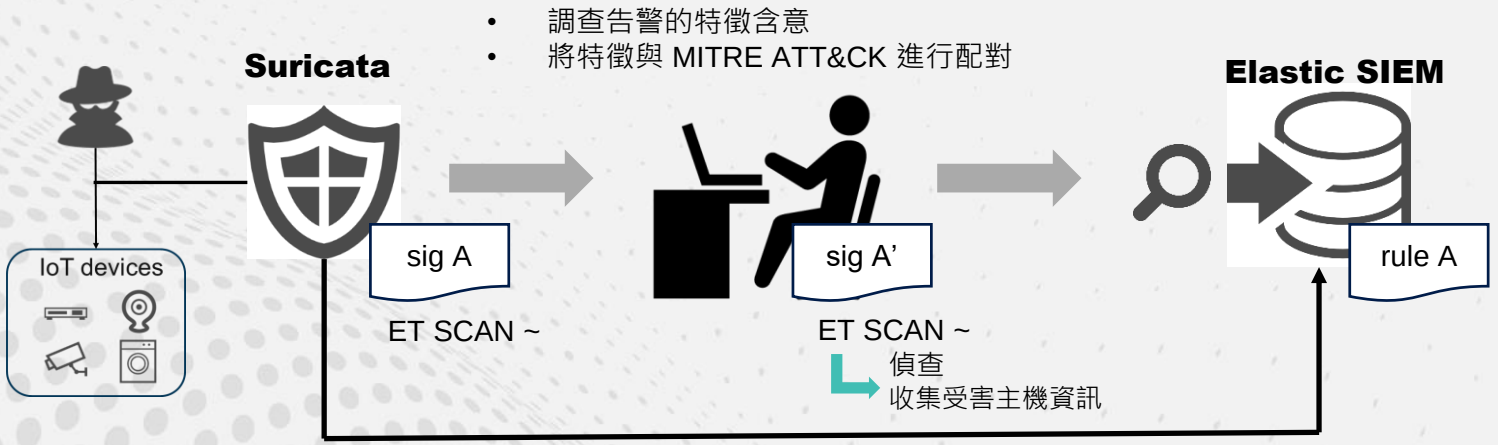
- 減少工作量
- 幫助開發人員更簡單的了解正在發生的事情



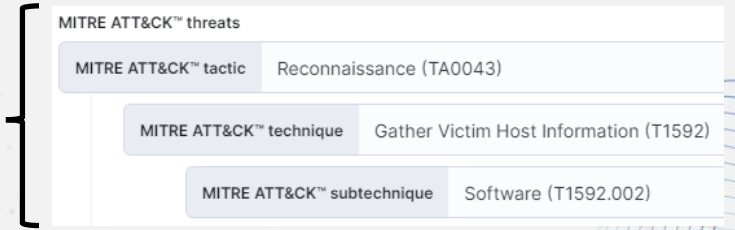
資料來源： https://attack.mitre.org/matrices/enterprise

如何將 **ASTIRA** 收集的資料對應到 **MITRE ATT&CK**

- ASTIRA 結合 “Suricata”
  - 開源入侵偵測系統 (IDS)
  - 透過 ASTIRA 收集的資料中的特徵，對於偵測到的可疑活動進行告警。
- 將告警的 IDS 特徵對應到 MITRE ATT&CK
- ASTIRA 結合 “Elastic SIEM”
  - 建立關於 MITRE ATT&CK 的偵測規則資訊
  - 自動配對可疑活動與MITRE ATT&CK



設計與 ATT&CK 對應的欄位



情資關聯流程

蒐集

資料來自
Honeypot

挑選

從未對應的特徵
發出告警

配對

將特徵對應至
ATT&CK

自動化

透過 Elastic SIEM
自動化配對

偵測

來自 IDS 的可疑
活動

調查

理解告警特徵與
目標漏洞的意義

創建

Elastic SIEM 使用
的偵測規則與配對
規則

Auto

Semi-auto or easy

Manual

真實設備的 MITRE ATT&CK 分析

No	Tactics	Technique	Attacks	Cumulative relative frequency
1	**Reconnaissance**	Active Scanning, Gather Victim Network Information, Gather Victim Host Information, Gather Victim Identity Information	**208,487**	**80.50%**
2	**Initial Access**	Exploit Public-Facing Application, External Remote Services	**50,354**	**99.94%**
3	**Execution**	User Execution, Shared Modules	**19**	99.95%
4	Persistence	-	0	99.95%
5	Privilege Escalation	-	0	99.95%
6	Defense Evasion	Indicator Removal on Host	6	99.95%
7	Credential Access	-	0	99.95%
8	Discovery	Network Share Discovery, File and Directory Discovery, System Information Discovery	128	99.99%
9	Lateral Movement	-	0	99.99%
10	Collection	Data from Configuration Repository	4	100%
11	C&C	-	0	100%
12	Exfiltration	-	0	100%

四捨五入至小數點後兩位

與開發部門協作進行風險回饋

到目前為止尚未觀察到受損的設備

Improve each phase of product lifecycle

規劃	設計	實作	驗證(測試)	上市
威脅 分析	原始碼 設計	撰寫 程式	漏洞 評估	事件回應 (Incident Response)

最新威脅訊息

開發階段的安全測試

風險評估

主動事件回應
出貨後定期進行安全測試

設備自我保護

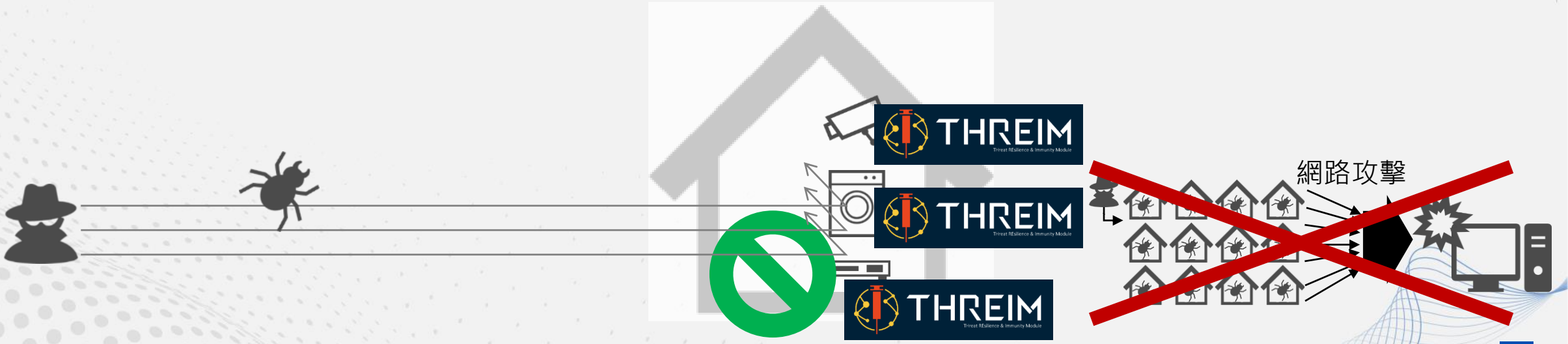
THREIM

IoT-specialized self-protection module

Panasonic 產品安全解決方案

防止設備被接管和濫用

網路攻擊鏈



資料來源： https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

THREIM 的主要功能

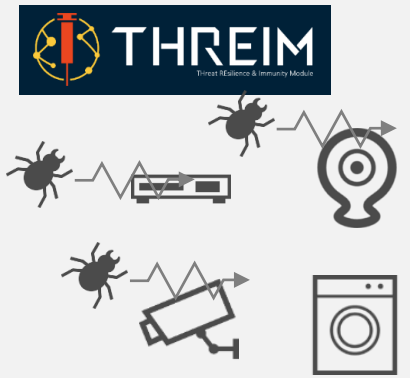
- 出廠時預設的自我保護模組，使用者不需要額外操作。
- 輕量級且對 IoT 產品運行影響最小
- 支援基於 Linux 的 IoT 裝置

- 能夠增強設備的安全性
  - 在產品上市發布後，可以自主的自我防護
  - 漏洞被開採時，在韌體更新前的防護手段

如何評估 THREIM 成效

- 使用來自 ASTIRA 所蒐集的惡意程式
- 將惡意程式放置 IoT 設備並且執行

超過 30,000 個 IoT 平台的惡意程式



將 IoT 惡意程式放入後執行

成效評估流程

列舉
列舉所有惡意程式的 CPU 架構

取出
從群體拿出對應 CPU 架構的惡意程式

執行
執行惡意程式

初始化
初始化設備，供下一次執行

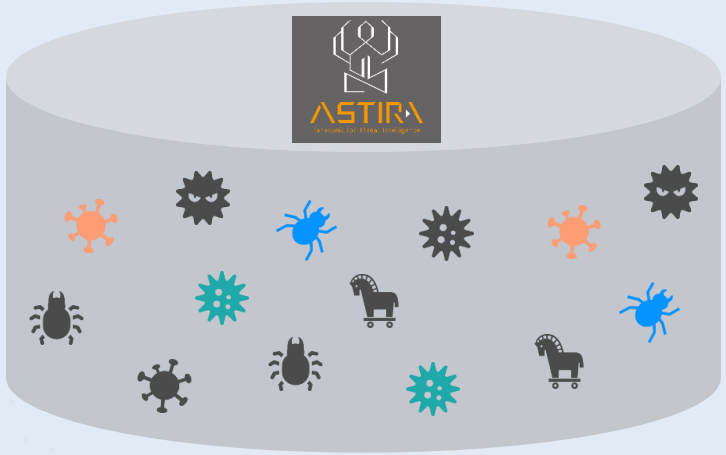
分群
將樣本依照CPU的架構進行分群

測試
惡意程式是否在裝置上成功運行

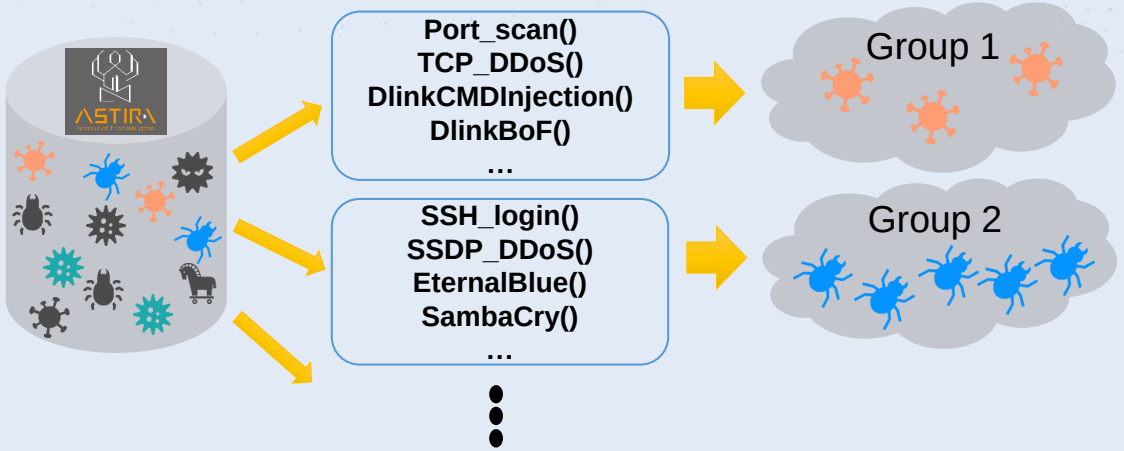
觀察
惡意程式被偵測到並且使其停止執行

分群與採樣惡意程式，用來提高效率

01 超過 30,000 個 IoT 惡意程式的集合

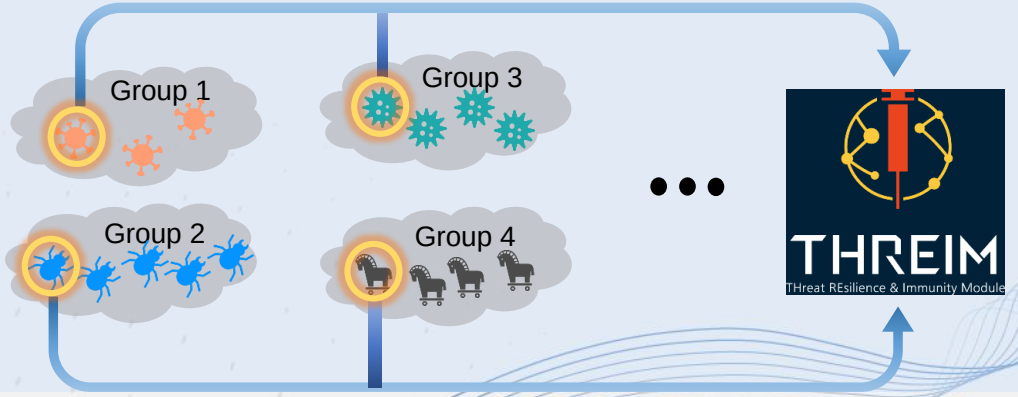


02 相似的惡意程式會被分到同一群



03 分群結果
e.g. ARM: 1,804 groups

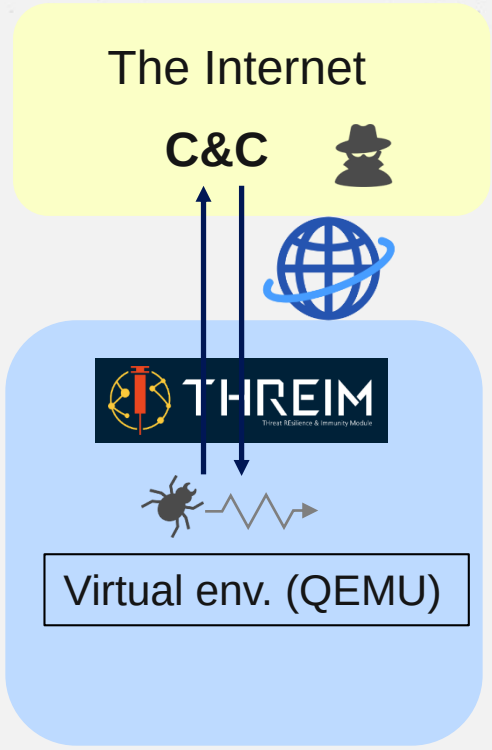
04 從各群中取出樣本



環境設定

- 隔離網路中的真實 IoT 產品
  - 避免產品機密外洩
- 能連接至網際網路的虛擬環境
  - 進行額外評估，因為大多數惡意程式需透過網路連接到 C&C

隔離網路的真實 IoT 產品評估



使用虛擬環境執行包含網際網路的評估

評估結果

- 最高有 86.1% 的樣本被偵測到
- 一半的樣本可以在真實設備上運行，一半的樣本失敗。
- 對設備的資源消耗影響不大

產品	CPU	偵測比例	設備上的惡意程式執行數量	受測的惡意程式總量	增加的 CPU 使用率	增加的記憶體使用率
設備 A	ARM	**86.1%**	275	1804	+0.3%	+0.9%
設備 B	ARM	57.7%	759	1804	+3.2%	+0.1%
設備 C	MIPS	66.1%	348	689	+5%	+0.7%
設備 D	AMD64	59.5%	742	1102	+2.1%	+0.1%

Notes: 偵測率移除了C2伺服器已失效的樣本統計。
CPU與記憶體的使用率為THREIM啟動前與啟動後的比較。

Summary

在這議程中...

1. 個人或者企業，如何安全地挑選物聯網產品

2. 針對物聯網威脅，松下如何應對
   => Panasonic ASTIRA

3. 物聯網產品出貨後保護效果大幅降低，松下如何提升產品安全性
   => Panasonic THREIM

THANK YOU

panasonic.pcsl@tw.panasonic.com

Panasonic PSIRT

Panasonic Cyber Security Lab