paloalto NETWORKS | Cybersecurity Partner of Choice

XaaS 網路犯罪即服務

Palo Alto Networks 台灣資安顧問

Matt Liu 劉宇庭

XaaS 是什麼？

SaaS

讓使用者可透過網際網路連接到雲端應用程式並加以使用

PaaS

幫助企業創建和部署應用程序，而無需建置和維護數位基礎架構

IaaS

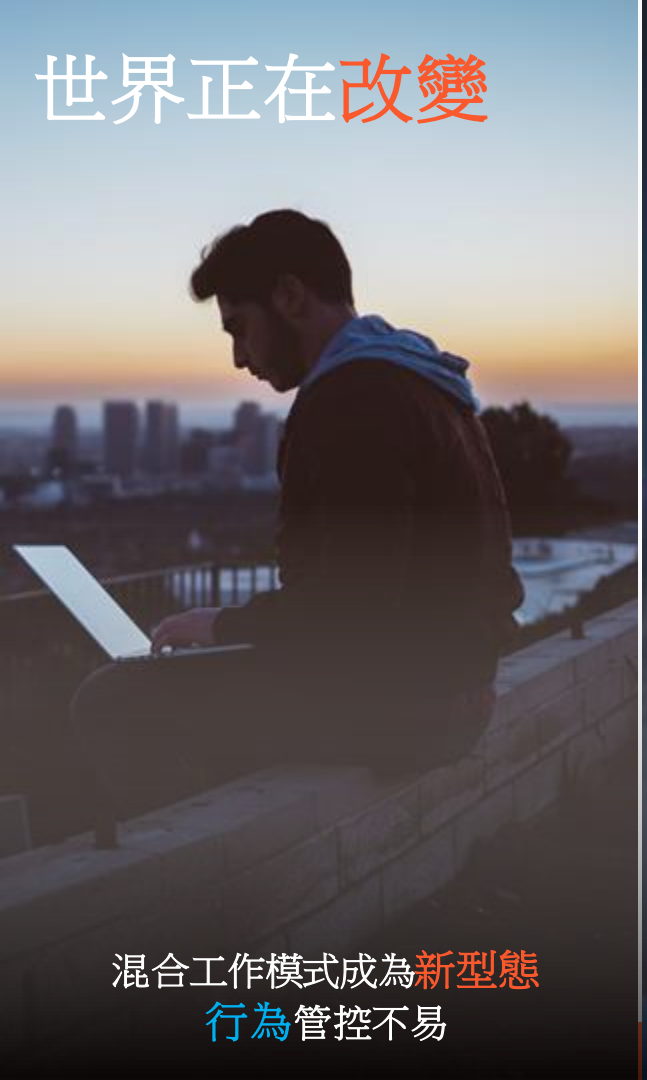
以隨用隨付的方式，依需求提供基本的計算、儲存體及網路等資源

世界需要的新方法

現在正參與其中

Image is from DATA UNIT AG. (https://www.dataunit.ch/digitale-transformation-vorteile-und-herausforderungen/)

世界正在改變



混合工作模式成為新型態
行為管控不易

SaaS 應用程式爆炸性的成長
資料外洩與駭客的攻擊

機器智能加速物聯網的發展
裝置識別問題

XAAS 正在吞噬世界

使用量爆炸性的成長...

100+ SaaS apps

企業購買佔其軟體的

70% 以上

...建立新的目標...

78%

的組織將敏感資料儲存在 XaaS 應用程式中

...引發更多攻擊

470%

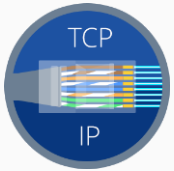
用於實施攻擊的 XaaS 同比增長

這種轉變帶來了獨特的安全挑戰

威脅途徑有哪些？

環境 / 管理機制

嵌入式環境



TCP/IP網路

智慧監控管理/供應鏈

威脅途徑

軟體/系統漏洞

網路存取

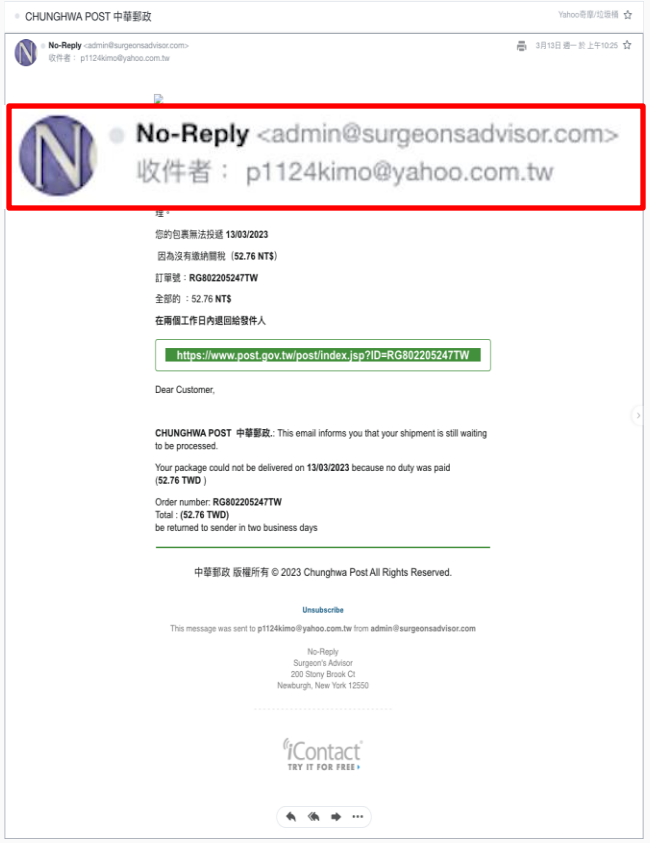
攜帶式媒體

社交工程

案例分享 - 郵件行銷平台


支付資格暫時被封鎖
APPLE PAY <infoadmin@noorgoldcosmetics.com> 取消訂閱
收件者： p1124kimo@yahoo.com.tw
Pay
你好，
我們注意到您在裝置上使用的卡片與多個裝置關聯。
作為安全措施，我們已阻止存取您的帳戶，直到我們確認您是您所使用的卡片的真正所有者為止。
確認>>
請在 12 小時內完成驗證，否則您的付款資格將被永久禁用
noorgoldcosmetics | 1871 Putnam Ave, Ridgewood, NY 11385
Unsubscribe p1124kimo@yahoo.com.tw
Update Profile | Constant Contact Data Notice
Sent by infoadmin@noorgoldcosmetics.com powered by
Constant Contact
Try email marketing for free today!


重要：您的钱包将被暂停
Line 支付 <jgarcia@declarafacil.com.mx> 取消訂閱
收件者： p1124kimo@yahoo.com.tw
declarafacil.com.mx | 6204 S Cooper St #132, Arlington, TX 76001
Unsubscribe p1124kimo@yahoo.com.tw
Update Profile | Constant Contact Data Notice
Sent by jgarcia@declarafacil.com.mx powered by
Constant Contact
Try email marketing for free today!


CHUNGHWA POST 中華郵政
No-Reply <admin@surgeonsadvisor.com>
收件者： p1124kimo@yahoo.com.tw
您的包裹無法投遞 13/03/2023
因為沒有繳納關稅（52.76 NT$）
訂單號：RG802205247TW
全部的：52.76 NT$
在兩個工作日內退回給發件人
https://www.post.gov.tw/post/index.jsp?ID=RG802205247TW
Dear Customer,
CHUNGHWA POST 中華郵政.: This email informs you that your shipment is still waiting to be processed.
Your package could not be delivered on 13/03/2023 because no duty was paid (52.76 TWD)
Order number: RG802205247TW
Total : (52.76 TWD)
be returned to sender in two business days
中華郵政 版權所有 © 2023 Chunghwa Post All Rights Reserved.
Unsubscribe
This message was sent to p1124kimo@yahoo.com.tw from admin@surgeonsadvisor.com
No-Reply
Surgeon's Advisor
200 Stony Brook Ct
Newburgh, New York 12550
iContact
TRY IT FOR FREE

駭客工具唾手可得 - 任何人都可能是下個目標！！！

Attack Anywhere

Develop Anywhere

Target Anywhere

Unit 42 - 當前的威脅情勢...

勒索行為呈上升趨勢

每四小時一個目標

Unit42 的威脅研究人員計算出，在暗網上，**每四小時**就會有一個公開發布的新勒索目標。

2679 名受害者

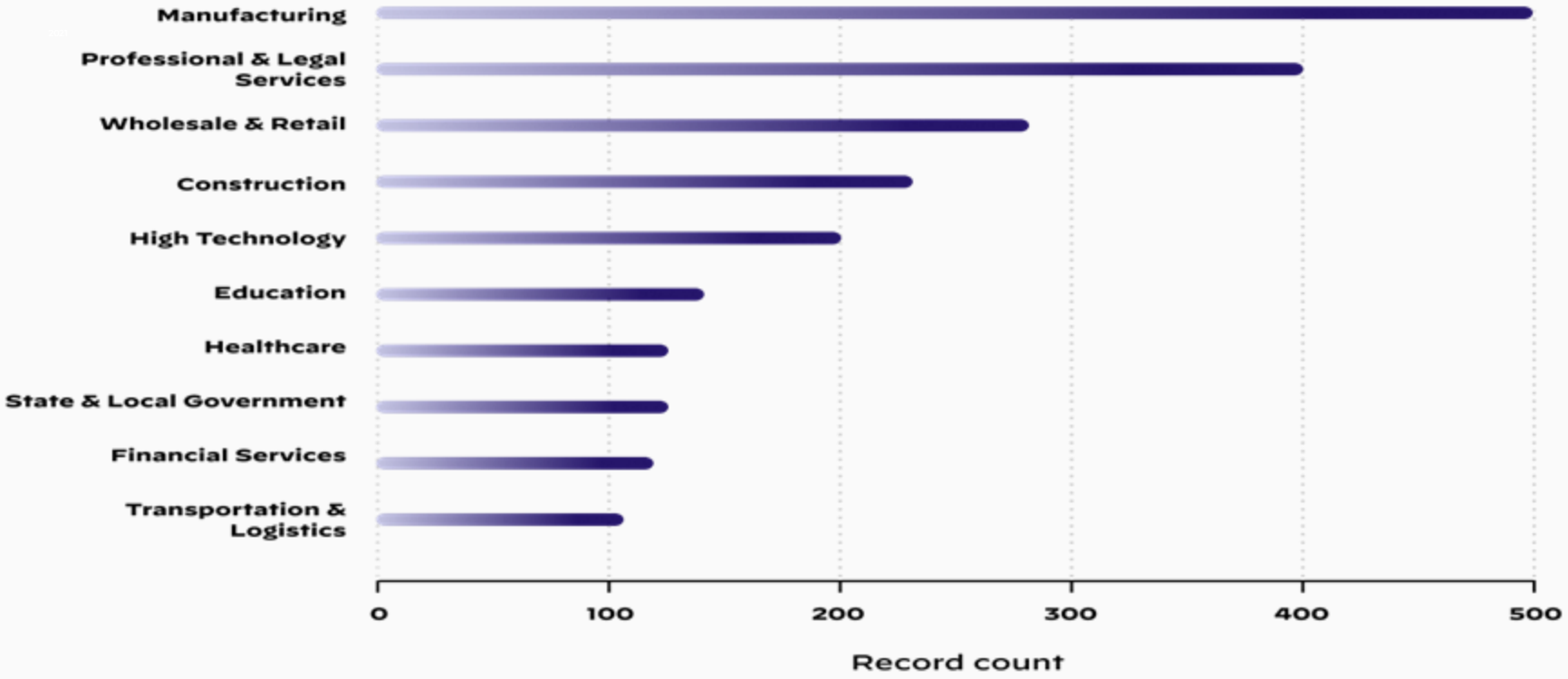
2022 年，洩密網站上發布了 **2,679** 名受害者的姓名和妥協證據，比 **2021 年**觀察到的數字高出約 **4%**。

107 個國家

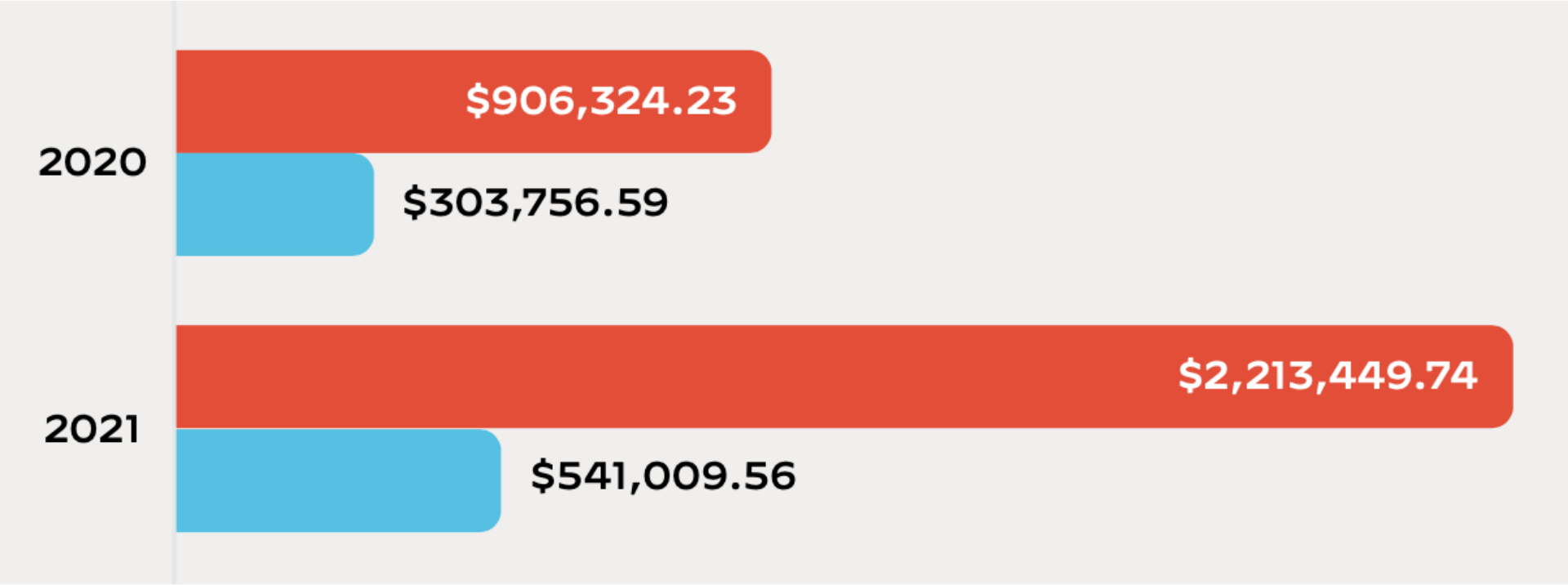
犯罪集團遍布全球，據觀察，到 2022 年，犯罪集團將影響 **107 個國家的組織**。

Unit 42 - 最常遭受到攻擊的行業

受勒索攻擊影響最嚴重的產業（Leak site data，2022 年）



Unit 42 - 勒索軟體資安事件贖金統計



近乎完美的犯罪行為

暗網”Leak Site”公布的機敏資料

85%↑

2020 對比 2021加密勒索犯罪事件

144 %↑

Ransomware

Unit 42 - 產業的習性

Unit 42 事件回應團隊發現的勒索軟體攻擊和違規行為中有 **75%** 是由於攻擊面暴露造成的

大多數威脅都會尋找有**漏洞**且有能力獲得**巨額賠償**的行業。 這些漏洞通常包括以下行業：

軟體已過時

利用運行在未修補或更新的舊軟體上的系統。

業務運營取決於產品時間表

駭客團體利用這些企業面臨的壓力來按時完成任務並交付贖金。

攻擊面暴露

Unit 42 事件回應團隊在勒索軟體攻擊和違規行為中，發現至少 75% 是由共同的團體所造成的。

我們所知道的

不採取行動的代價是...

遭受攻擊

90%

在台灣，去年企業受到攻擊的比例

來源: International Information Security Companies Survey (Taiwan), June 2022

中斷營運

33%

資安專家表示在遭受攻擊後面臨營運中斷

來源: Palo Alto Networks What's Next In Cyber

財務及業務衝擊

$2.4M

從攻擊中回復所需的平均成本

來源: Forrester

資安威脅風險衝擊不亞於重大天災

生產作業停擺

設備系統損壞

企業財務損失

企業商譽受損影響：供應鏈合作，商品可靠度

員工人身安全

營業機密遭竊、商業競爭破壞

限制企業未來科技發展

Photo by Science in HD on Unsplash

Industrial Cyber Security

對 XaaS 產生疑問？

應用程式

員工使用哪些應用程式以及如何使用？

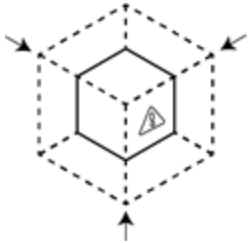
資料

如何保護雲端中的敏感資料？

使用者

管理對 SaaS 應用程式的存取並保護它們免受威脅

如何預防資安事件的發生？

Complete Visibility → Reduce Attack Surface → Prevent Known Threats → Prevent Unknown Threats

Consistent Across all Locations

- Headquarters
- Branch Offices
- Data Center/ Private Cloud
- Public Cloud
- SaaS
- Mobile Users
- IoT

總結 - 小小的建議

1. 即時了解不斷變化的威脅情勢
2. 分析遺失關鍵資料對業務的影響
3. 評估內部及外部準備情況
4. 檢視與測試對事件的回應計畫
5. 實施零信任
6. 識別暴露資產
7. 防止已知與未知威脅
8. 自動化
9. 保護雲端服務
10. 跨界合作減少回應時間

我們所知道的業界最佳的資安平台

透過新世代資安解決方案協助轉型

資安維運 (Operation)

A complete suite of analytics and automation solutions to power a modern SOC, including XDR, SOAR, and attack surface management

網路安全 (Networks)

Best-in-class Network Security Platform across hardware, software and SASE - securing hybrid workforces and complex infrastructures of today

雲端安全 (Cloud)

Comprehensive cloud-native application protection platform from development to runtime, across multi-cloud and hybrid environments

端點安全 (Endpoint)

Best performing endpoint protection in 2022 MITRE ATT&CK, with 100% detection

資安情資及事件回應(IR)

Unit 42 brings together world-renowned threat researchers, incident responders, and security consultants to help you proactively manage cyber risk

企業資安升級充電

掃描活動QRcode立即報名！

paloalto NETWORKS | Cybersecurity Partner of Choice

THANK YOU