SYSTEX A DATA SOFTWARE COMPANY

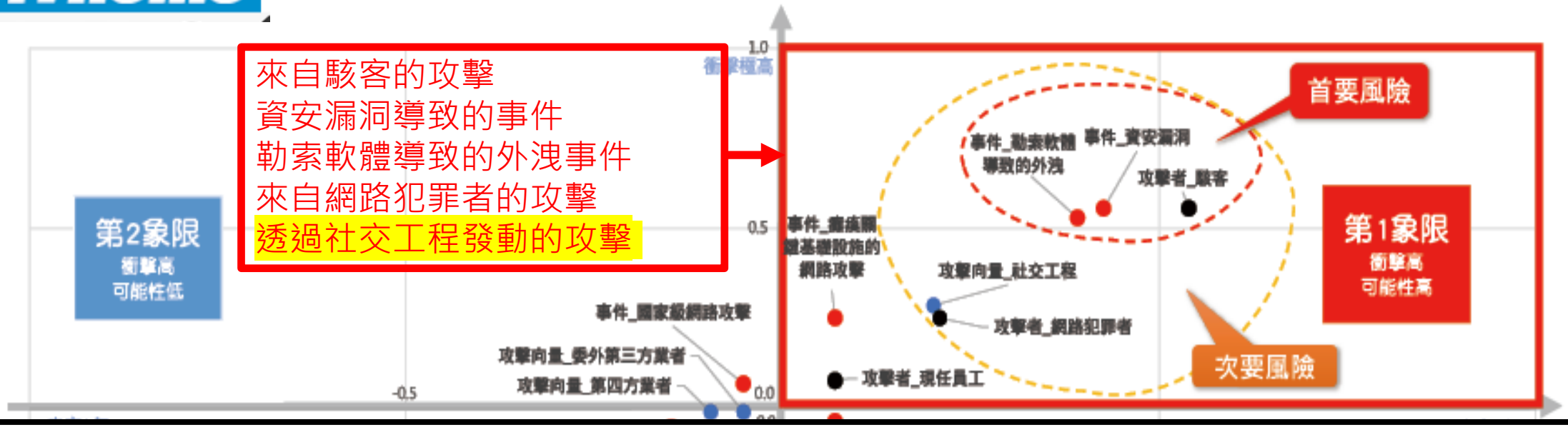
從駭客入侵輪廓
淺談社交工程的重要性

Agenda

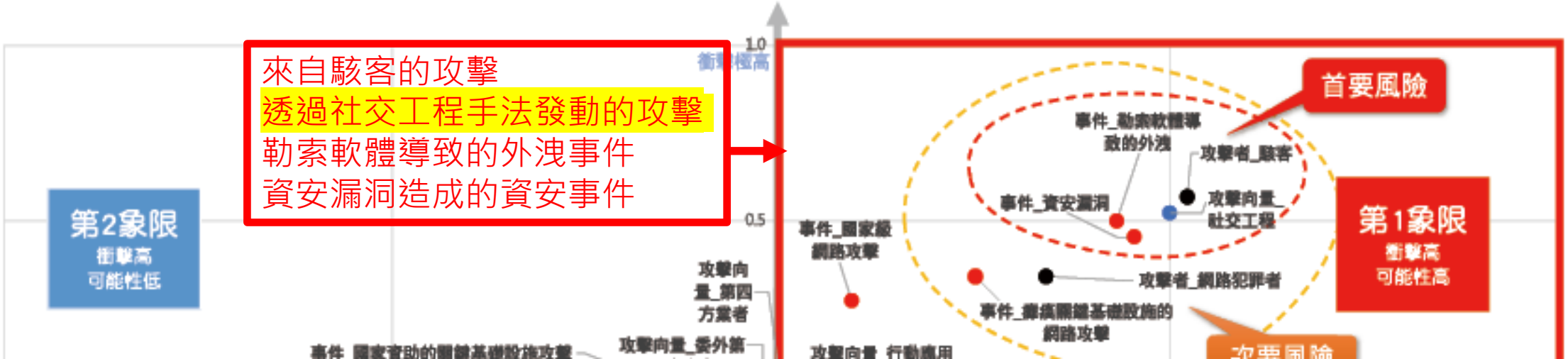
- 社交攻擊的威脅及趨勢
- 如何防範社交攻擊
- 電子郵件威脅及趨勢
- 如何防禦

2021資安衝擊風險圖

【服務業】2021企業資安風險圖（未來1年）

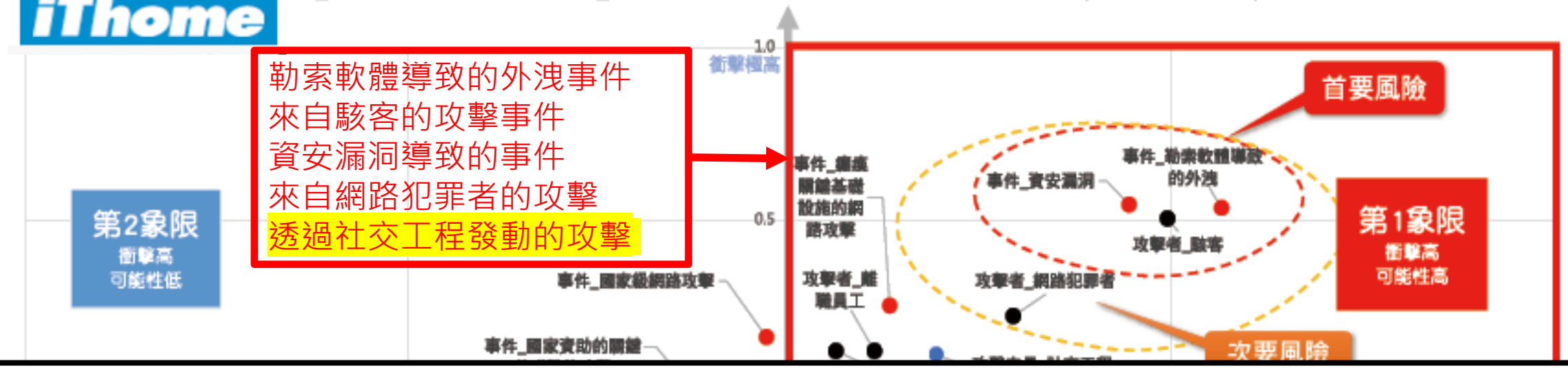


【金融業】2021企業資安風險圖（未來1年）

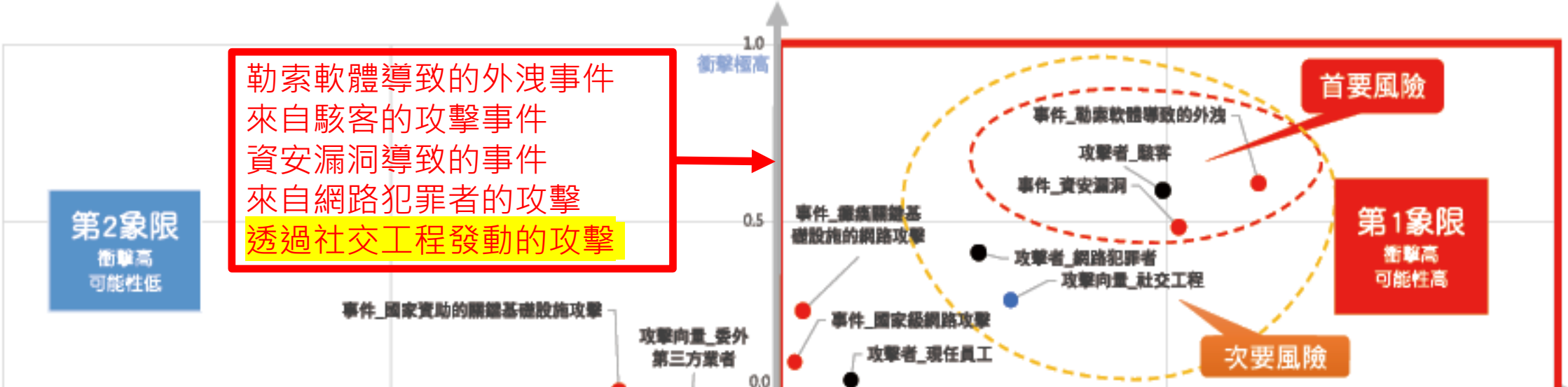


2021資安衝擊風險圖-續

【高科技製造業】2021企業資安風險圖（未來1年）



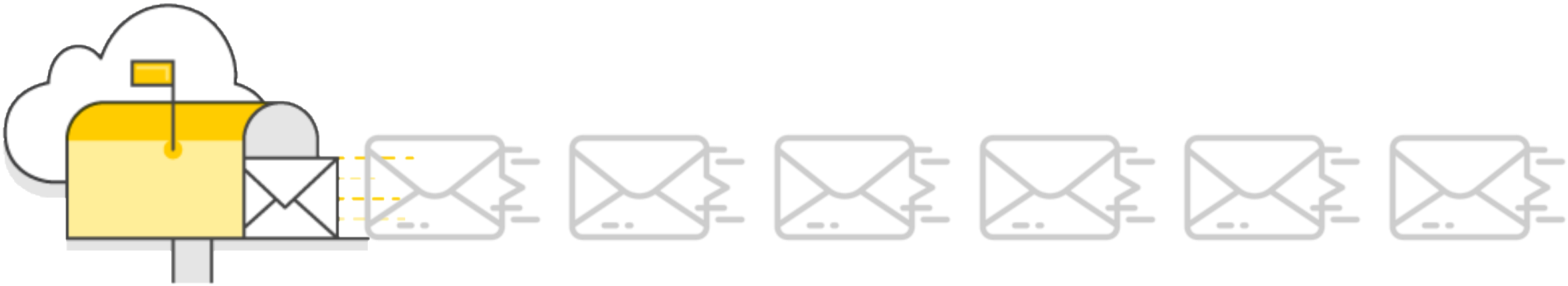
【一般製造業】2021企業資安風險圖（未來1年）



驚人的損失-還不包括沒有揭露的

另一方面，根據美國聯邦調查局（FBI）網路犯罪投訴中心（Internet Crime Complaint Center，IC3）2021年的統計，商業電子郵件詐騙（Business Email Compromise，BEC）是去年網路犯罪投訴數量排行榜上的第九名，遠不如網釣、交易詐騙、個資外洩、身分竊盜或勒索等，但該類型的詐騙卻高居損失排行榜的第一名，去年因BEC而造成的損失為24億美元，占所有網路犯罪金額的35%，也無怪乎駭客費力部署AiTM的最終目的是進行商業電子郵件詐騙。

駭客透過企業資安防禦最薄弱的員工意識下手

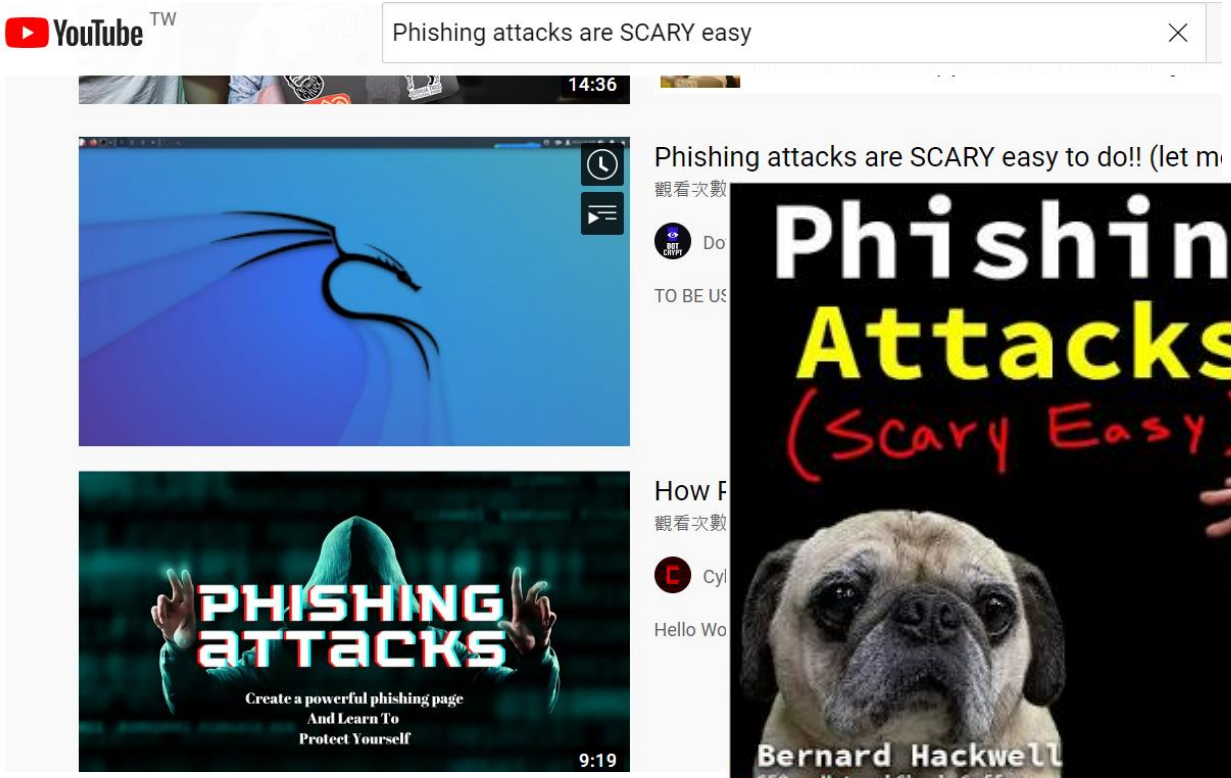


根據國際調查顯示
一般上班族平均每天會接收60封電子郵件
其中有16%郵件是垃圾或釣魚郵件

平均員工每年需處理
約2300封有風險的郵件

社交攻擊技術門檻不斷降低

- 搜尋 “Social Engineering Toolkit” 您可找到[工具箱]、[教學影片]、
- 社交攻擊常用工具Phishing Frenzy, LUCY



差異化在「行銷創意」，更多利用的是「人心」

- 網路釣魚(Phishing)- 透過吸引人的電子郵件標題與網站內容誘使點擊

資料來源：資安人

人依然是最大漏洞

對Twilio的攻擊中，駭客進行簡訊網路釣魚詐騙，冒充Twilio的IT部門並警告員工他們的密碼已過期需要更改。受騙員工被帶到看似Twilio登錄頁面的釣魚網站，駭客在該頁面中獲取了Twilio員工的身分驗證資訊，後來他們使用這些憑證存取公司的內部系統並查看了客戶的資料。

而思科的資料洩露事件中，「閻羅王」組織聲稱竊取了思科2.8G資料。在這次攻擊中，攻擊者首先控制了一名員工的個人google帳戶，用戶將該帳戶的身分憑證同步到瀏覽器。隨後，攻擊者冒充各種該員工信任的組織單位進行了一系列語音網路釣魚攻擊和大量發送MFA（多因子身分驗證）通知直至該員工確認了其中一次驗證請求，從而使攻擊者能夠存取VPN和關鍵內部系統。

Twilo和思科的資料洩露事件都表明，企業不能僅僅依靠員工來識別日益複雜的社交工程騙局，即使是這些員工本身也是IT技術人員。

專家表示，這兩次攻擊說明社交工程仍然是獲取組織存取權限的最有效方法之一，且任何組織都可能成為攻擊目標。人類永遠都是攻擊的目標。如果使用者收到一封來自看似可信來源的電子郵件或短信，其中又包含緊急資訊，使用者很可能會不經安全確認就點選連結。

典型BEC變臉詐騙

[redacted] (週二) 上午 11:00
[redacted] Accounting <act@[redacted]line.co.kr>
[redacted]CER / APR SOA

正常的往來Email

收件者 [redacted];
副本 [redacted]smile@[redacted]line.co.kr

20190430_SOA_[redacted]CER.pdf
137 KB

Dear All,

Good day,

Please see attached file for APR SOA.

Please kindly check and give your request if any. Thanks.

Thanks & Brgds

[redacted] (週二) 下午 08:19
[redacted] Accounting <act@[redacted]line-co.kr>
RE: [redacted]CER / APR SOA

駭客利用時間差發送詐騙Email

收件者 [redacted]
副本 [redacted]smile@[redacted]line.co.kr

Dear All,

Hope you received the APR SOA I sent in my previous email.

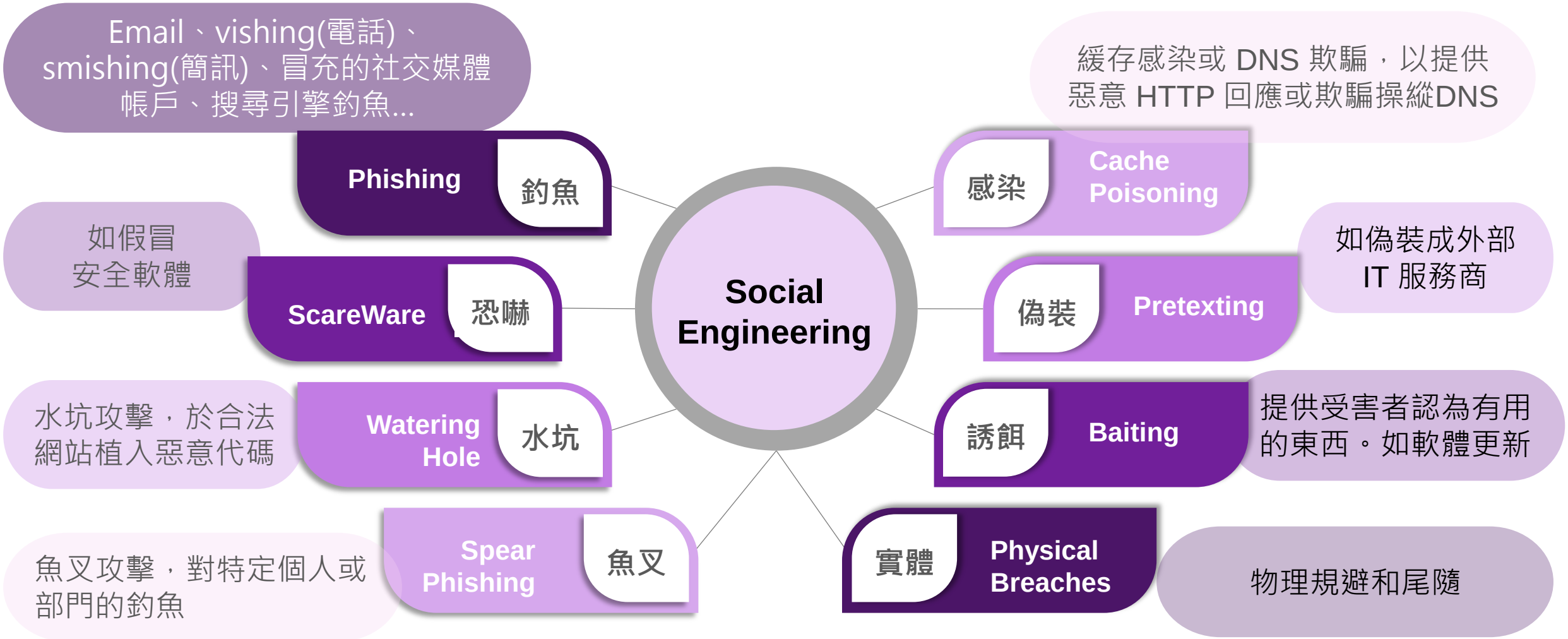
Kindly note that the bank account on the SOA is currently on hold and cannot receive money at the moment, please let us know when you are ready to make payment so we can provide the new details for payment.

Please kindly check and give your request if any. Thanks.

Thanks & Brgds

前封對帳單上的匯款帳戶目前暫停使用，暫時無法收款，請在準備付款時告知，以便提供新的付款資訊

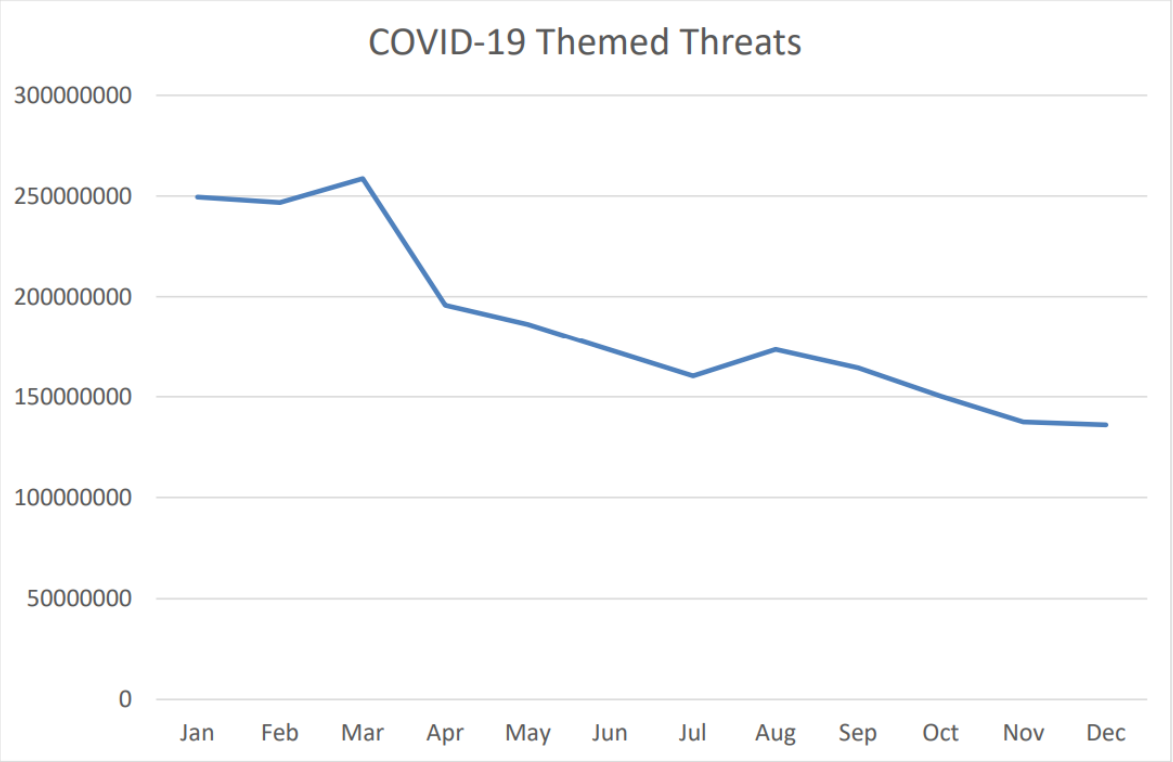
8 大社交工程技術


Email、vishing(電話)、smishing(簡訊)、冒充的社交媒體帳戶、搜尋引擎釣魚...
Phishing
釣魚
如假冒安全軟體
ScareWare
恐嚇
水坑攻擊，於合法網站植入惡意代碼
Watering Hole
水坑
魚叉攻擊，對特定個人或部門的釣魚
Spear Phishing
魚叉
Social Engineering
緩存感染或 DNS 欺騙，以提供惡意 HTTP 回應或欺騙操縱DNS
感染
Cache Poisoning
如偽裝成外部 IT 服務商
偽裝
Pretexting
提供受害者認為有用的東西。如軟體更新
誘餌
Baiting
實體
Physical Breaches
物理規避和尾隨

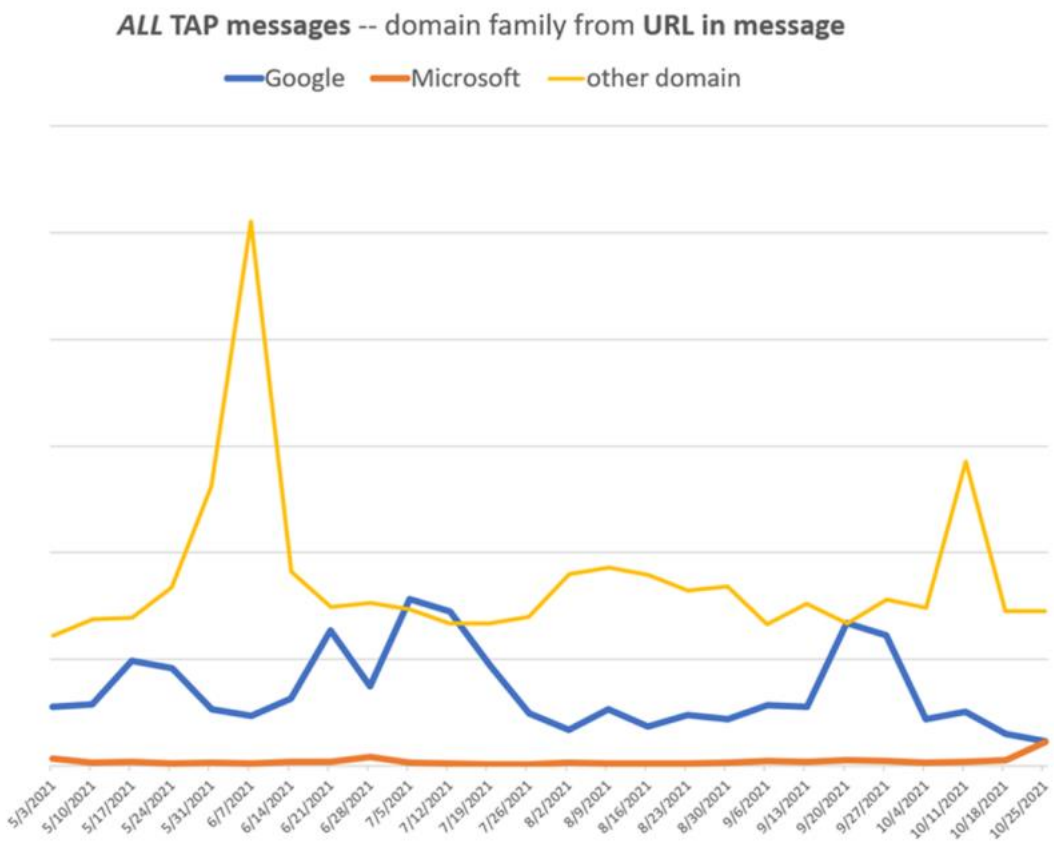
資料來源：ProofPoint

社交攻擊新趨勢

新冠疫情的主題已經看膩了



目標式、容易被信任的來源(如知名雲服務)、夾雜惡意網址的攻擊，逐漸成為顯學



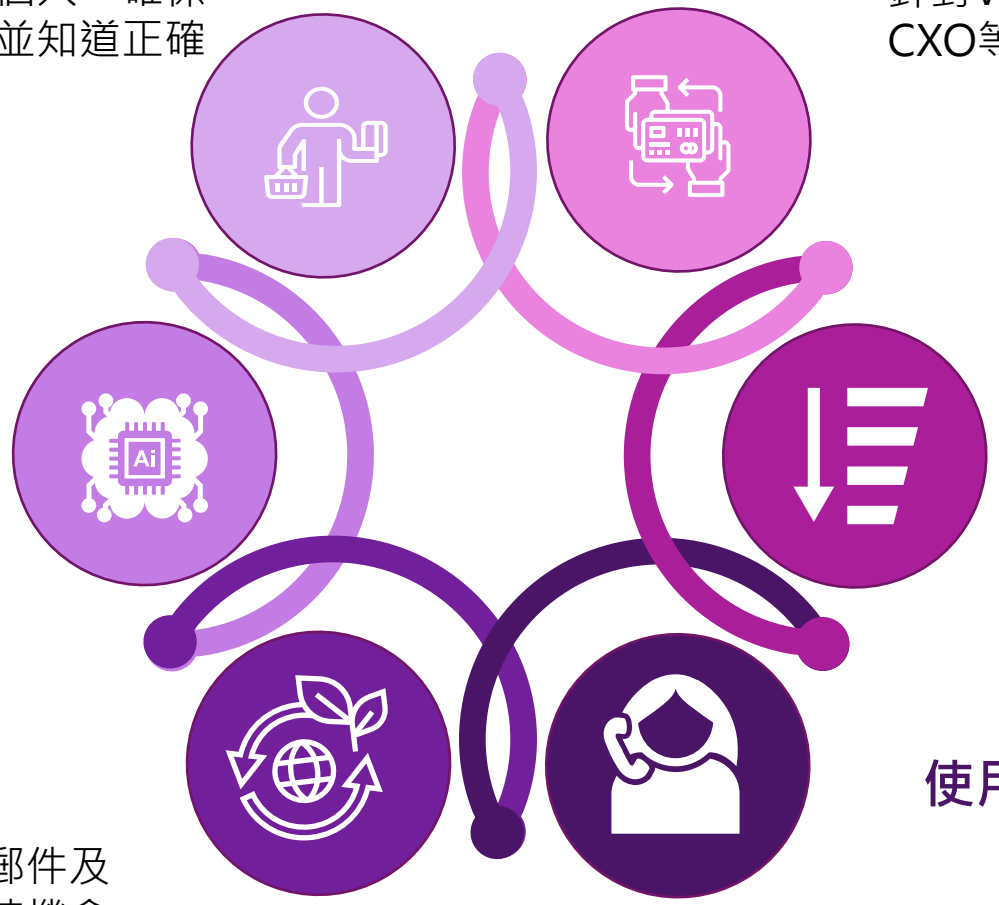
阻止社交攻擊的六種方法(郵件是攻擊發起線)

教育員工，人是最好的也是最後一道防線

惡意電子郵件的目標始終是接收它的個人。確保員工能夠識別惡意或網路釣魚郵件，並知道正確的後續程序是什麼。

個性化自適應控制

針對VIP及高風險的個人，例如負責付款的人、CXO等能夠調整出更細的可見度及防禦規則。



應用AI/機器學習

人類總會犯錯，釣魚郵件越來越先進，一些郵件就從指縫中溜走，透過AI/ML發揮的算法及建模，能以超出人類能力的準確度識別異常郵件

建立新世代的郵件安全防護

傳統SPAM、防毒明顯不足，AI、多層次偵測、自動識別/刪除有害的 URL。有了這些功能，員工犯錯的機會就會減少

封閉式郵件分析

進行沙箱分析，提供自動化篩選郵件及回饋機制，讓偵測變得更準確同時機會造福其他員工

使用其他管道再做確認

如付款前以電話聯絡，或主動另以郵件確認

電子郵件威脅

電子郵件安全趨勢

資料來源：Minecast、Abnormal

3/4

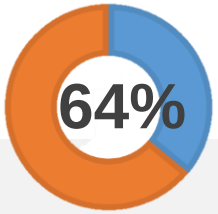
組織收到了越來越多的電子郵件攻擊

~80%

八成受訪者的電子郵件使用率上升

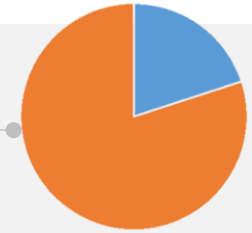
75%

的公司受到勒索軟件攻擊的傷害



面臨勒索攻擊時，**64%** 的公司付了贖金

但其中**近四成**未能恢復資料



超過**八成**的公司由於粗心或疏忽的員工無意中洩露資料而面臨風險

從一名受感染的員工傳播到其他人的網路攻擊呈上升趨勢

96%

的公司已成為與電子郵件相關的網路釣魚嘗試目標。

52%

的受訪者表示，網路攻擊正變得越來越複雜

只有 **23%** 的公司持續為其員工提供網路安全意識培訓，但 **87%** 的公司至少每季度提供一次。

80%

的公司正在為電子郵件攻擊的後果做好準備

93%

的組織已經採用了雲端郵件方案(或計劃中)

79%

在 Microsoft 365 安全電子郵件用戶中，**79%** 的用戶在過去一年中遇過服務中斷

惡意程式附件攻擊

過去2年有近4成被勒索攻擊的企業選擇付錢解決，美國平均支付贖金居各國之冠達600萬美元

根據電子郵件安全業者Mimecast調查，在過去2年內遭到勒索軟體攻擊的企業中，有39%選擇支付贖金以救回資料，其中以美國和加拿大當地企業付款金額最高，平均達500~600萬美元

文/ 林妍溱 | 2021-11-10 發表

全民健康保險扣費明細申報結果通知(u2110
中央健康保險署 (@nhi.gov.tw) 新增連絡人
收件者:

DPR60
28596
5110...

*** 本EMAIL係以系統自動傳送，請

衛生福利部中央健康保險署中區業務組
40709
臺中市西屯區市政北一路６６號
收件人：
(統編：6

扣費

申報單位名稱			
申報單位統編	6	健保署入檔編號	00
處理日期	23/08/2021	申報方式	E-EMAIL檔
申報檔名	DPR60285965110012500 1V1100125154830E		

TNT進口通知--- 提單號碼 09 (發船舶) 04 --- 請確認報單是否正確
@fedex.com) 新增連絡人
收件者:

29608
2809.z
ip

TO : 進口人員 --- 是否轉報？ OR 完稅進口？

. 請確認 INVOICE是否正確，是貴公司的貨嗎?

. 報單無誤 或 需更正，請多利用E-MAIL回覆 並回傳個案委任

. 預估稅費合計 (報單右下角) NTS 貨到收稅
(有先放後稅案號者無需貨到收款;實際金額依 EDI日期匯率

任何貨件派送要求 及 貨件查詢 都請洽: 0

商聯邦快遞國際股份有限公司台灣分公司
胡s --
FEDEX--TNT Import Clerk
Operations Department
桃園
Tel :
Fax :

296082809.zip
檔案(F) 指令(C) 工具(S) 我的最愛(O) 選項(N) 說明(H)
加入 解壓縮到 測試 檢視 刪除 尋找 精靈 資訊 防毒
296082809.zip\296082809 - ZIP 壓縮檔, 未封裝大小 352,939 位元組
名稱
..
296082809.exe
總共 1 個檔案, 352,939 個位元組

惡意程式附件攻擊

2021 年 09 月 08 日

近日網路出現
偽冒衛福部名義的釣魚郵件

勿開啟
以免電腦中毒

最近有偽冒衛福部名義發送的電子郵件（顯示寄件者名稱為 mohw.gov.tw），經過查證，實際寄送郵件的伺服器是國外主機（網域為 static.servebyte.com），研判應該是釣魚郵件，可能夾帶惡意網址連結或木馬程式，請勿開啟。

近日網路出現偽冒本部名義之釣魚郵件，請民眾勿開啟以免電腦中毒。

- 資料來源：資訊處
- 建檔日期：110-09-07
- 更新時間：110-09-07

近日本部發現偽冒本部名義發送之電子郵件(顯示寄件者名稱為mohw.gov.tw)，查實際寄送郵件之伺服器為國外主機(網域為static.servebyte.com)，研判應為釣魚郵件，可能夾帶惡意網址連結或木馬程式，請民眾若收到類似電子郵件，勿開啟以降低電腦中毒及駭客入侵竊取個資之資安風險。

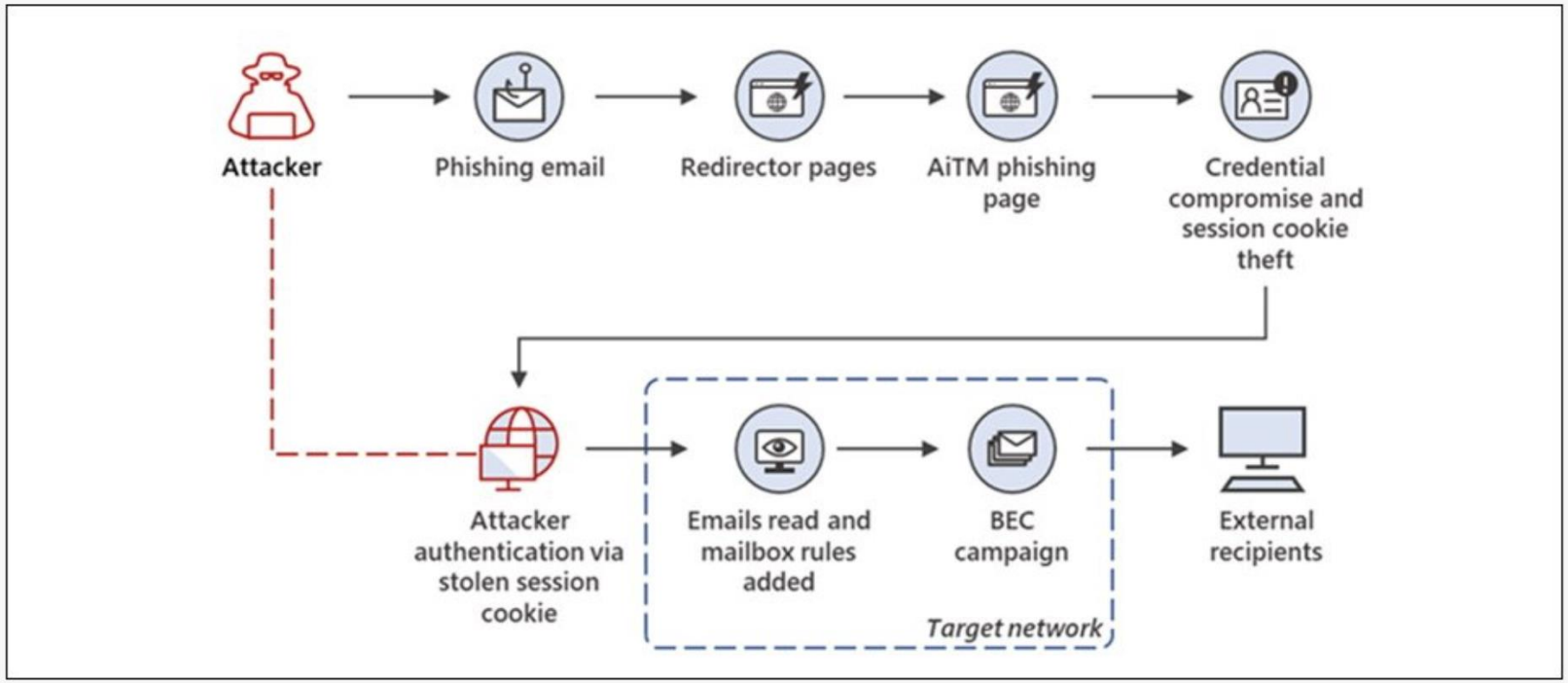
標的愈明顯被攻擊機率愈高

使用微軟郵件服務的企業正遭到大規模網釣攻擊

資安業者Zscaler在今年6月發現一個大規模的網釣活動，鎖定使用微軟電子郵件服務的企業，而且採用了先進的中間人（AiTM）攻擊，以繞過多因素認證（MFA）機制，目的是挾持受害者的微軟帳號，並展開商業電子郵件詐騙（BEC）

文/ 陳曉莉 2022-08-04 發表

讚 153 分享



資安業者Zscaler在今年6月發現一個大規模網釣活動，鎖定使用微軟電子郵件服務的企業，而且採用了先進的中間人（AiTM）攻擊，以繞過多因素認證（MFA）機制，目的是挾持受害者的微軟帳號，並展開商業電子郵件詐騙（BEC）。微軟在7月初也曾揭露類似的攻擊行動，強調駭客是藉由AiTM盜走了期間Cookie，因而不論使用者採用任何身分認證方法，都無損於駭客獲准進入期間的能力。（圖片來源 / 微軟）

標的愈明顯被攻擊機率愈高

資安業者Zscaler本周警告，他們在今年6月發現了一個大規模的網釣活動，此一惡意活動鎖定了使用微軟電子郵件服務的企業，而且採用了先進的中間人（Adversary–in–The–Middle，AiTM）攻擊，以繞過多因素認證（Multi–Factor Authentication，MFA）機制，目的是挾持受害者的微軟帳號，並展開商業電子郵件詐騙（Business Email Compromise，BEC）。

在AiTM網釣攻擊中，駭客在使用者與所造訪的網站之間建立一個代理伺服器，藉以竊取使用者所輸入的憑證，以及已通過身分認證的期間Cookie，因而得以挾持使用者的帳號。

微軟在今年7月初也曾揭露類似的攻擊行動，強調駭客是藉由AiTM盜走了期間Cookie，因而不論使用者採用任何身分認證方法，都無損於駭客獲准進入期間的能力，並非為MFA的安全漏洞。

根據Zscaler的觀察，駭客的攻擊對象遍布美國、英國、紐西蘭與澳洲，涵蓋金融科技、借貸、保護、能源與製造業，雖然坊間已有常見的AiTM網釣套件，諸如Evilginx2、Muraena與Modlishka，但駭客在這波攻擊中使用的是客製化套件，且在文章發表時，相關攻擊仍在持續中，每天都會註冊新的網釣網站。

傳統的垃圾郵件閘道無法應付APT攻擊

如何防禦少量、目標客製鎖定、持續性的混合手法?

Gartner電子郵件安全指南-Key Finding

雲端郵件方案逐漸成為主流，防護方式也隨之改變

- 雲端電子郵件應用的持續成長，迫使安全和風險管理者重新評估現有防禦方案(或開始評估)。

雲原生/雲整合/API整合方案逐漸抬頭

- 透過 API 直接整合到雲端電子郵件的解決方案(而不是傳統的Gateway模式)，可以簡化評估和部署並提高偵測準確性，同時網路釣魚防護與核心平台整合，仍舊十分重要。

更需要全方位整合

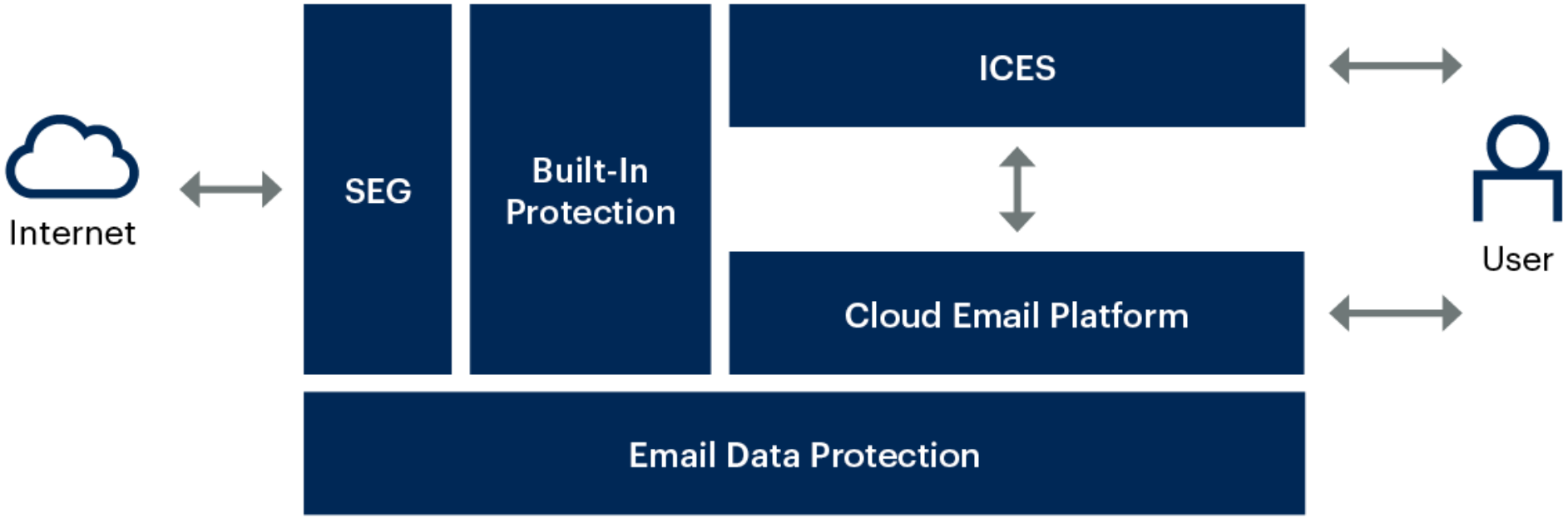
- 整合式解決方案及其他安全工具的整合可提高偵測和回應能力（如擴展偵測與回應 [EDR]）。

DMARC、CASB、MSOAR

- 勒索攻擊、假冒和帳戶接管攻擊正在增加，並導致直接的經濟損失，使用者過於信任與電子郵件代表的身份，而這些身份很容易受到欺騙和社交工程的攻擊。
- 威脅的演變導致對其他技術和服務的需求增加，例如基於Domain-Base的身份、信息驗證 (DMARC)、雲存取安全代理 (CASB)/API 集成、郵件安全治理自動化及響應（MSOAR）。

電子郵件安全子市場架構-Gartner

Email Security Submarket



Source: Gartner

SEG: Secure email gateway; ICES: Integrated cloud email security

735200_C

Gartner

Email安全至少需要的功能

- 多AV掃描
- 網址重寫
- 沙箱整合
- 帶有摘要(end-user digests)的SPAM隔離
- 灰色郵件處理
- 關鍵人物假冒防護 (CIO/CFO)
- 發送後追回
- 其他各種更先進的檢測技術，包括AI、自然语言理解NLU、NLP、社交圖分析（電子郵件通信模式）和圖像識別。

整理一下Gartner建議

新技術/方案應用

- 尋找應用AI 的反釣魚技術進行 BEC 保護。除了通信模式和對話式異常分析，還包含上下文感知，並可協助加強安全意識培訓。以及能檢查(防護/重寫)可疑URL的能力。

將具備 API 的 ICES 解決方案納入評估

- 即使現在用不到，未來也很可能會用 (*ICES：Integrated Cloud Email Solutions)

投資於使用者的教育訓練

- 訓練員工安全意識並建立標準作業程序

強化整合

- XDR、SIEM、SOAR、資料保護

結語

- 壞人永不休息：威脅的形勢嚴峻
- 每個人都能有網路釣魚的故事—而且都是真的。
- 太多的組織仍然沒有準備好，可能正準備要作，但需要付出更多更積極。
- 使用雲端郵件(如M365)，改變了架構，安全策略也需隨之調整。
- 人工智能和機器學習大幅地推動了安全。
- 不要責怪員工，而是給他們更好的培訓。

精誠集團自有產品

SESC次世代郵件安全雲

HEIS資安意識培訓系統

SYSTEX | FOREKNOW LABS

問卷

SYSTEX A DATA SOFTWARE COMPANY

Thank You