網路安全與個資保護認知宣導課程(包含社交工程宣導)

資訊安全人人有責

00 近期資通安全情資分享

01 威脅與趨勢

02 作業安全

03 資訊安全

04 結論

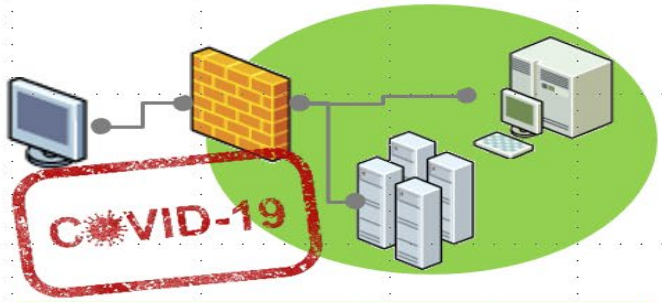
Agenda

近期資通安全情資分享

00

資通安全情資分享

- 綜整112年全球資安威脅與相關研究報告，歸納全球資安 威脅趨勢



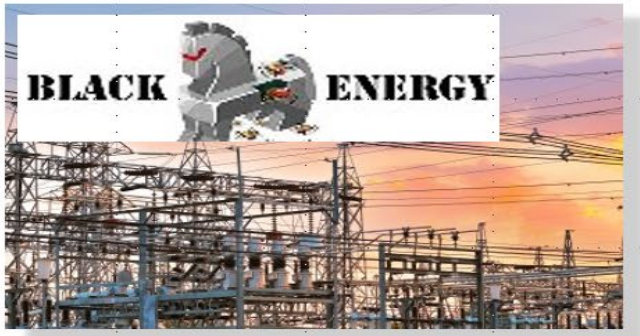
遠距工作型態
促使網路攻擊提升

勒索軟體攻擊
風險激增

社交工程手法仍頻繁

國家層級駭客
攻擊仍頻繁

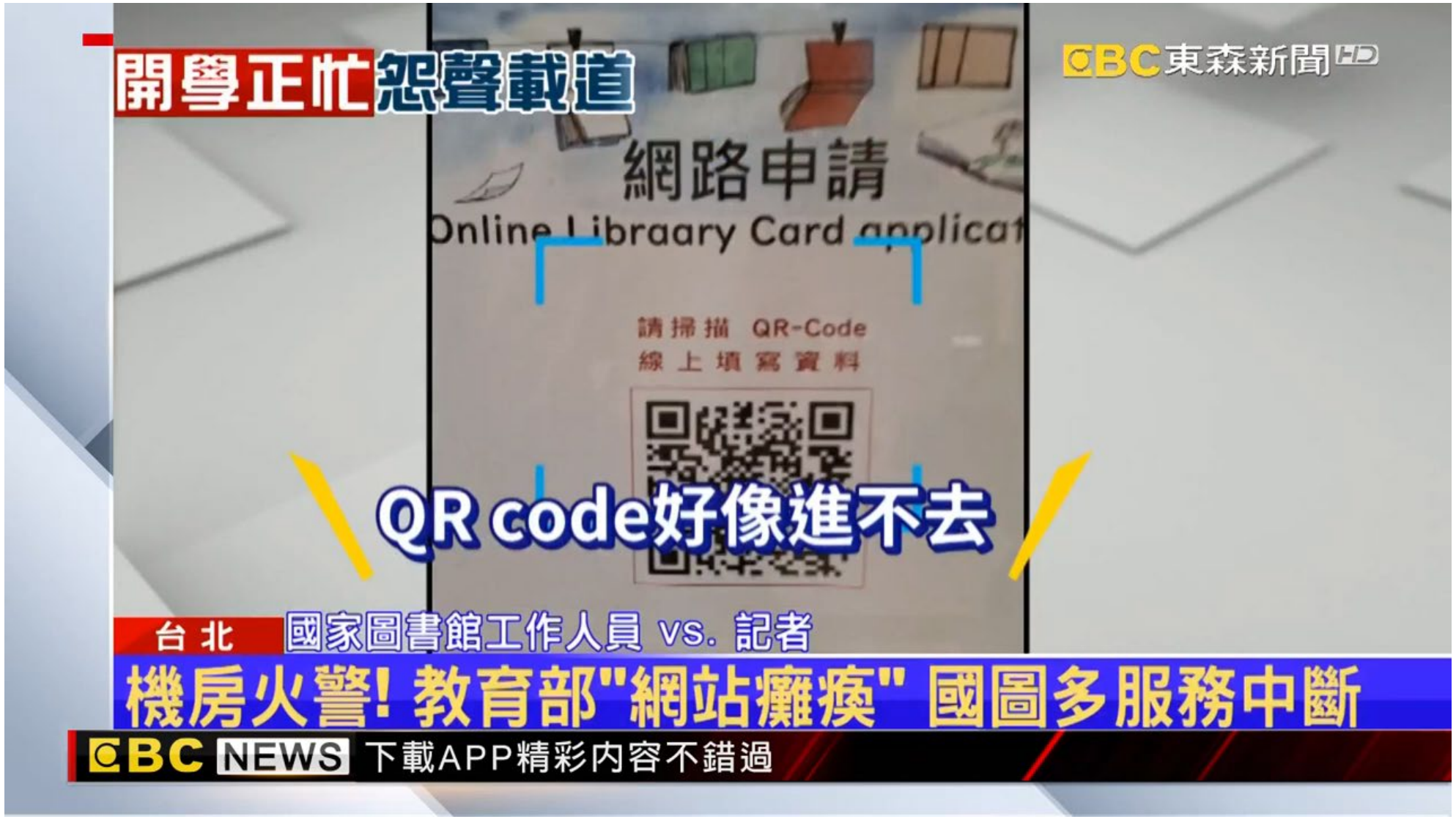
資安(訊)供應商持續遭
駭破壞供應鏈安全



關鍵基礎設施
資安風險倍增

資料來源：1.ENISA Threat Landscape 2021
2.ACSC Annual Cyber Threat Report
3.Microsoft Digital Defense Report
4.Fortinet Global Threat Landscape Report

資通安全情資分享


開學正忙怨聲載道
CBC東森新聞HD
網路申請
Online Libraary Card applicat
請掃描 QR-Code
線上填寫資料
QR code好像進不去
台北 國家圖書館工作人員 vs. 記者
機房火警! 教育部"網站癱瘓" 國圖多服務中斷
CBC NEWS 下載APP精彩內容不錯過

資通安全情資分享


財政部 E-Invoice Platform
電子發票整合服務平台
全民共享
普發現金
電子發票資安漏洞
晚間新聞
PTS EVENING NEWS
電子發票平台資安漏洞 130家公司受影響

資通安全情資分享


公視
19:15:37
中駭客頻入侵
晚間新聞
PTS EVENING NEWS
台鐵與統一超商設備 出現羞辱裴洛西字眼

資通安全情資分享

全國2357萬個資全被駭 科技男花15萬驗真假！檢通緝陸籍駭客

駭客兜售2357萬餘筆我國戶役政資料。（示意圖／翻攝自Pixabay）

去年傳得沸沸揚揚的全台戶役政資料外洩資料，有一名科技男花費約15萬元購買取得，經證實2357萬餘筆份個資經查為我國2018年間全台總人口數的個資，其中包含身分證統一編號、姓名、出生、婚姻狀況代碼、地址、父母姓名、教育程度等個資，幾乎與當年的戶役政資料完全吻合。

北檢分案展開調查，透過科技偵查並與暗網登記所在國連繫後，追查出「OKE」真實身分疑為一名中國籍男子童自強。

資通安全情資分享

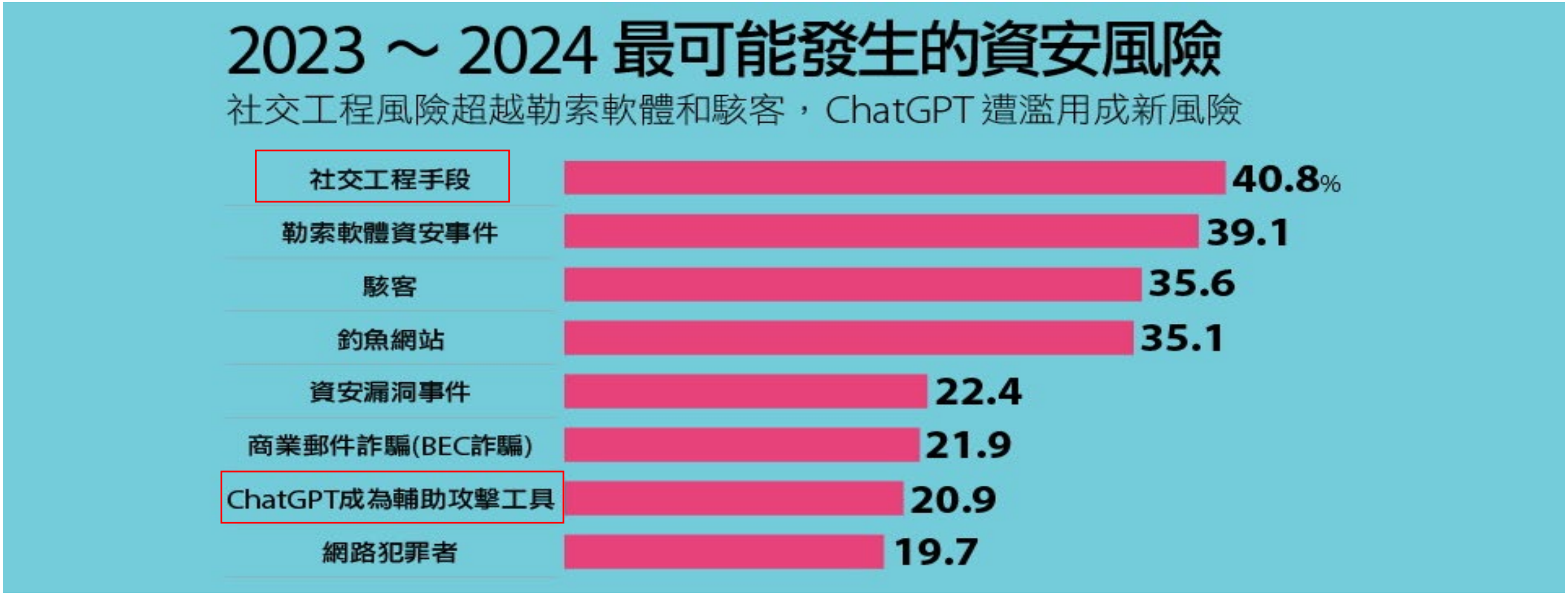
台灣資安威脅猛增！最新報告：2023上半年每秒遭網攻近1.5萬次成亞洲之冠(112/10/13)

全球資安廠商Fortinet近日發布《2023 上半年全球資安威脅報告》，報告顯示台灣資安環境急遽惡化，攻擊數量驚人增加。根據報告，台灣成為亞太地區資安威脅的焦點，每秒約1.5萬次網路攻擊在上半年內肆虐，居亞太之冠。

報告數據顯示，2023年上半年，亞太地區偵測到4,120億次惡意威脅，其中台灣占比逾55%，數量高達2,248億次，每秒近1.5萬次的攻擊頻率令人擔憂。相比2022年同期，台灣的威脅數量更是激增81.6%，最常見的攻擊手法包括分散式阻斷服務（DDoS）攻擊和濫用Double Pulsar漏洞等。

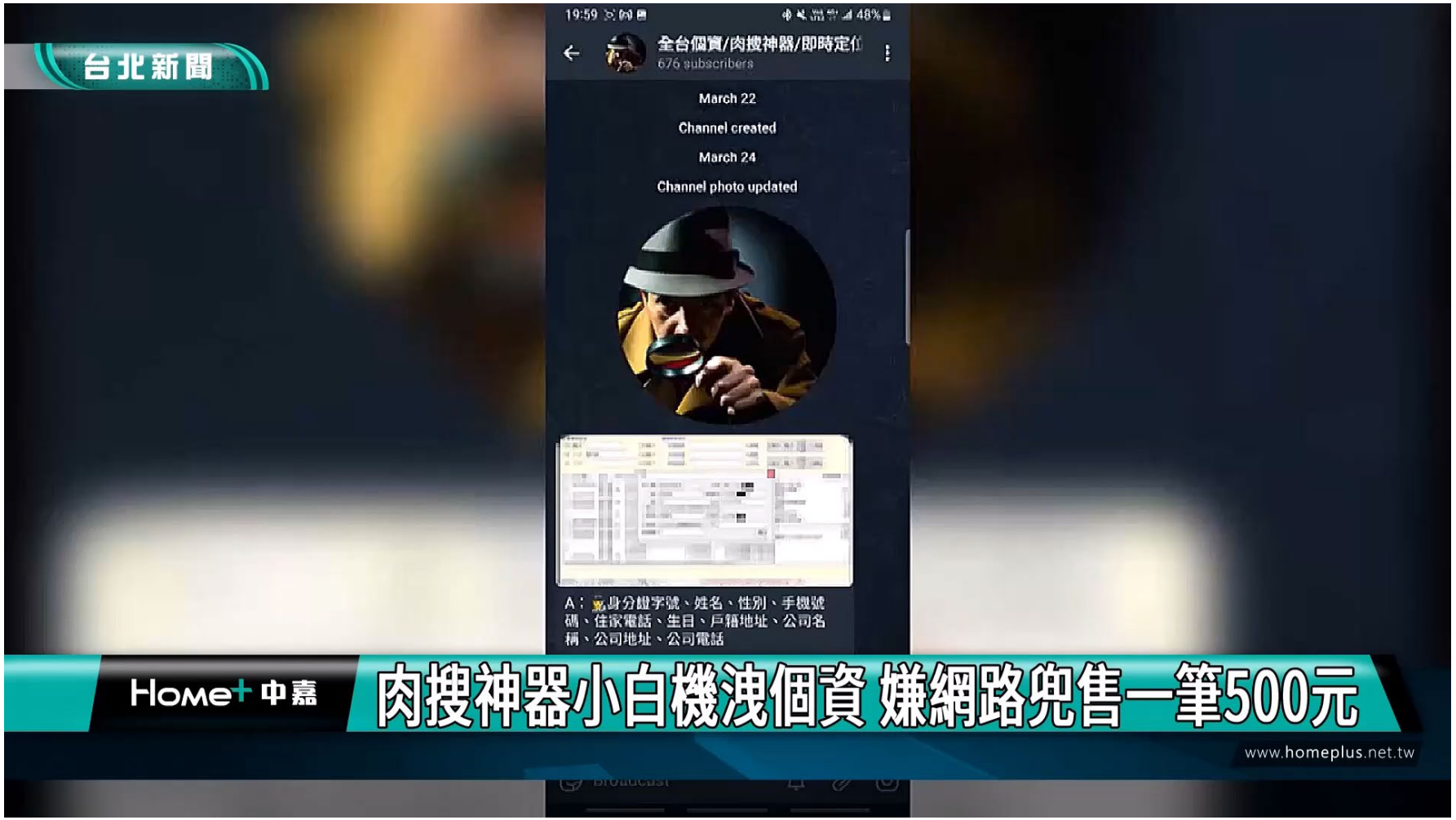
資通安全情資分享

【iThome 2023資安大調查系列2】社交工程風險超越勒索軟體和駭客，ChatGPT濫用成新威脅



個資外洩連環爆-資安法修法4方向

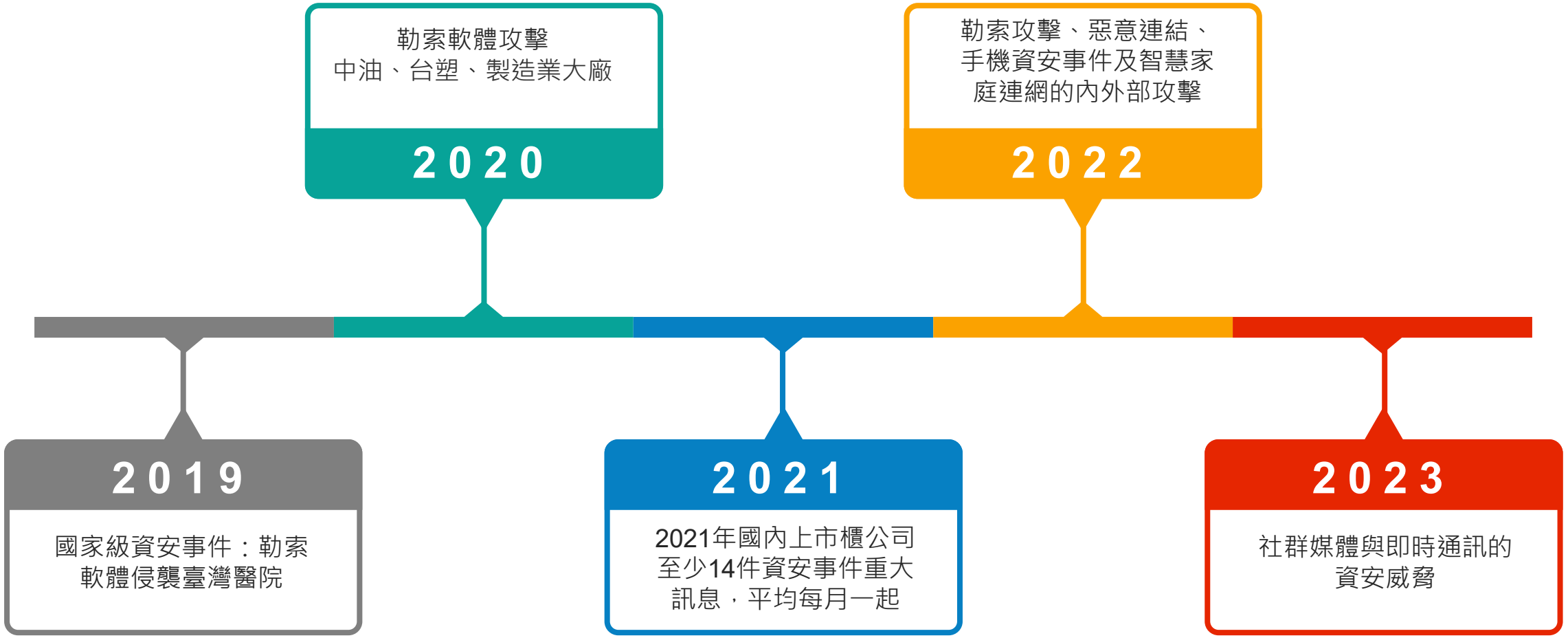
「肉搜神器」查1筆賺500元 台中2男握全台1700萬筆個資遭逮



威脅與趨勢

01

資安事件趨勢


2020
勒索軟體攻擊
中油、台塑、製造業大廠
2022
勒索攻擊、惡意連結、
手機資安事件及智慧家
庭連網的內外部攻擊
2019
國家級資安事件：勒索
軟體侵襲臺灣醫院
2021
2021年國內上市櫃公司
至少14件資安事件重大
訊息，平均每月一起
2023
社群媒體與即時通訊的
資安威脅

- ✓ 雲端漏洞
- ✓ 資料外洩
- ✓ 混合或遠端工作環境風險
- ✓ 行動設備攻擊
- ✓ 網路釣魚變得更加複雜
- ✓ 勒索軟體策略不斷演變
- ✓ 密碼劫持
- ✓ 網路實體攻擊

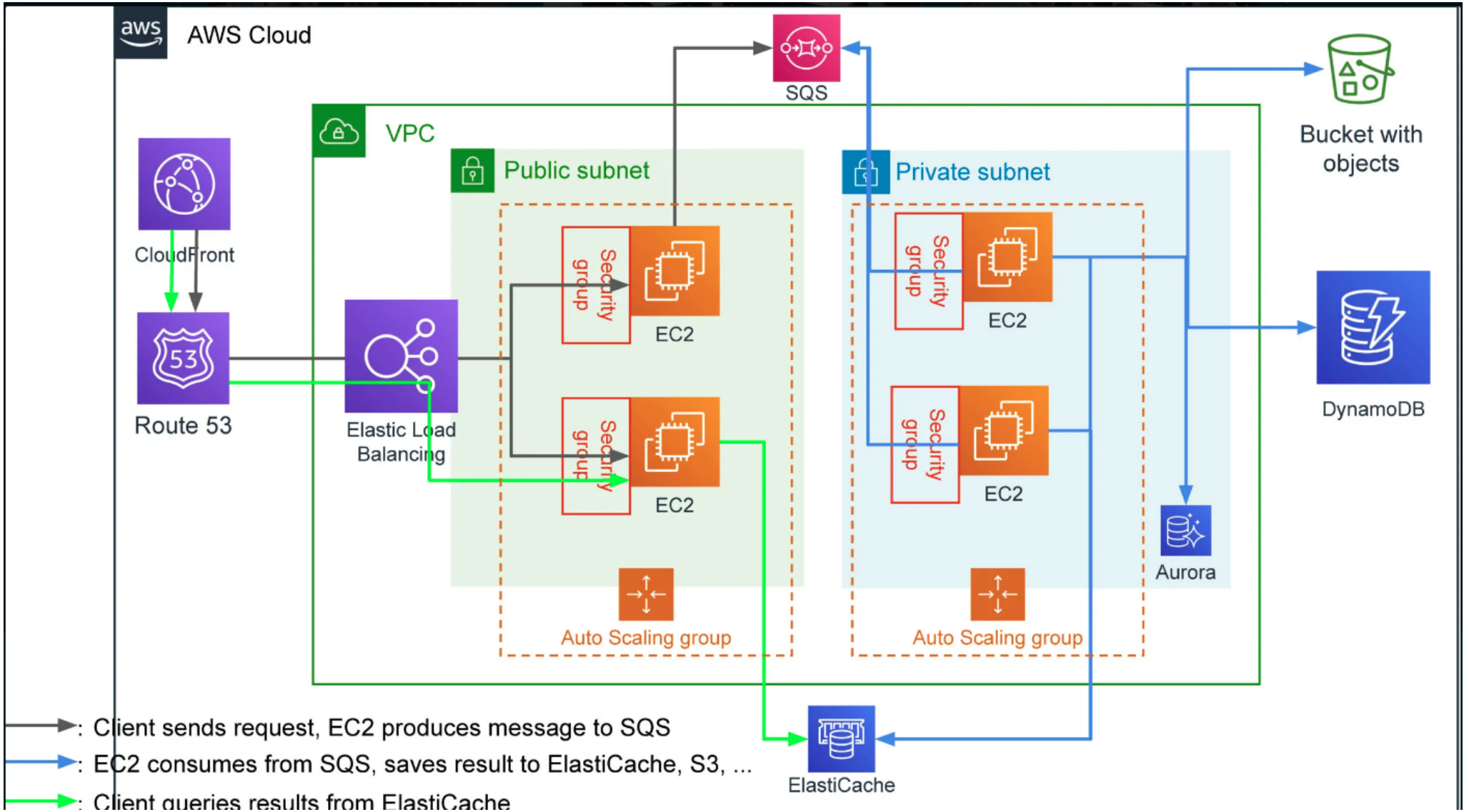
- ✓ 國家級攻擊
- ✓ IOT攻擊
- ✓ 智能醫療設備和電子病歷的漏洞
- ✓ 第三方漏洞
- ✓ 聯網汽車和自駕車隱私問題
- ✓ 社交工程
- ✓ 網路安全專業人員嚴重短缺
- ✓ 正在採取哪些措施來應對

整 體 威 脅 情 勢

資　訊　安　全

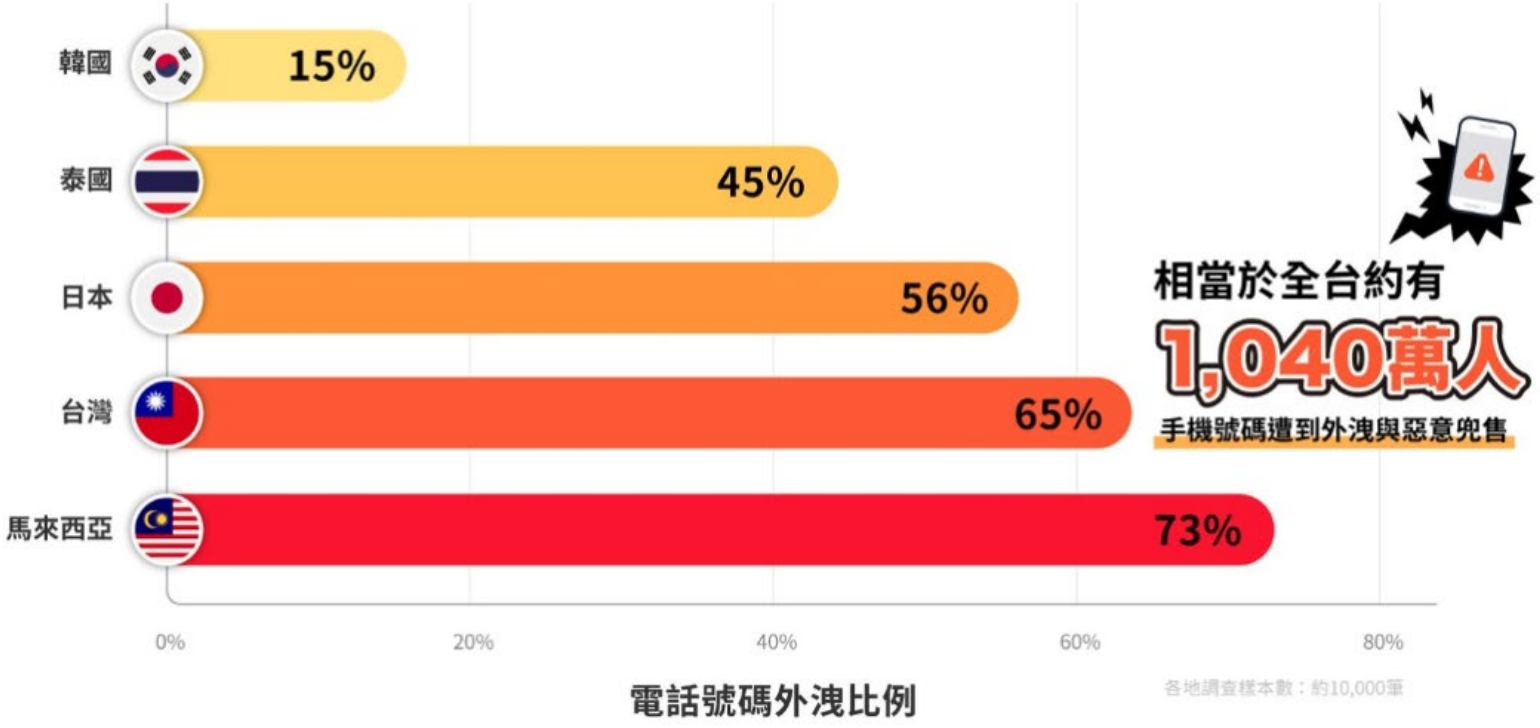
Top Cybersecurity Threats in 2023

雲端安全


AWS Cloud
SQS
VPC
Public subnet
Private subnet
Bucket with objects
CloudFront
Route 53
Elastic Load Balancing
Security group
EC2
Security group
EC2
Security group
EC2
Security group
EC2
DynamoDB
Aurora
Auto Scaling group
Auto Scaling group
ElastiCache
: Client sends request, EC2 produces message to SQS
: EC2 consumes from SQS, saves result to ElastiCache, S3, ...
: Client queries results from ElastiCache

資料外洩

根據非營利組織Privacy Rights Clearinghouse的統計資料，在過去十年中，共有超過40億起資料被盜或外洩的紀錄，並有超過7,000起個別違規事件，大規模資料洩漏事件的發生頻率正在上升。由於目前大量個資儲存在網路上，因此其落入網路罪犯手中的情況日益普遍。



	第一名	第二名	第三名	第四名	第五名	第六名	第七名
台灣	登入密碼	電話號碼	姓名	國籍	Email	地址	出生年月日
泰國	登入密碼	電話號碼	姓名	國籍	地址	出生年月日	Email
馬來西亞	登入密碼	電話號碼	姓名	地址	國籍	出生年月日	Email
日本	姓名	登入密碼	電話號碼	國籍	地址	Email	出生年月日
韓國	姓名	登入密碼	電話號碼	國籍	地址	Email	出生年月日

遠距辦公

面向	項目	建議內容
政策制度面	遠距辦公政策制定	制定遠距辦公流程、資安管理政策，以及員工權責規範
	遠距辦公設備管理	設備管理辦法，包括登記、遺失、註銷流程，並制定企業設備安全設定項目
	網路管理政策	因應前述政策的網路管理方法
	員工意識培訓	遠距辦公政策宣導、遠距辦公資安意識培訓
	政策定期審查	規劃政策落實度評量方法，並定期審查與調整政策內容
設備管理層面	遠距辦公設備盤點	建議盤點遠距辦公設備，做為設備管理的依據
	行動裝置管理(MDM)	登入功能、APP 應用管理等，進階功能如遠端鎖定、遠端清除
	身分識別與存取管理	建議使用多因子身分驗證
	防毒軟體或其它資安防護軟體	建議再加裝惡意軟體檢測工具
	安全設定	建議為強制安全設定，或以指引、稽核形式執行
網路管理層面	VPN 連線	應考量 VPN 伺服器之承載量，確保遠距連線穩定性
	身分識別與存取管理	建議使用多因子身分驗證
	安全區域劃分	可區分為公共、辦公、機敏等區域，使用不同層級的管理方式
	測試安全機制	除定期資安檢測外，應考量遠距辦公情境，納入檢測項目
資料安全層面	重要資料服務盤點	進行資料盤點，做為資料管理依據，進階可建立企業內容管理(ECM)機制
	資料加密	建議對遠端辦公設備進行全機加密，亦或依據資料盤點結果，加密機敏資料
	最小的存取權限	資料存取權限應依據最小權限原則進行規劃
	資料管理功能	重要資料存取應有系統日誌紀錄以供稽核，建議導入虛擬移動基礎設施(VMI)，使資料不需傳輸至終端操作

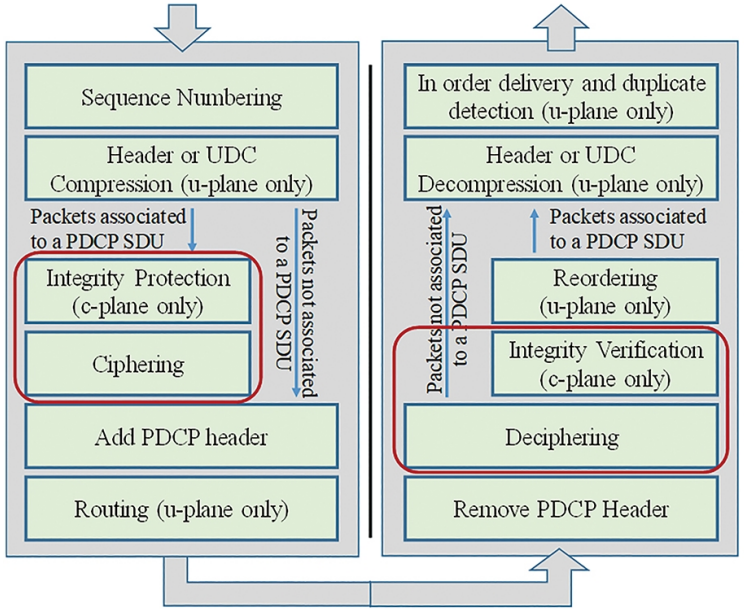
行動設備

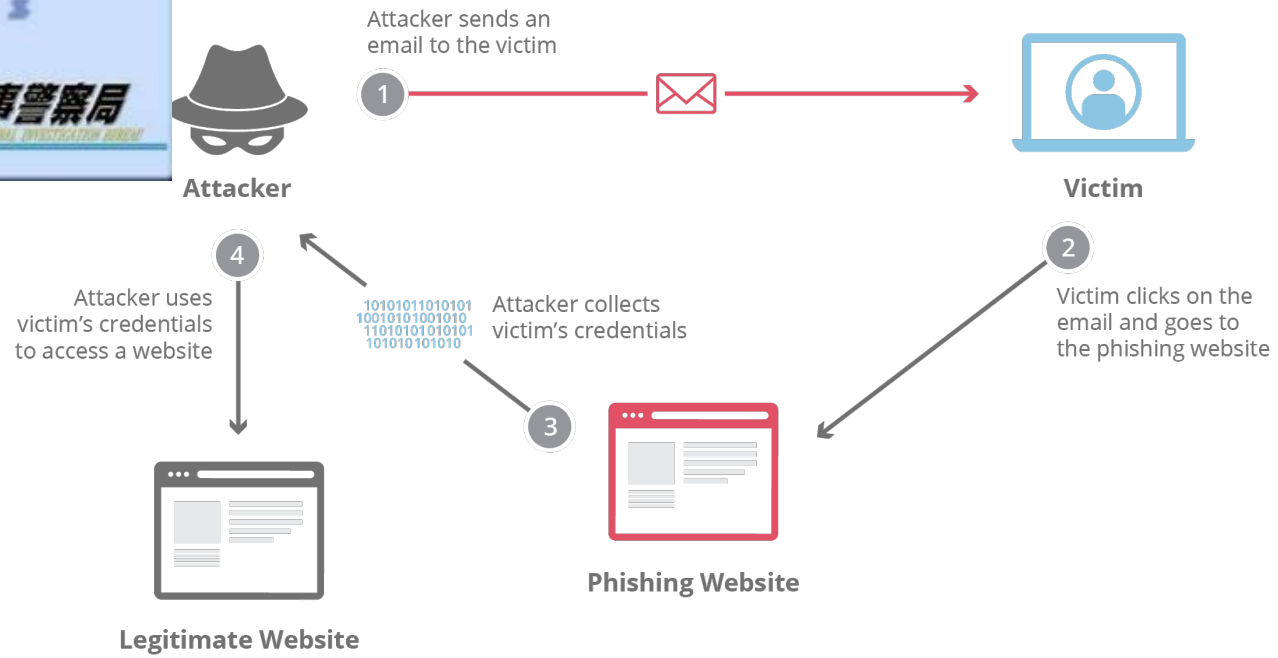

請稍候掃描正在運行...
警告!
您的Apple手機已被感染病毒!
建議現在快速掃描.
確定


8:40
4G
8月
日 一 二 三 四 五 六
26 27 28 29 30 31 1
初六 初七 初八 初九 初十 十一 十二
2020年8月1日 週六 庚子年六月十二
中午
下午1時
隐藏您的IP地址以进行匿名浏览和洪流
https://entysaturesc.club/14iHqZ6
下午2時
删除iPhone上可能的感染，立即保护您的数据
https://entysaturesc.club/14iHq0t
下午3時
您的iPhone可能不受保护！单击以保护它。%
https://entysaturesc.club/14iHq0A
下午4時
下午5時
%确保您的在线保护，立即单击以获得帮助
https://entysaturesc.club/14iHq0J
下午6時
下午7時
删除iPhone上可能的感染，立即保护您的数据
https://entysaturesc.club/14iHq0y
下午8時
下午9時
%清除您的iPhone免受可能的恶意攻击！
https://entysaturesc.club/14iHq0r
下午10時
%清除您的iPhone免受可能的恶意攻击！
https://entysaturesc.club/14iHq0O
下午11時
删除iPhone上可能的感染，立即保护您的数据
https://entysaturesc.club/14iHq0C
上午12時
今天
行事曆
收件匣

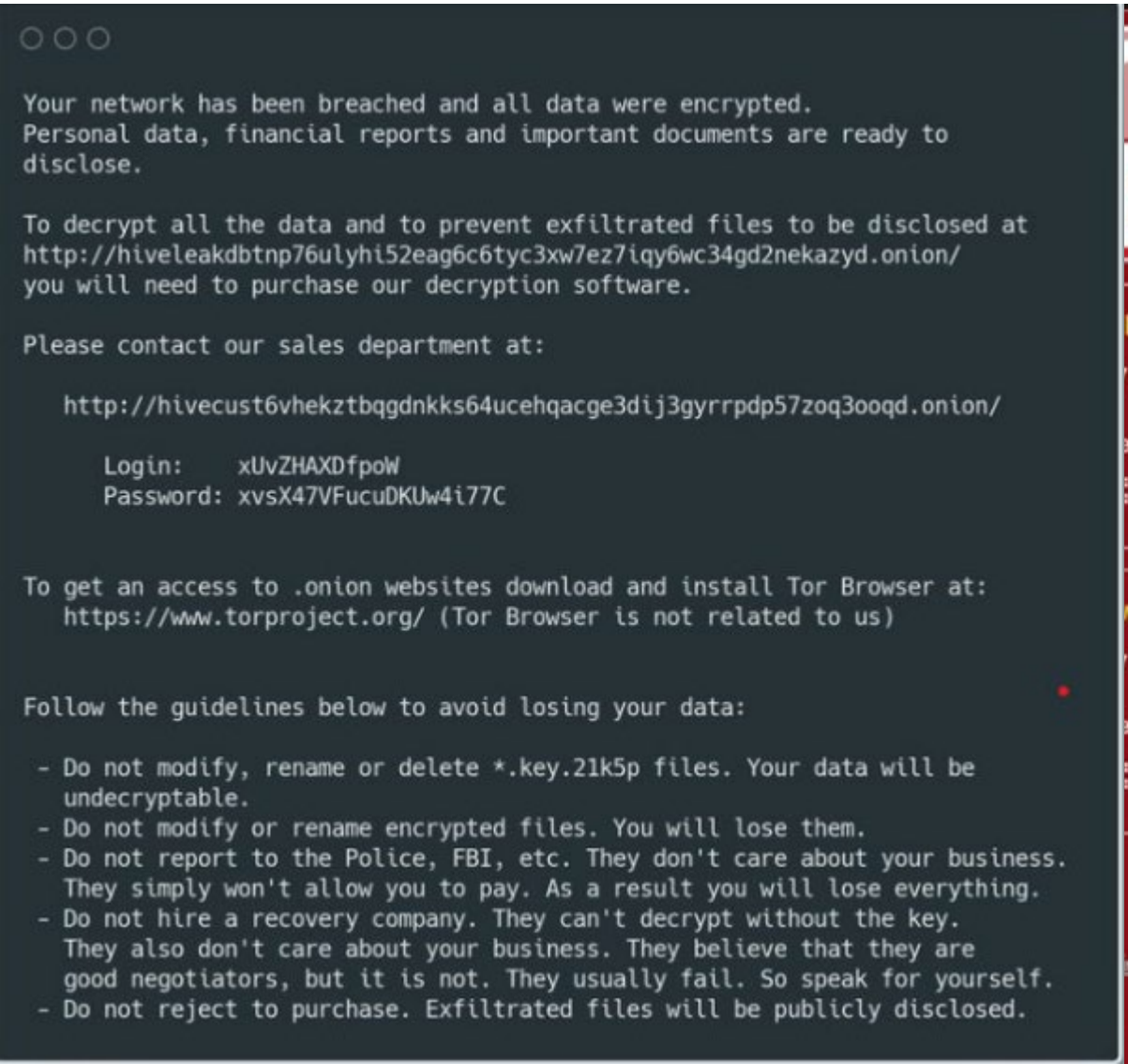
網路釣魚


假基地臺發送釣魚簡訊詐騙流程圖
輸入個資、信用卡號、簡訊驗證碼
假網站
被害人
發送釣魚簡訊
行動偽基站
電信網路
金融
綁定行動支付帳號
境外機房
盜刷信用卡
銷贓
車手集團
刑事警察局


Sequence Numbering
Header or UDC Compression (u-plane only)
Packets associated to a PDCP SDU
Integrity Protection (c-plane only)
Ciphering
Packets not associated to a PDCP SDU
Add PDCP header
Routing (u-plane only)
In order delivery and duplicate detection (u-plane only)
Header or UDC Decompression (u-plane only)
Packets not associated to a PDCP SDU
Packets associated to a PDCP SDU
Reordering (u-plane only)
Integrity Verification (c-plane only)
Deciphering
Remove PDCP Header

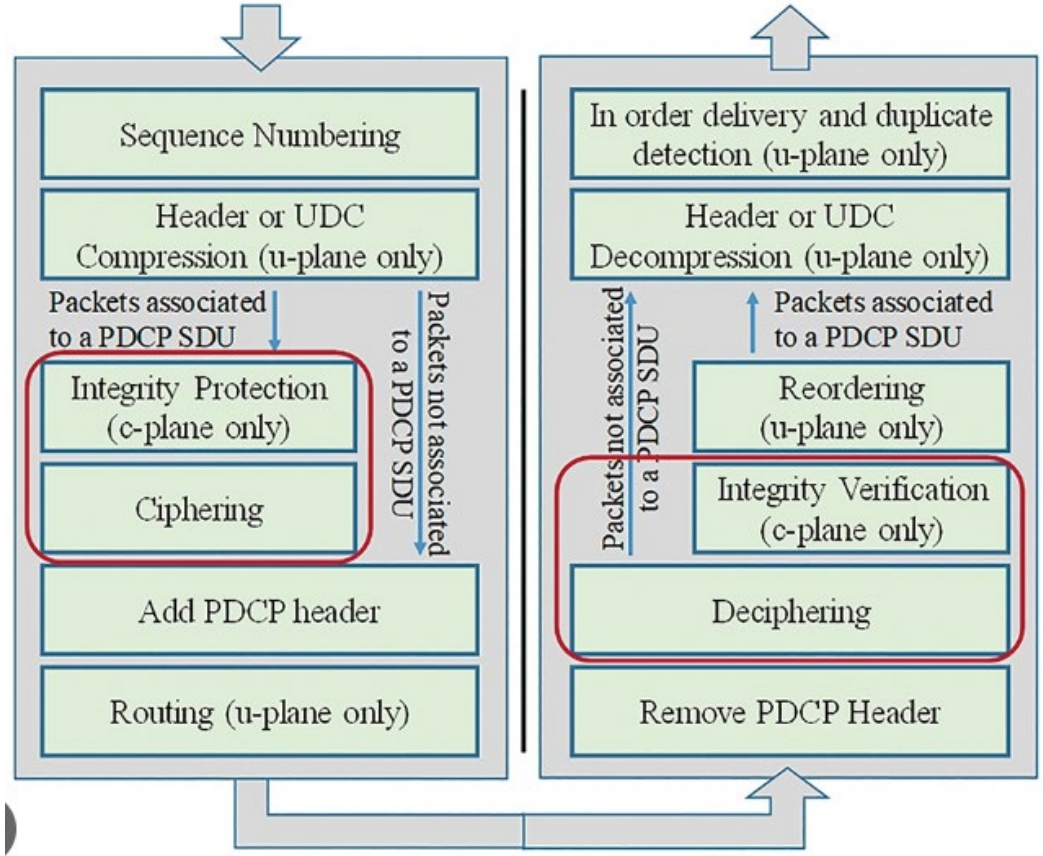

Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
4
Attacker uses victim's credentials to access a website
Phishing Website
Legitimate Website

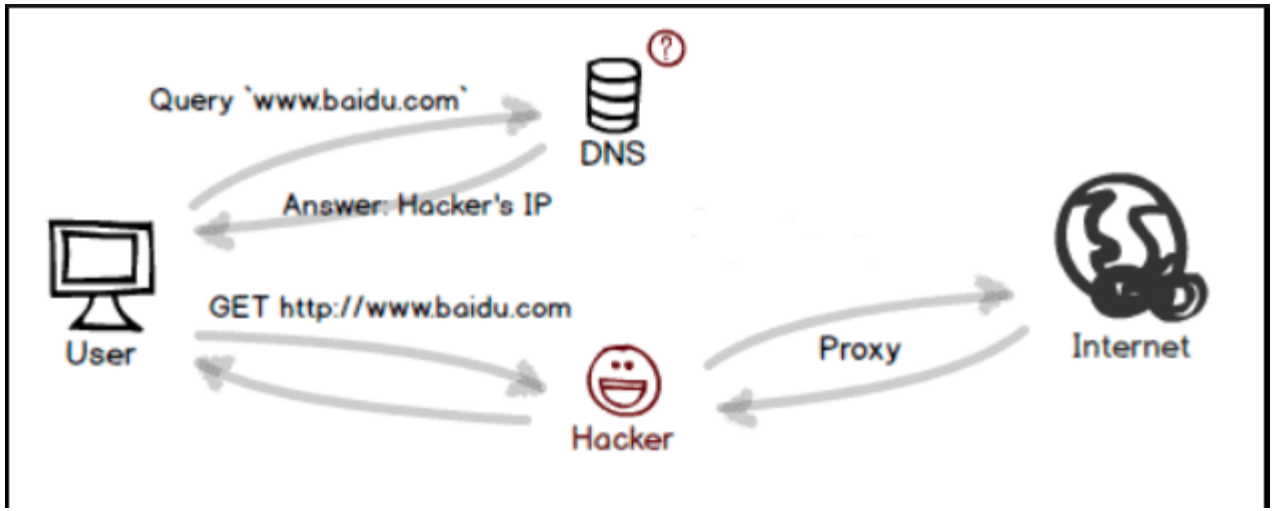
勒索軟體

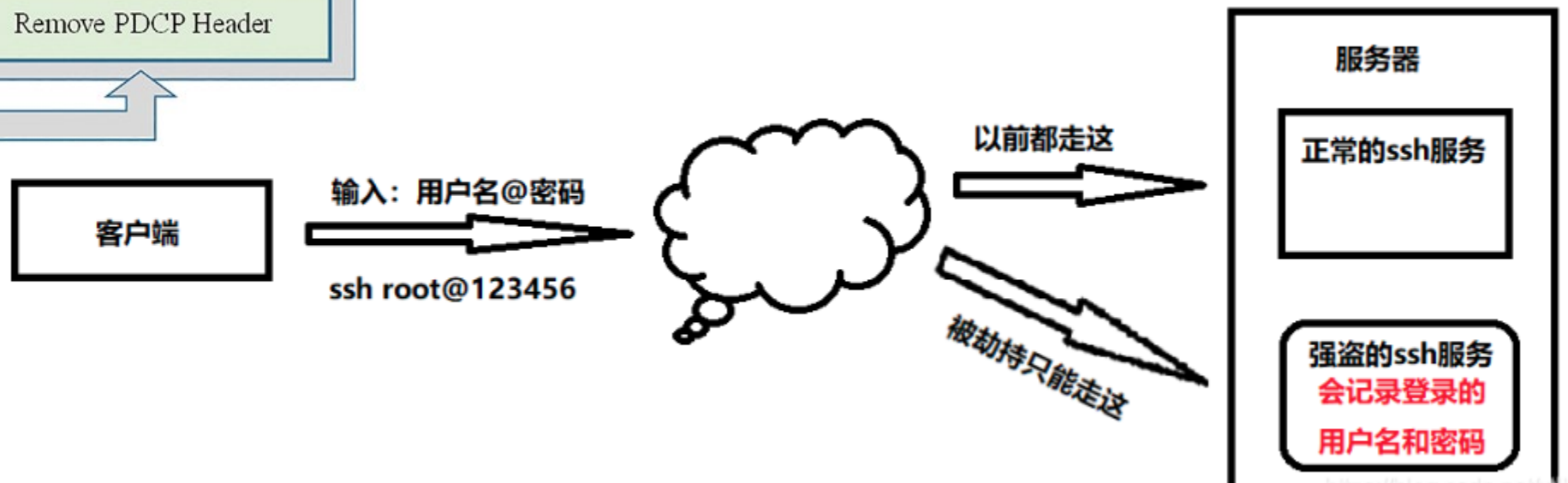

Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.
To decrypt all the data and to prevent exfiltrated files to be disclosed at http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/ you will need to purchase our decryption software.
Please contact our sales department at:
http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd.onion/
Login: xUvZHAXDfpoW
Password: xvsX47VFucuDKUw4i77C
To get an access to .onion websites download and install Tor Browser at:
https://www.torproject.org/ (Tor Browser is not related to us)
Follow the guidelines below to avoid losing your data:
- Do not modify, rename or delete *.key.21k5p files. Your data will be undecryptable.
- Do not modify or rename encrypted files. You will lose them.
- Do not report to the Police, FBI, etc. They don't care about your business. They simply won't allow you to pay. As a result you will lose everything.
- Do not hire a recovery company. They can't decrypt without the key. They also don't care about your business. They believe that they are good negotiators, but it is not. They usually fail. So speak for yourself.
- Do not reject to purchase. Exfiltrated files will be publicly disclosed.


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

密碼劫持

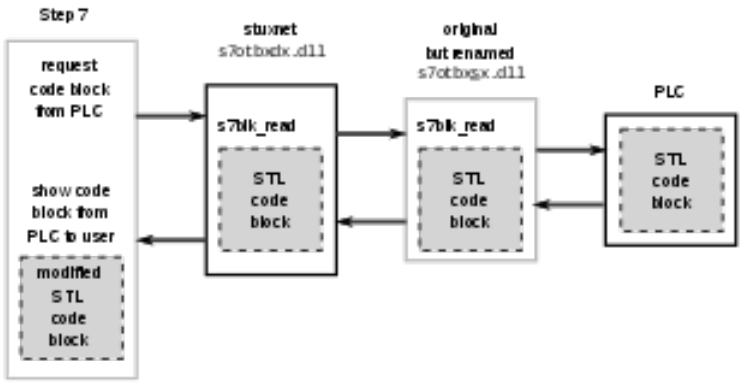

Sequence Numbering
Header or UDC Compression (u-plane only)
Packets associated to a PDCP SDU
Packets not associated to a PDCP SDU
Integrity Protection (c-plane only)
Ciphering
Add PDCP header
Routing (u-plane only)
In order delivery and duplicate detection (u-plane only)
Header or UDC Decompression (u-plane only)
Packets not associated to a PDCP SDU
Packets associated to a PDCP SDU
Reordering (u-plane only)
Integrity Verification (c-plane only)
Deciphering
Remove PDCP Header

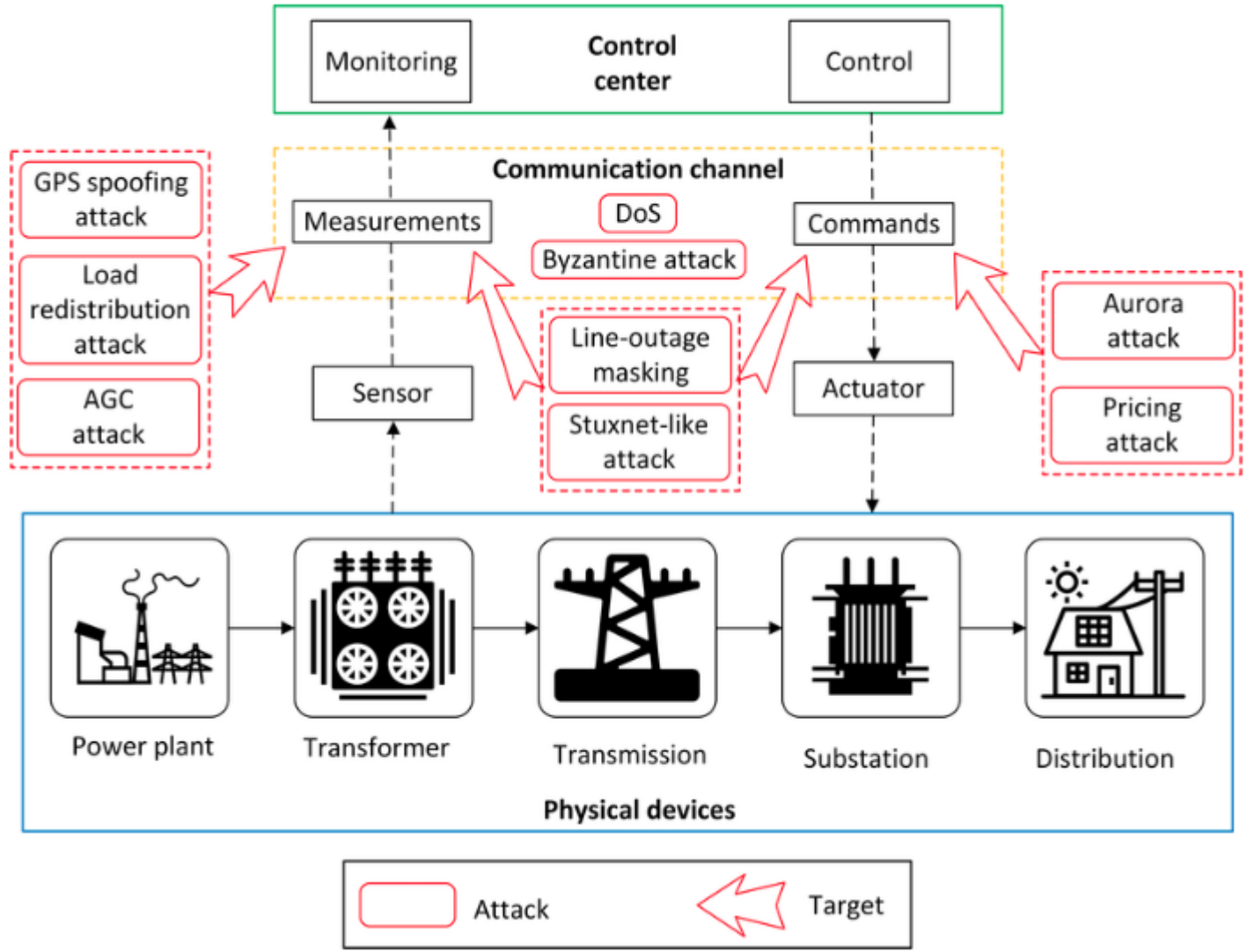

Query `www.baidu.com`
DNS
Answer: Hacker's IP
User
GET http://www.baidu.com
Proxy
Internet
Hacker


客户端
输入：用户名@密码
ssh root@123456
以前都走这
被劫持只能走这
服务器
正常的ssh服务
强盗的ssh服务
会记录登录的
用户名和密码

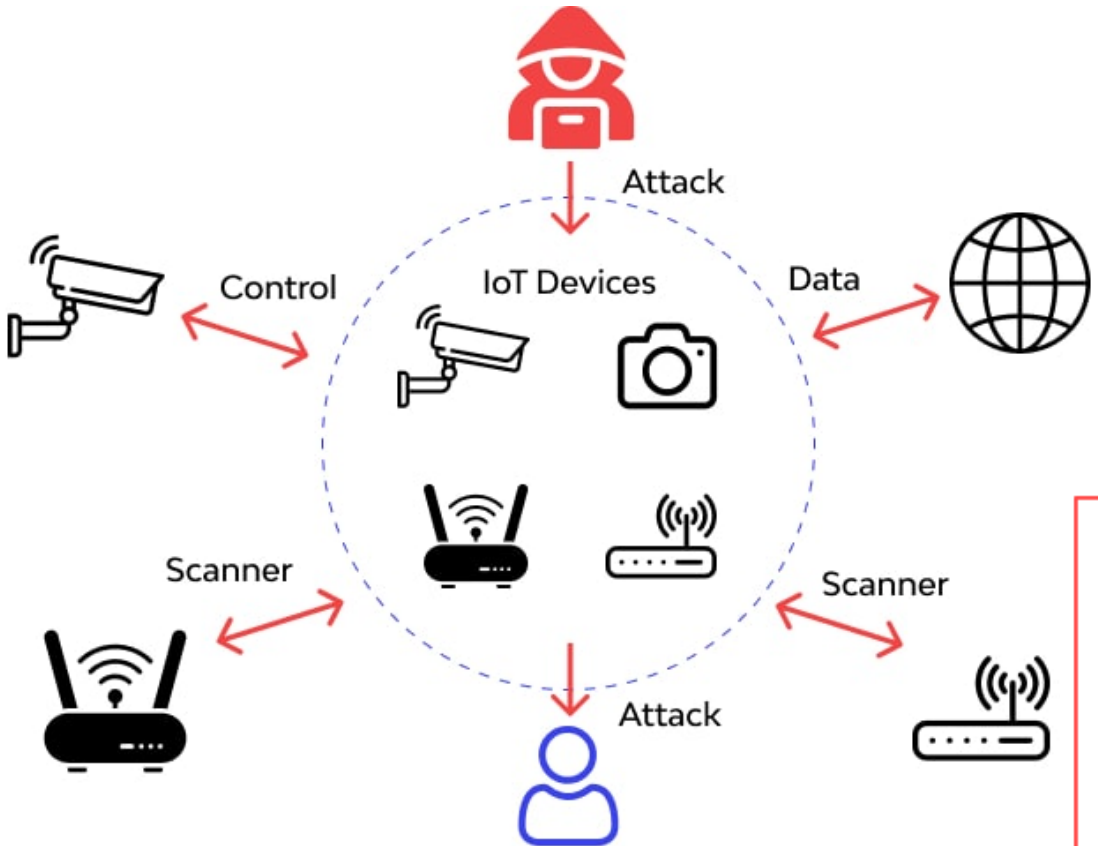
網路實體攻擊

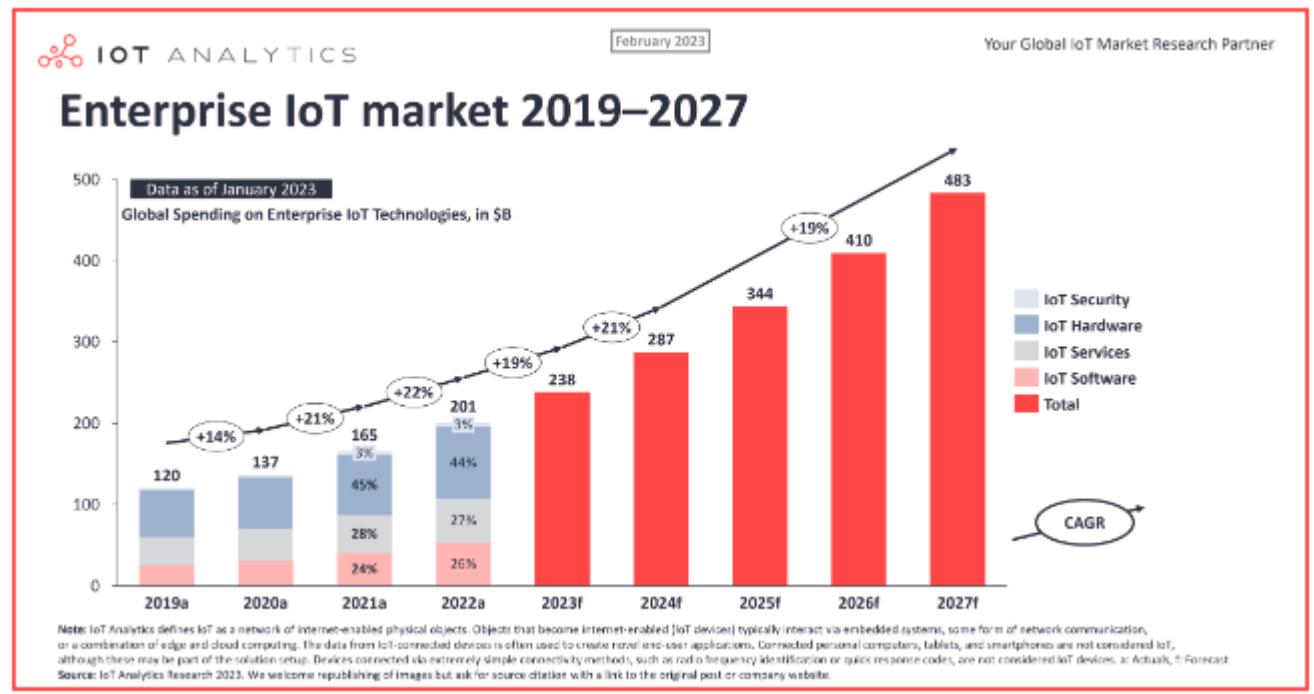
網路實體攻擊是影響操作、損壞財產或以其他方式影響實體環境的安全漏洞。





IOT攻擊


Attack
Control
IoT Devices
Data
Scanner
Scanner
Attack


IOT ANALYTICS
February 2023
Your Global IoT Market Research Partner
Enterprise IoT market 2019–2027
Data as of January 2023
Global Spending on Enterprise IoT Technologies, in $B
500
400
300
200
100
0
+14%
+21%
+22%
+19%
+21%
+19%
120
137
165
201
238
287
344
410
483
3%
45%
28%
24%
3%
44%
27%
26%
IoT Security
IoT Hardware
IoT Services
IoT Software
Total
CAGR
2019a
2020a
2021a
2022a
2023f
2024f
2025f
2026f
2027f
Note: IoT Analytics defines IoT as a network of internet-enabled physical objects. Objects that become internet-enabled (IoT devices) typically interact via embedded systems, some form of network communication, or a combination of edge and cloud computing. The data from IoT-connected devices is often used to create novel end-user applications. Connected personal computers, tablets, and smartphones are not considered IoT, although these may be part of the solution setup. Devices connected via extremely simple connectivity methods, such as radio frequency identification or quick response codes, are not considered IoT devices. a: Actuals, f: Forecast
Source: IoT Analytics Research 2023. We welcome republishing of images but ask for source citation with a link to the original post or company website.

社交工程

- **冒名電話（Pretexting）**是透過電話對話，以預先編造的故事或藉口勸服目標受害人去做一些事，例如：透露某些資料等。
- **網絡釣魚（Phishing）**是一種騙取個人資料的技術。通常 騙子會以合法商業機構（例如：銀行或信用卡公司）的名義發送電郵給受害者，要求用戶提供資料以作核實，並警告如不執行後果嚴重。
- **電話詐騙（Phone-phishing or Vishing）**以複製其它銀行或商業機構的自動語音電話系統（IVR）中的語音，來建立粗糙但讓人感覺正規的電話系統。受害人會被要求（通常是通過網絡釣魚電郵）撥打電郵中提供的免費電話聯繫「銀行」來「查核」電郵的真偽。
- **利誘（Baiting）**就像是現實世界中的特洛伊木馬，它使用真實的物件作為媒介並利用受害者好奇或貪便宜的心理。在這個騙局中，騙徒會故意將一些被病毒感染了的磁碟片、光盤或 USB 等包裝得如同正版並且貼上引人注目的標籤，放置在顯眼的地點（例如：洗手間、電梯、人行道、停車場），等待受害者使用這些裝置。
- **等價交換（Quid pro quo）**騙徒隨意撥打一些公司的電話號碼，並聲稱自己是某技術維修部打來的。無論如何，騙徒總會遇到真正有技術問題並需要幫助的人，他 / 她甚至會感謝騙徒打電話回來幫助他們。
- **魚叉式網絡釣魚（Spear phishing）**是透過電郵企圖欺詐某些特定的組織或機構，尋求在未經授權的情況下進入其機密數據的機會。類似網絡釣魚的慣常手法，魚叉式網絡釣魚的電郵看似來自可靠來源。網絡釣魚郵件通常看起來是來自一家大型知名公司或是有廣大會員基礎的網站，例如 eBay 或 PayPal。在魚叉式網絡釣魚中，電郵很可能看似來自某家公司老闆或管理階層的個人郵箱。

資訊安全

02

ISMS改版主條文差異

ISO 27001:2022

1.名稱

2.頁數

3.術語與定義(參考資訊)

4.新增要求(4.2瞭解利害關係方的需求與期望)

5.強化過程導向(4.4資訊安全管理系統)

6.新增要求(6.2資訊安全目標與達成之規劃)

7.新增要求(6.3變更規劃)

8.簡化要求(7.4溝通)

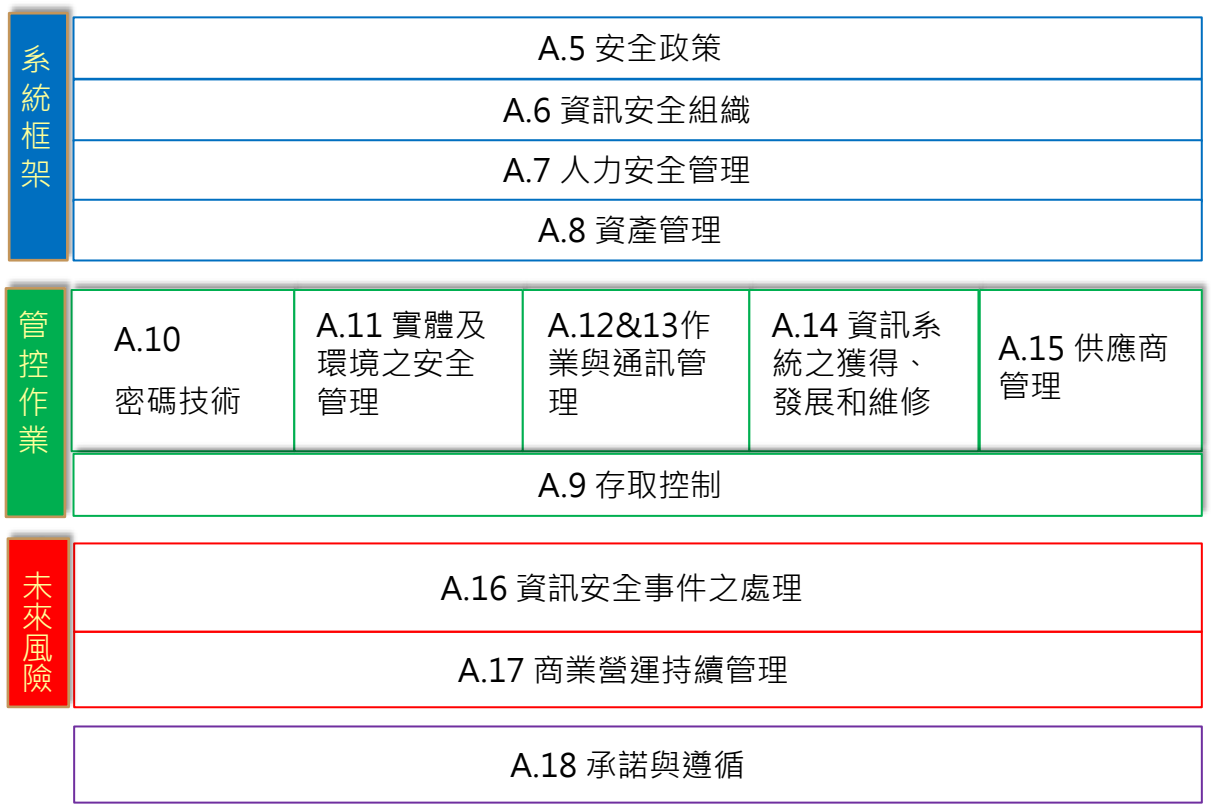
9.新增要求(8.1運作的規劃與控管)

10.新增要求(9.1 監督、量測、分析與評估)

11.要求架構變更(9.2、9.3)

12.要求架構變更(10.改善)

附錄A 差異



ISO 27002:2013

ISO 27002:2022

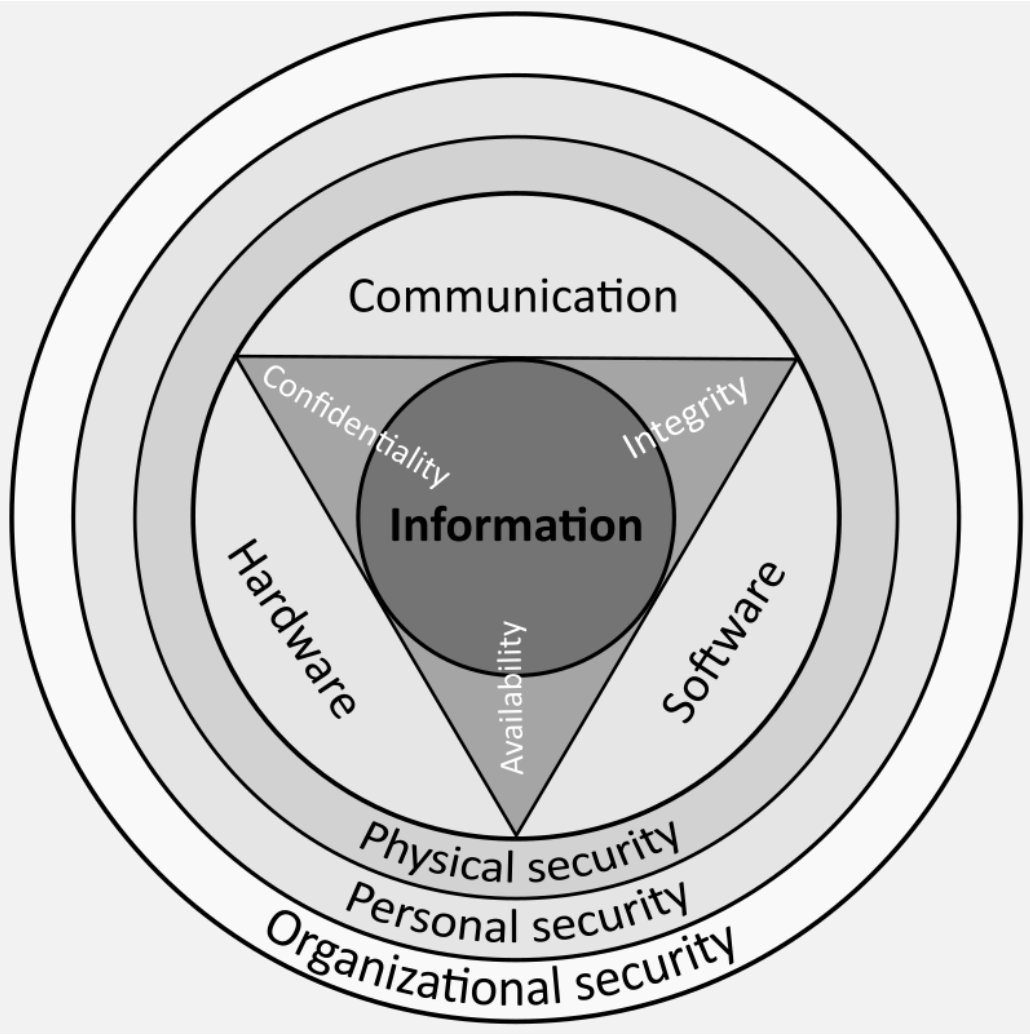
控制措施數量

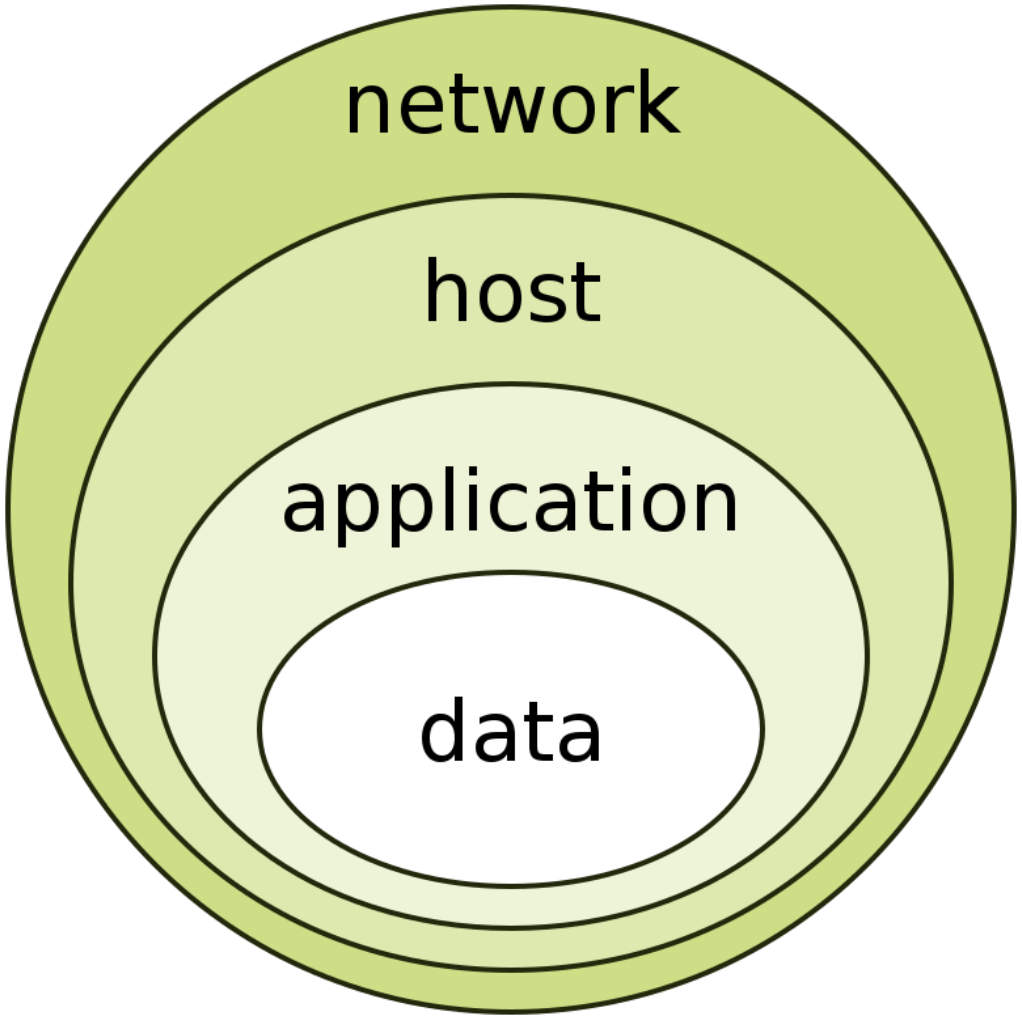
114項控制措施

93項控制措施

新增控制措施

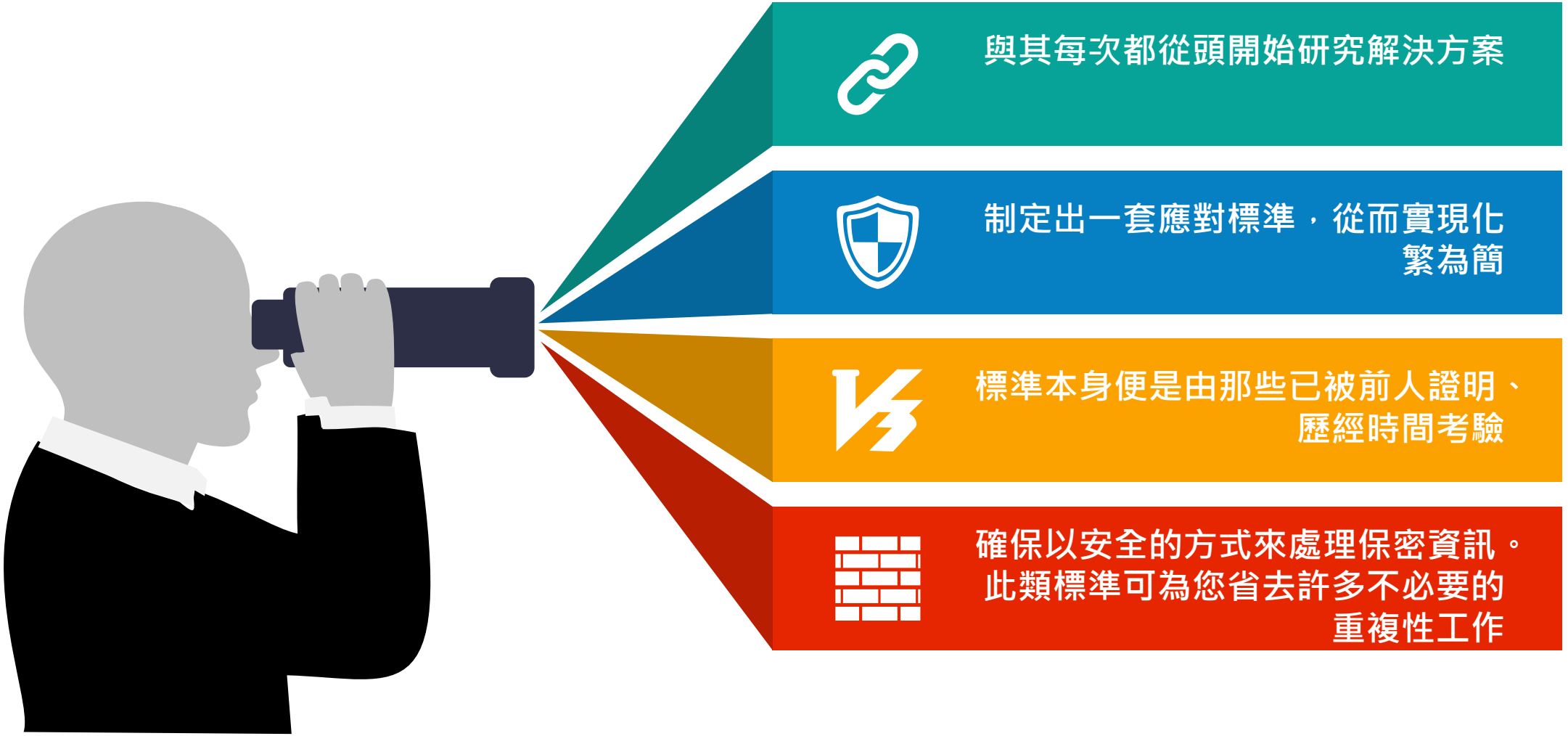
編號	控制措施名稱
5.7	威脅情資
5.23	使用雲端服務之資訊安全
5.30	為營運持續性做好資通技術（ICT）的準備
7.4	實體安全監控
8.9	組態管理
8.10	資訊刪除
8.11	資料遮蔽
8.12	預防資料洩漏
8.16	活動監控
8.22	網頁過濾
8.28	安全編碼


Communication
Confidentiality
Integrity
Information
Availability
Hardware
Software
Physical security
Personal security
Organizational security


network
host
application
data

資　訊　安　全　架　構

誰來定義"安全"標準


與其每次都從頭開始研究解決方案
制定出一套應對標準，從而實現化繁為簡
標準本身便是由那些已被前人證明、歷經時間考驗
確保以安全的方式來處理保密資訊。此類標準可為您省去許多不必要的重複性工作

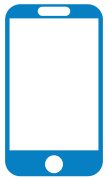
作業安全

03

社群媒體與即時通訊

社群媒體與即時通訊資安威脅

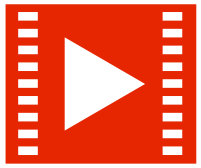
惡意軟體傳播管道.



機敏資料外洩

社群媒體與即時通訊所具備的的資訊分享、快速傳播、社群影響、商業內容等特性，在駭客集團眼中已成為蒐集或竊取資訊的最佳管道

社交工程攻擊.



隱私保護議題.

保護在社群媒體上發布的內容

01 確保只有授權人員才能發佈內容

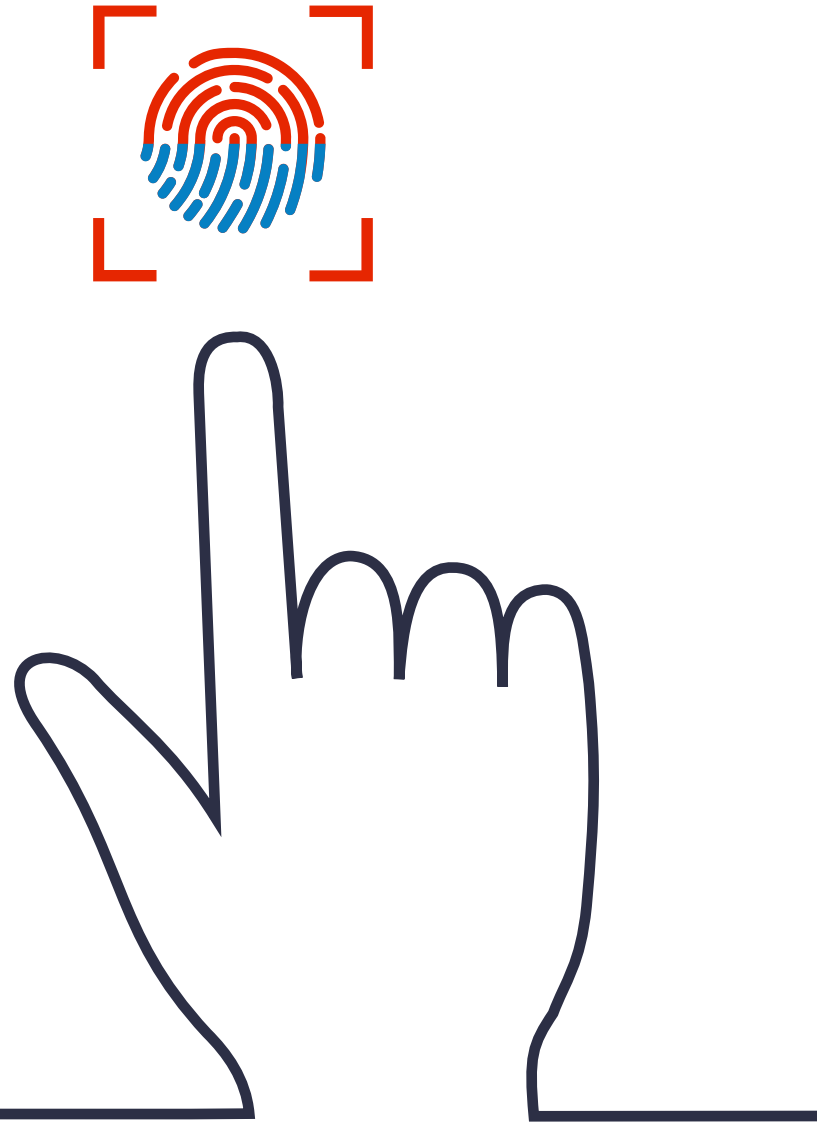
02 對離職者或調離部門者進行追蹤管理

03 使用提供良好安全功能的社交媒體平台

04 確保內容在發佈前可以經過審核和授權

05 使用組織設備創建和發佈內容

06 制定緊急損害復原計劃



如何安全使用社群媒體

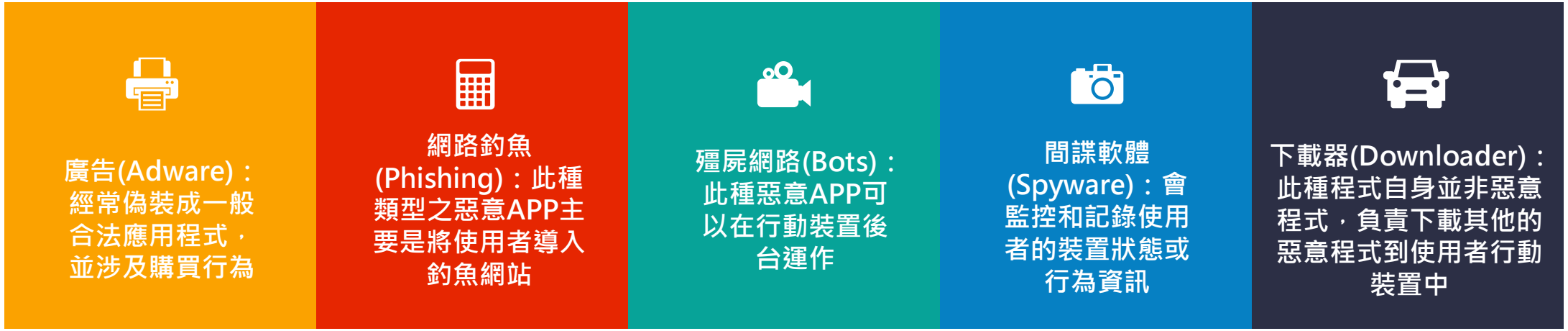
01 依循來自社交媒體平台的安全建議，並設定安全 policy

02 使用雙因子身分驗證 (2FA)來保護帳戶

03 制定政策並強化存取網路與端點資料的控制措施

04 建立與供應商及協力廠商的安全管理機制

行動應用APP資安威脅及案例



隨著APP數量以及使用者將機敏資訊存於行動裝置的比例增加，惡意APP對使用者的威脅以及損害程度逐漸上升。除了個人使用者外，企業同樣也遭受惡意APP的入侵，這些惡意APP可被分為上面五種類型

所有的惡意APP中，比例最高的為工具類型，其次為生活風格類型，再其次為娛樂類型之APP。工具類型的APP通常會要求給予較高的使用權限，駭客即利用此較高的授權，進行資料竊取、修改設定等惡意行為

即時通訊安全

- **最小化**即時通訊軟體的權限設定，如: 關閉自動下載或只允許通訊錄的人員通訊
- **避免**透過即時通訊軟體**提供機密資料**，並確認對方身份
- **定期更新**即時通訊軟體
- **封鎖不明使用者**的訊息
- 了解即時通訊軟體的**安全機制**，如: 訊息加密、訊息刪除、雙因子身分驗證、安全設定、雲端備份機制等，並採用適合該軟體應用安全的設定
- **關閉自動接受好友**申請與搜尋功能
- **不**隨意**開啟連結**
- 使用即時通訊軟體的設備應啟用**螢幕保護程式**、使用電腦或網頁版的通訊軟體後確實進行**登出**
- 企業應**明訂即時通訊軟體政策**，如: 指定員工使用特定即時通訊軟體不可傳送企業機密與文件、使用即時通訊軟體的手機應設定自動螢幕鎖定及加密儲存等
- 訂定行動裝置使用**管理機制**
- 定期舉行員工資**安意識教育訓練**

手機

你該養成的良好習慣

- 從官方網站下載應用程式和更新。
- 下載應用程式前，請閱讀其他用戶的評論,並檢查一下應用程式要求的所有權限。
- 隨時保持裝置作業系統與應用程式更新至最新版本。
- 立即更換所有網路帳號的密碼。
- 刪除所有不明的應用程式。
- 避免連上公共或無安全性的 WI-FI 網路。
- 藍牙不用時請關閉。
- 如果遭到駭客入侵，立即通知親朋好友忽略任何可疑訊息。
- 最後真的不得已時，備份重要資料，並將裝置回復至原廠設定。
- 使用能即時偵測網址安全性，為您封鎖惡意網站、詐騙連結、假購物網站和假臉書粉專等具有安全風險的防毒軟體

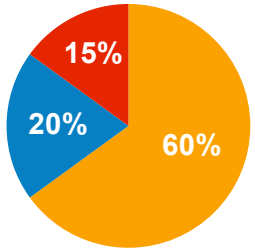
TREND MICRO 趨勢科技

行動應用程式安全

- ❖平臺使用不妥當(Improper Platform Usage)
- ❖不安全的數據存取(Insecure Data Storage)
- ❖不安全的通訊(Insecure Communication)
- ❖不安全的身分驗證(Insecure Authentication)
- ❖不足夠的加密法(Insufficient Cryptography)
- ❖不安全的授權(Insecure Authorization)
- ❖較差的程式碼品質(Poor Code Quality)
- ❖程式碼竄改(Code Tampering)
- ❖逆向工程(Reverse Engineering)
- ❖額外功能(Extraneous Functionality)

勒索軟體

勒索軟體



勒索軟體是一種惡意軟體，以加密設備上的文件來威脅受害者，要求受害者支付贖金(通常是加密貨幣)才能解密文件，還會嘗試傳播感染網路上其他設備，無差別或是針對具有高價值的目標攻擊。

20%
資料可用性

是最主要的威脅傷害型態，加密受害電腦中的檔案，要求受害者支付贖金換取解密金鑰，然而即使受害者願意支付贖金，也未必能確保資料完整的恢復

60%
系統可用性

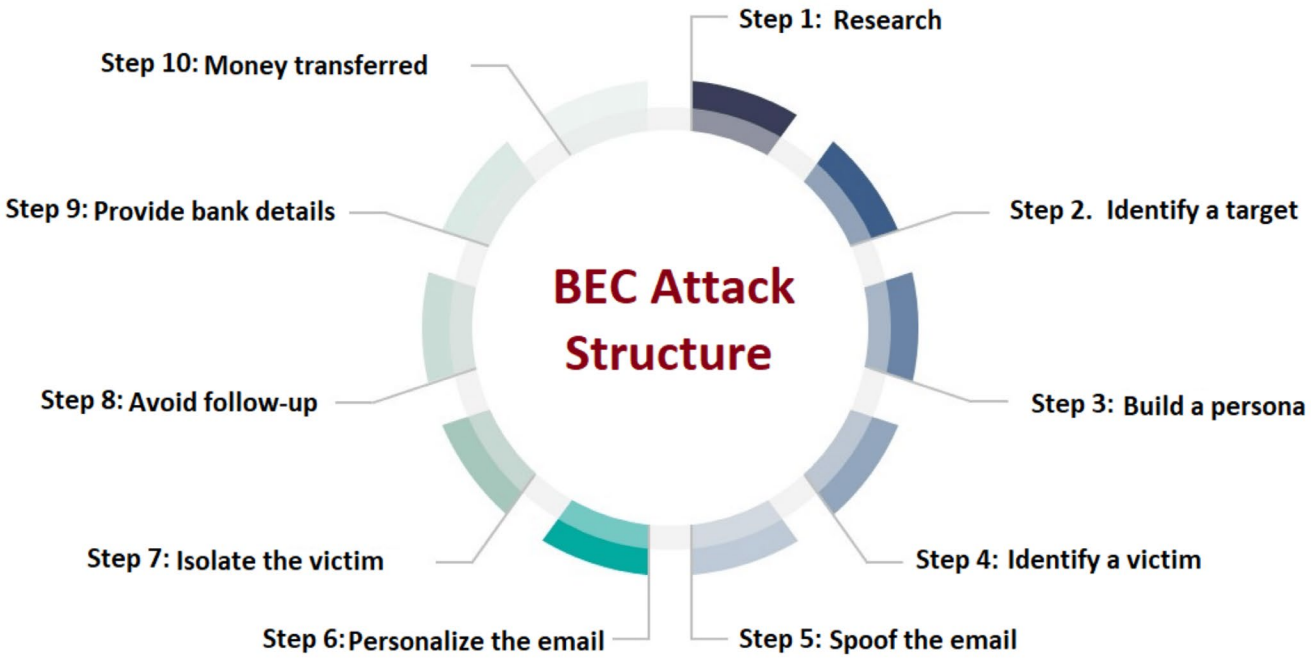
特徵是阻止受害者存取受感染的電腦或行動裝置，鎖住電腦螢幕與瀏覽器導致無法使用，藉以達到威脅的目標

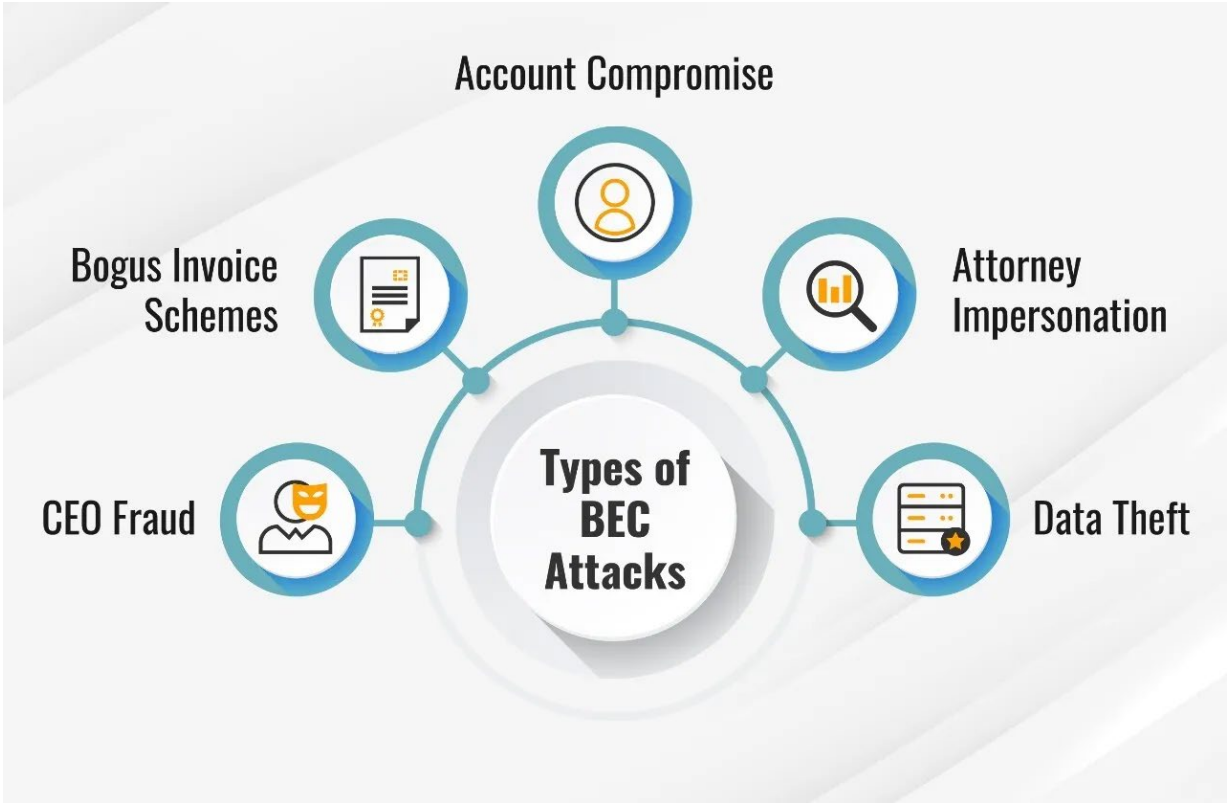
15%
隱私挾持
(Doxware)

主要是對資料的機密性造成傷害，駭客將受害者電腦中的資料大量加密和上傳，以洩漏該隱私或機敏資料作為要脅，迫使受害者支付贖金換取資料不外洩

商務電子郵件詐騙

商務電子郵件詐騙(Business Email Compromise, BEC)





BEC資安強化措施

建議如果收到聲稱是合作企業或高階主管的電子郵件，務必利用其他管道查明對方身分，或是向其所屬企業確認身分.

建議不論個人或企業都應定期將系統進行更新，安裝防毒軟體與防火牆，確保設備軟體處於最新版本，以免被駭客利用資安漏洞進行攻擊

收到電子郵件務必確認電子郵件地址的正確性，駭客可能將郵件地址的英文字母小寫改成大寫或相似字等方式，偽冒成主管或合作夥伴

建議企業落實對員工的資安宣導，定期舉辦資安教育訓練及社交工程演練。疫情期間許多企業讓員工遠距在家上班，員工家中設備網路安全防護不足，也是企業應宣導及協助的部分

不開啟不明寄件者或可疑標題的郵件，勿點擊郵件中的連結及附檔，進入可疑網站不隨意輸入帳密和個資，即使看起來像官方網站，也要確認網址的正確性，以免被駭客利用釣魚網站竊取帳戶資訊或被暗植木馬程式.

LINE

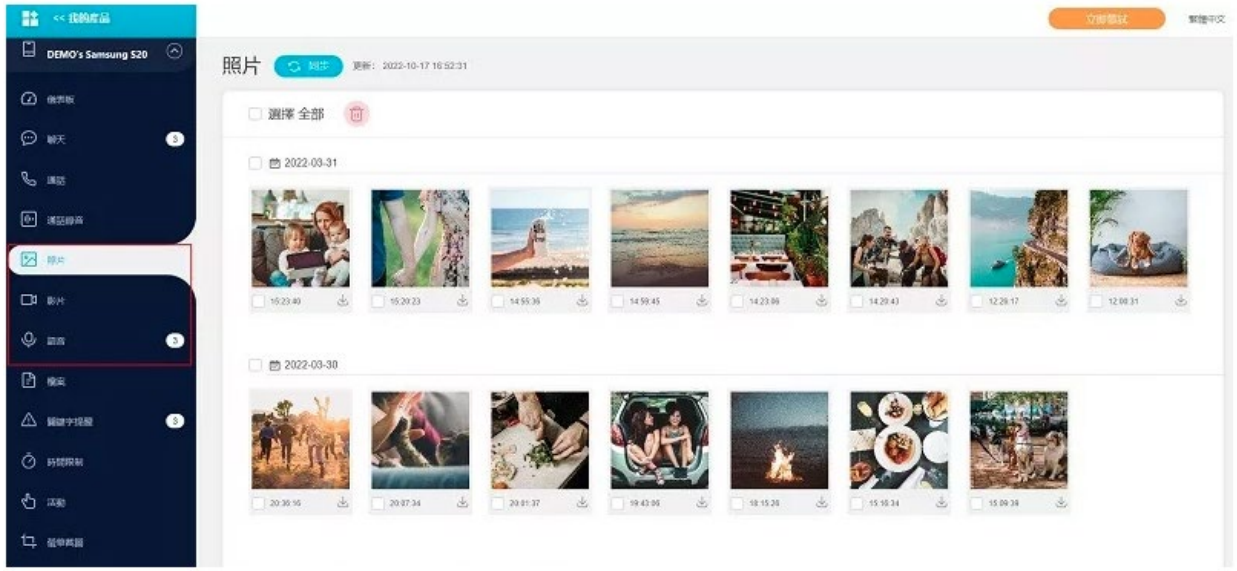
LINE的安全性

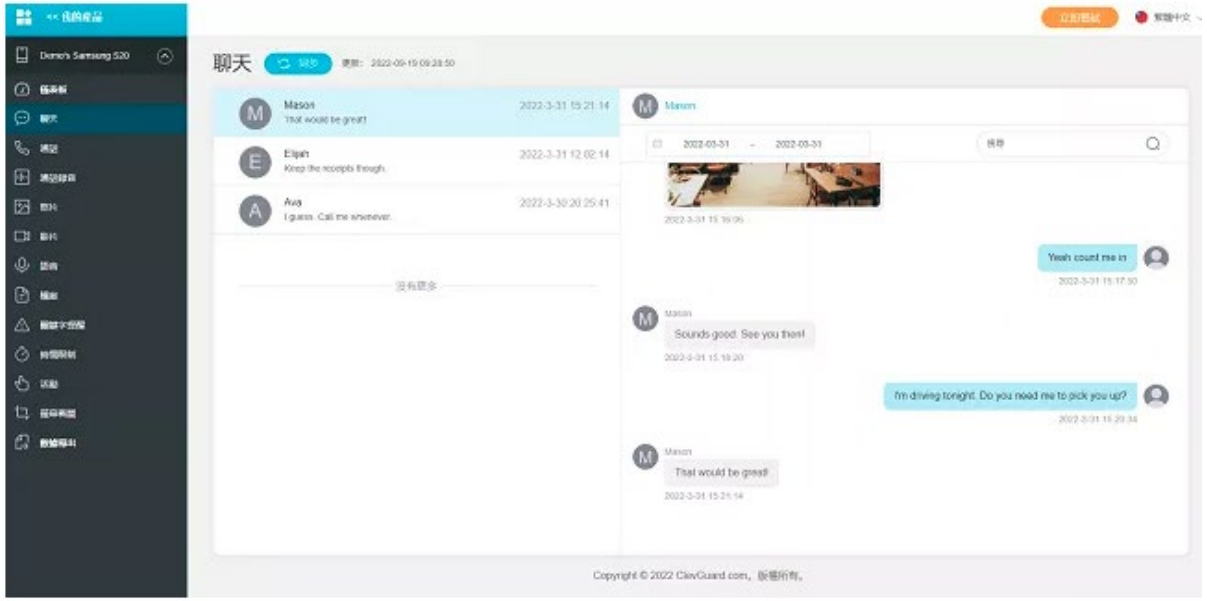
LINE 驚傳遭到駭客入侵，府院高層等 100 多人帳號被鎖定

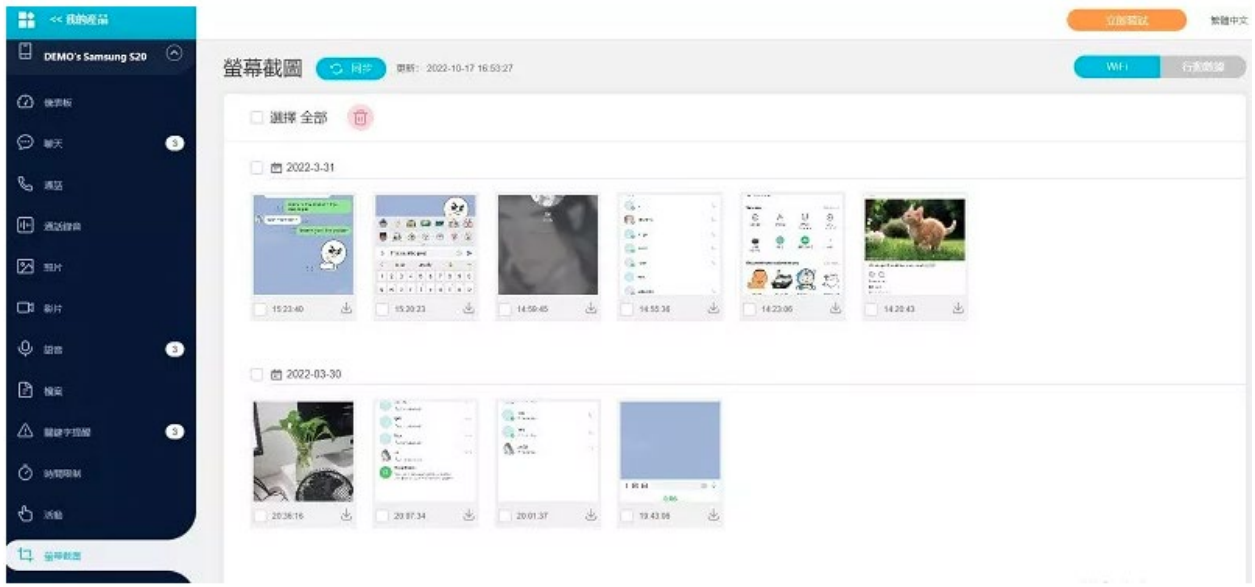
作者 陳 冠榮 | 發布日期 2021 年 07 月 28 日 11:15 | 分類 app , 社群 , 資訊安全 分享 分享 Follow 讚 520 分享

我國府院高層人士驚傳遭駭客鎖定，藉由 LINE 入侵、擷取內容再外流，LINE 系統偵測到異常後，立即採取必要措施保護用戶，並由台灣總公司向執法單位報案。由於被鎖定的對象牽涉府院高層人士，恐有國家安全疑慮，國安單位展開專案調查。

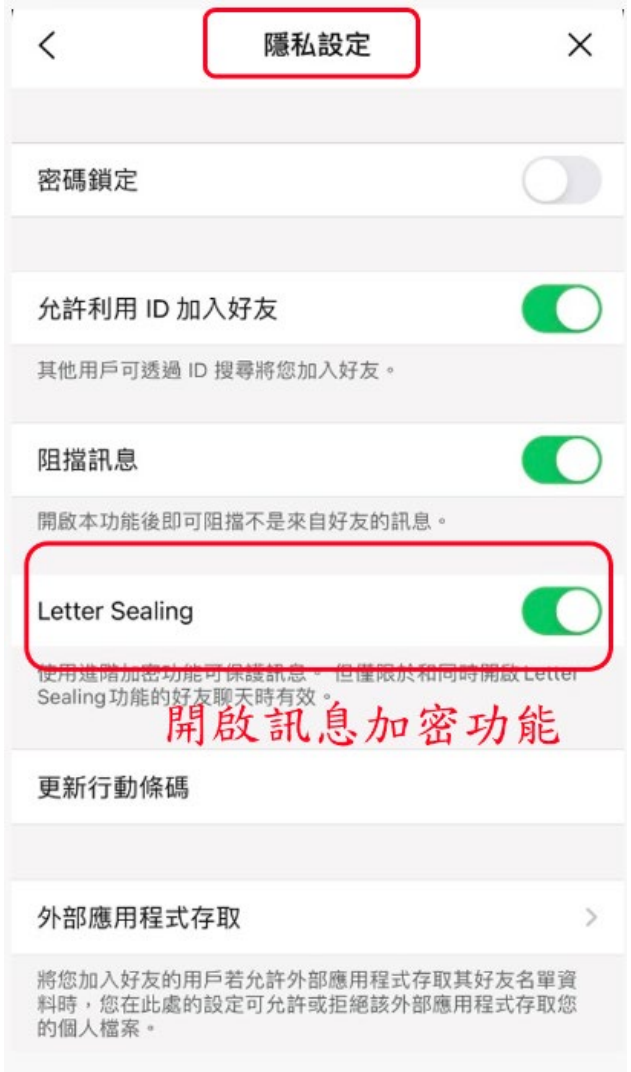
KidsGuard for LINE







LINE帳號的安全性設定



https://help.line.me/line/ios/categoryId/20007829/3/pc?lang=zh-Hant

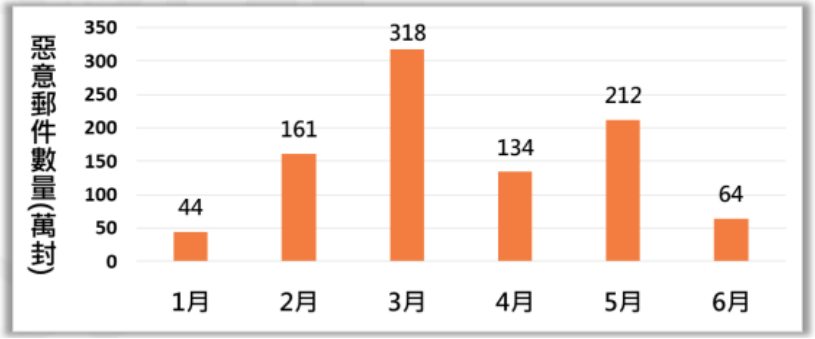
LINE帳號的安全性設定

https://help.line.me/line/ios/categoryId/20007829/3/pc?lang=zh-Hant

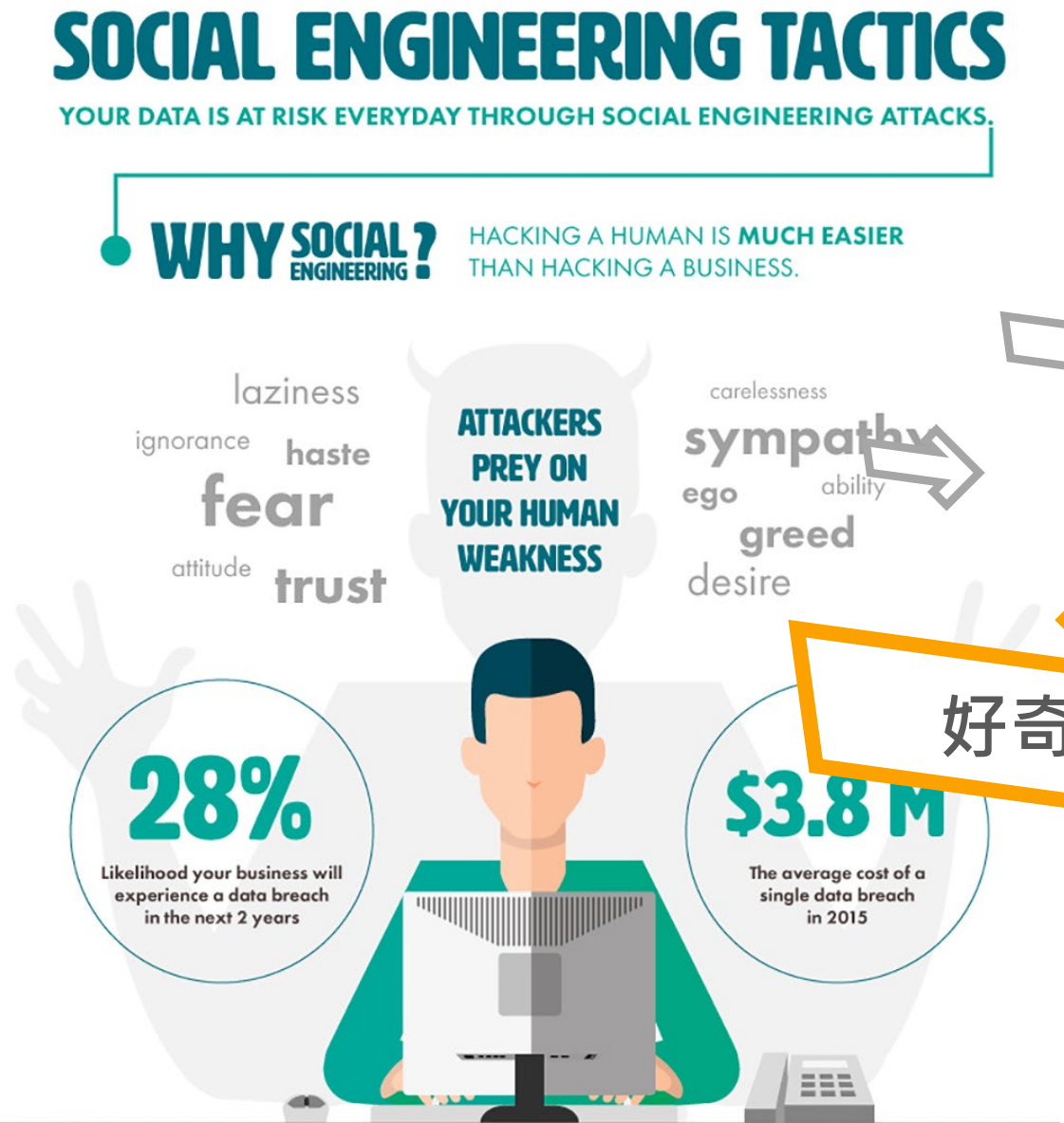
社交工程

社交工程

- 111年上半年政府領域社交工程釣魚郵件攻擊
  - 2月、3月及5月偵測到大量詐欺釣魚郵件散布，皆以取得收件人電腦機敏資訊或掌握使用者不堪影片為由，向受駭者勒索比特幣
- 111年上半年政府領域惡意程式垃圾郵件攻擊
  - 自2月底起至今，發現Emotet惡意垃圾郵件開始大量散布，並使用社交工程手法以增加成功率



人的弱點-群體



貪小便宜

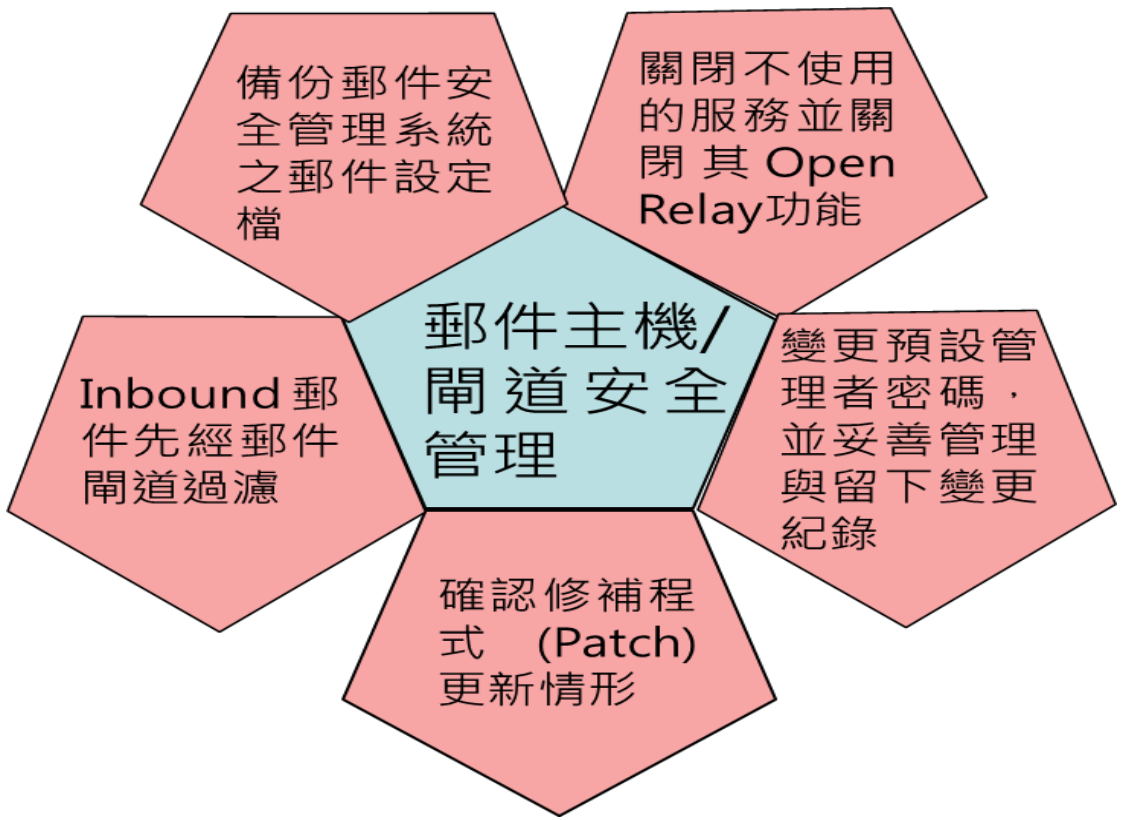
盲從

自以為是

好奇心

畏懼

社交工程防範



個人端郵件安全管理	
	勿隨意開啟不明來源或奇怪主旨內容之郵件
	隨時更新病毒程式碼
	時常確認是否有修補檔 (Patch) 可更新
	不使用公務帳號加入網路社群或購物服務會員
	避免使用公共場所的電腦來收發電子郵件
	取消帳號密碼自動記憶功能
	提高個人郵件操作軟體之安全設定(如關閉預覽窗格、純文字模式讀取信件、關閉圖片自動下載等)
	除非清楚此附件的來源及寄送原因，否則不要隨意開啟附件檔案
	若要傳送機密性郵件，須以郵件加密方式進行傳送

結論

04

資訊安全是一種管理

永無止盡 矛與盾之爭，藉由管理機制完善

管理

風險評鑑

風險評估(Risk Evaluation)-將估計的風險與所訂的風險準則加以比較，以. 決定風險重要性的過程。 • 風險處理(Risk Treatment)-選擇與實施各項控制措施，以修正風險的過程

威脅來源(Threat Agent)-引發潛在威脅的源頭。 暴露(Exposure)-弱點誘發威脅的情況。 弱點(Vulnerability)-指單一或一系列會讓威脅有機可趁而 造成資產損害的狀況。 資產的脆弱點本身並不會造成傷害。

威脅與弱點

駭客