白皮書

CLOUDFLARE
AREA 1 SECURITY

如何阻止企業電子郵件入侵威脅

抵禦金融網路釣魚詐騙的進階技術

概觀

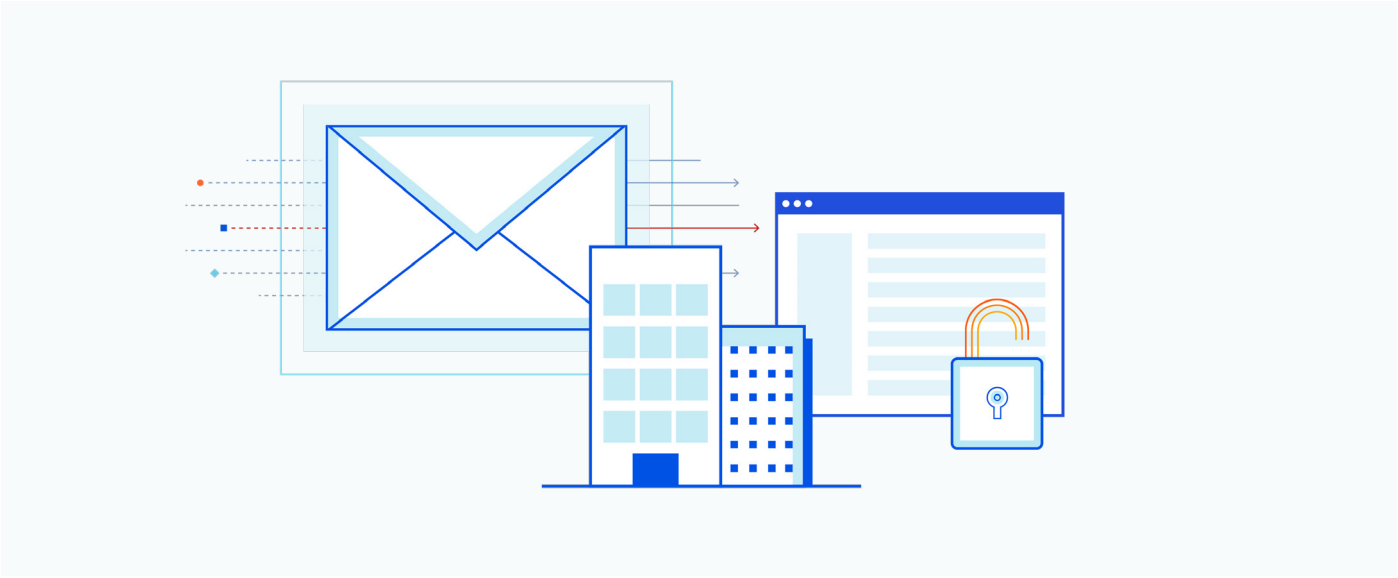
利用受害者與組織之間的現有關係，企業電子郵件入侵 (BEC) 攻擊是一種特定形式的、帶有經濟動機的網路釣魚攻擊。在我們第三次有關 BEC 狀態及演進的年度更新中，我們發現 BEC 仍然是代價最為高昂的網路攻擊，可導致數百萬美元的損失，並超過報告的勒索軟體攻擊造成的損失。

到目前為止，BEC 已經成為多個產業內廣為人知的一個詞彙，因此我們在本報告中不再贅述 BEC 類型的明細。（我們之前對各種 BEC 類型進行了細分，如有興趣，請參閱先前的電子書「2021 年 BEC：基於供應鏈的網路釣魚攻擊呈上升趨勢」）。執法部門在將 BEC 執行者繩之以法方面也取得了進展。最近，有幾名國際 BEC 團夥的犯罪者遭到逮捕，包括一項金額高達 1,000 萬美元的洗錢活動的參與者以及 SilverTerrier，這是一個奈及利亞的大型網路犯罪團夥，其從 50,000 個目標處積聚了超過 800,000 的被盜密碼。

從出奇簡單到精心研究的「長期騙局」，儘管這些網路釣魚攻擊已經在公眾視野中出現很多年，但 BEC 卻能不斷躲過安全系統並與受害者連絡。

為什麼呢？這在很大程度上是因為 BEC 及威脅執行者技術仍在不斷地演進。我們先前提供了有關攻擊者濫用新冠肺炎疫苗供貨情況，以及其他即時事件來作為誘餌的報告。此外，相對簡單、執行成本低以及獲利率也對網路團夥有著極大的吸引力，包括希望「拓寬視野」的民族國家駭客集團。

如欲進一步瞭解 BEC 攻擊的目前狀態以及如何對其進行有效阻止，請繼續閱讀。



BEC – 就像勒索軟體一樣（如果不是更嚴重）影響惡劣

雖然猛增的勒索軟體需求往往佔據著頭條，但根據 FBI 的報告，BEC 卻是最具金融破壞性的網路犯罪之一，造成超過 20 億美元的損失。

然而各類組織卻往往低估 BEC 攻擊的嚴重性。部分原因是大多數公司未能報告 BEC 事件。此外，與攻擊非常明顯的勒索軟體不同，部分組織在之後進行稽核或第三方報告之前，甚至都不知道自己是 BEC 詐騙的受害者。畢竟，BEC 轉帳通常都會經過合法員工的核准！

儘管存在漏報情況，根據「2021 年 Verizon 資料外洩調查報告 2」，BEC 攻擊仍然是第二大常見的社交工程攻擊形式，在每起事件造成的財務損失中，有 95% 介於 250 美元到 984,000 美元之間。

我們自己的資料（來自 2021 年電子郵件威脅報告）顯示，平均 BEC 請求為 150 萬美元。而中位數為 26 萬美元。

雖然 BEC 僅佔攻擊的 1.3%，卻很容易被許多傳統的安全性工具遺漏，因此可能會造成嚴重的財務後果。2021 年，Area 1 Security（已被 Cloudflare 併購）識別並阻止了將近五百萬 (4,987,526) 個 BEC 攻擊 — 其中很多都被傳統的安全電子郵件閘道以及雲端電子郵件套件所遺漏。

Area 1 攔截的平均 BEC 請求 = 150 萬美元

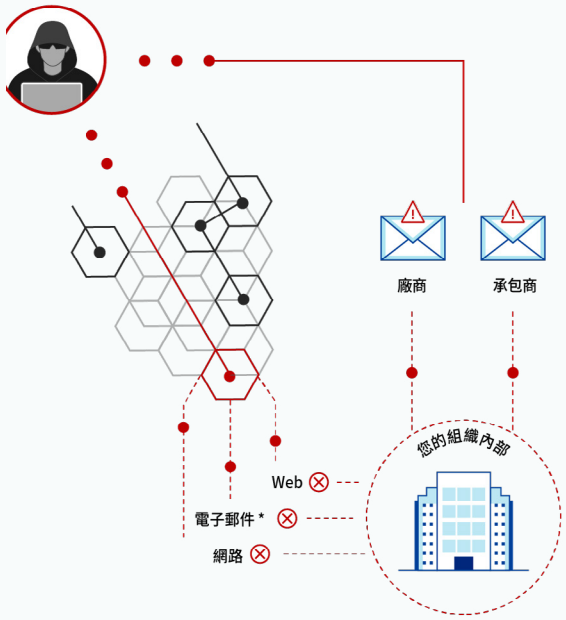
2021 年，Area 1 識別並阻止了將近 500 萬個 BEC 攻擊

[1] https://www.ic3.gov/Media/Y2020/PSA200406
[2] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

BEC「最惡劣的攻擊」

下面是一些最為[惡]名昭彰的 BEC 攻擊，它們打擊各大品牌，造成數百萬美元的損失。

受害者	損失	年	狀況說明
Facebook 及 Google	1.23 億美元	2019	一名立陶宛詐騙者模擬 Facebook 及 Google 的電子產品供應商 Quanta Computer。Facebook 及 Google 向詐騙者支付了 1.23 億美元的假發票。
Crelan Bank	7580 萬美元	2016	總部位於比利時的 Crelan Bank 因詐騙者入侵 CEO 的電子郵件帳戶而損失了超過 7000 萬歐元（約合 7580 萬美元）。該攻擊後來在一次內部稽核中被發現。
Toyota 子公司	3700 萬美元	2019	Toyota Boshoku Corporation（Toyota 集團的子公司）的一間歐洲子公司在一起 BEC 詐騙中被騙，進行了 40 億日元（約合 3700 萬美元）的轉帳。
Scoular	1720 萬美元	2014	美國商品交易公司 Scoular 在收到一封來自 CEO 的虛假電子郵件之後，將 1720 萬美元電匯至詐騙離岸帳戶。
Mattel	300 萬美元（已追償）	2016	Mattel 的一位財務高管在收到一封貌似來自 CEO 的詐騙電子郵件後，將 300 萬美元轉帳至詐騙帳戶。



BEC 攻擊成功率為何仍然居高不下？

眾所周知，偵測 BEC 攻擊相當困難，因此也很難阻止。這些攻擊依賴於真實性以及對目標行為和業務程序的深入瞭解。這種瞭解也會延伸至入侵目標的供應鏈及合作夥伴。其他電子郵件安全解決方案（包括雲端電子郵件提供者及安全電子郵件閘道），無法精確地將這些電子郵件識別為惡意郵件（如欲進一步瞭解攻擊者如何「透過雲端進行網路釣魚」，請按一下這裡）。

受害者陷入 BEC 的四大理由

01

BEC 使用社交工程而非惡意軟體。

BEC 通常為簡短的純文字訊息，不會包含惡意連結或武器化附件。它們依賴於我們遵循社交禮儀（比如向同事伸出援手）或權力動態（比如遵從高管的緊急請求）的習慣，來誘騙受害者向詐騙帳戶轉錢。

傳統的電子郵件安全性工具依賴於掃描惡意連結或附件來尋找已知簽章，而這種做法會遺漏 BEC。

02

攻擊者使用合法網域。

透過以雲端為基礎的電子郵件提供者，任何人都能以低廉的成本輕鬆獲得一個合法的電子郵件網域。例如，攻擊者經常利用免費或低成本的 Gmail 網域，來傳送網路釣魚電子郵件。而購買與目標受害者網域「類似」的合法網域，對於攻擊者而言也不過是小事一樁。

透過使用合法及/或新建立的網域，網路釣魚電子郵件可以通過電子郵件認證檢查。僅依賴網域信譽來確定惡意的解決方案，也可能會遺漏這些 BEC。

03

BEC 數量不多，但針對性很強。

我們的「2021 年電子郵件威脅報告」顯示，BEC 僅佔攻擊的 1.3%，而在電子郵件總量中所佔比例甚至更低。不過，BEC 的針對性極強 — 攻擊者對目標及預定收件者進行研究，製作出看似合法的個人郵件。

安全性工具依賴於基準化「正常」的良性郵件外觀，或者需要更大數量的威脅來製作簽章，因此無法精確地偵測到 BEC。

04

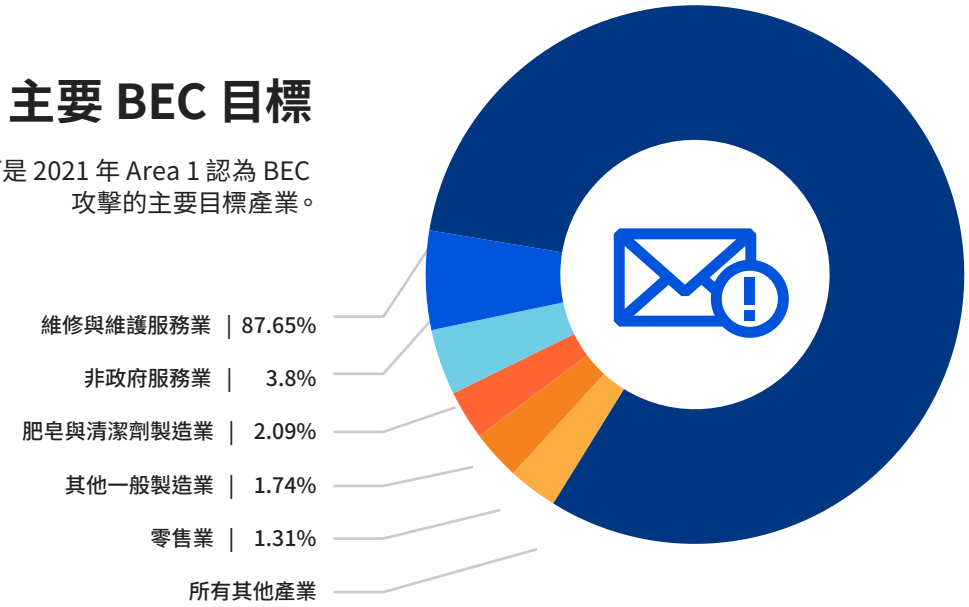
受害者通常不知道帳戶被接管或憑證已外洩

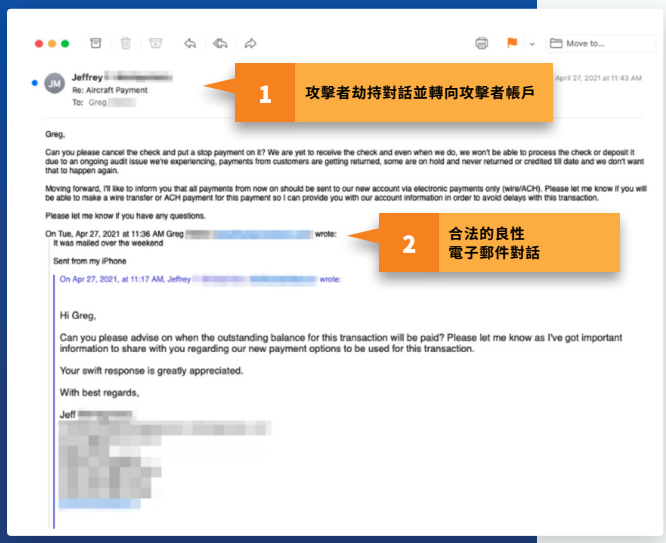
4 型（由 Gartner 的「防範企業電子郵件入侵網路釣魚」報告定義）是最複雜的 BEC，通常利用帳戶接管，即攻擊者劫持了合法使用者的帳戶。攻擊者會默默地觀察正在進行的電子郵件對話（有時會持續數月），然後在關鍵時刻自行插入交談以轉移付款。

只有使用關聯式分析的進階偵測技術，才能截獲這些複雜的入侵廠商攻擊。

主要 BEC 目標

以下是 2021 年 Area 1 認為 BEC 攻擊的主要目標產業。





複雜的 4 型 BEC 是什麼樣的？

BEC 詐騙企圖超過 400 萬美元

此攻擊使用合作夥伴帳戶接管，來劫持合法的良性交談對話，然後將交談轉向攻擊者的帳戶。

攻擊者入侵合作夥伴的帳戶 (「Jeffrey」)，然後劫持對話。透過從惡意的類似網域傳送，攻擊者將對話轉向攻擊者的帳戶。類似寄件者網域與良性網域完全相同，但結尾是 .co 而非 .com。

此攻擊完全符合上文討論的四大「BEC 成功因素」。

阻止 BEC 攻擊的四種技術

雖然細心的收件者可以發現部分 BEC，但最複雜的 BEC 攻擊 – 這些攻擊會導致更大的財務損失 – 通常需要訓練有素的專業人士以及進階網路釣魚偵測解決方案才能發現。細節上的小變化非常重要，特別是在涉及合作夥伴帳戶接管的 BEC 中，因為攻擊者已經擁有正確的「登入」及權限。

01

情緒分析

僅僅查看郵件內容是不夠的。精確的 BEC 偵測需要瞭解郵件的意圖。郵件語氣、寄件者與收件者之間的關係，以及任何關係層次結構都需要考慮在內。

02

主動詐騙決策向上呈報

在複雜的 4 型 BEC 中，交談內的大部分郵件都是良性的。唯一的攻擊者短暫地自行插入對話中來轉移付款。有效的 BEC 偵測解決方案必須包含一種向上呈報方法，並通知即時發生的潛在詐騙通訊。自動封鎖/隔離/撤銷惡意郵件並啟動審查程序可防止資金轉移。

03

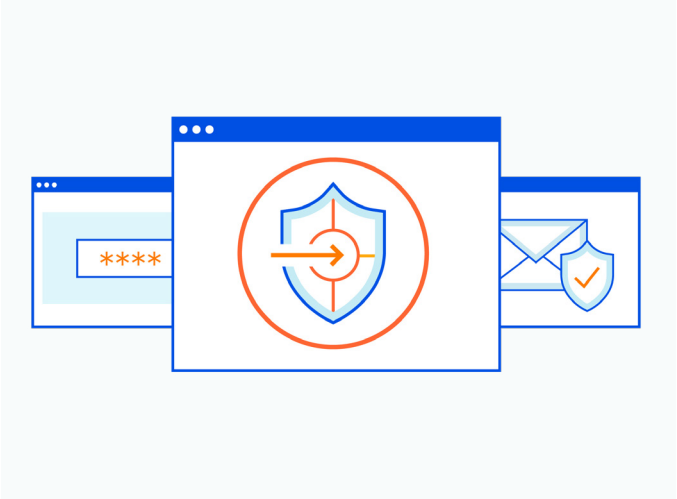
交談與對話分析

與情緒分析類似，交談與對話分析會關注整個交談對話內的意圖與關係。一些細微差別（例如，對話內郵件中的變化以及郵件長度）可能指示寄件者並非他們看起來的樣子，從而指示帳戶被接管以及交談已被攻擊者劫持的情況。

04

寄件者信任圖表

社交圖表在偵測 BEC，特別是以供應鏈為基礎的攻擊方面非常重要，因為該圖表可用於對應風險暴露程度及信任關係。這是發現帳戶接管及合作夥伴模擬的關鍵，其中寄件者是自己組織外部的「受信任」的個人。進階 BEC 偵測技術還會分析合作夥伴社交圖表及傳送歷程記錄。



將 Zero Trust 原則延伸至電子郵件

隨著組織尋求採用新的安全原則及網路架構（如 Zero Trust），電子郵件成為一個關鍵的漏洞。在本電子書中，我們看到了攻擊者如何在適當的時候「僅僅透過詢問」來盜取金錢與資料。BEC 攻擊無需複雜的惡意軟體或網路入侵便可得手 – 它們利用我們對電子郵件通訊的盲目信任。

在 Area 1 加入 Cloudflare Zero Trust 後，客戶將獲得全面的 Zero Trust，其中包含現在最常用且攻擊性最強的 SaaS 應用程式 — 電子郵件。

下文將討論 Area 1 如何協助將 Zero Trust 原則延伸至電子郵件：

假定違規

Area 1 正確地假定始終在發起網路釣魚活動。透過大規模的網路釣魚索引，Area 1 會掃描網際網路來搜捕攻擊者基礎結構，並在到達收件匣的前幾日主動封鎖網路釣魚攻擊。

從不信任

電子郵件是一扇敞開的大門，甚至會入侵最堅不可破的 Zero Trust 網路架構。只是因為電子郵件已設定電子郵件認證，來自信譽良好的網域，或者擁有先前與潛在目標通訊的歷程記錄，Area 1 不會對其信任。實際上，BEC 更可能來自受決定性安全控制「信任」的寄件者和基礎結構。

始終驗證

Zero Trust 的基本原則是不斷地對每個使用者及請求進行驗證，即使其位於企業網路內部。Area 1 在電子郵件到達收件匣前、中、後實施多個保護層級。對所有通訊類型（外部、內部、來自受信任的合作夥伴）都進行類似的盡職分析。透過 Area 1 與 Cloudflare 遠端瀏覽器隔離整合，可以為使用者提供保護，使其免受延遲攻擊活動的影響 — 其中良性連結在到達收件匣後會轉向攻擊者控制的基礎結構。

瞭解（及分享）電子郵件威脅環境

電子郵件與其他所有 SaaS 應用程式都不相同，因為它會產生大量的「模糊」訊號，包括電子郵件內容、語氣及情緒、電子郵件對話中的非預期變化，以及寄件者-收件者關係。Area 1 使用複雜的關聯式分析，來剖析並權衡所有上述訊號，進而識別針對性較強的進行中攻擊 — 保護最常用（也是最不同）的 SaaS 應用程式的使用者。

此外，對 Area 1 產生的威脅情報與在 Cloudflare 網路上觀察到的每日超過 1T 的 DNS 請求進行交叉共用，將會更好地保護客戶，使其免遭所有網際網路威脅。

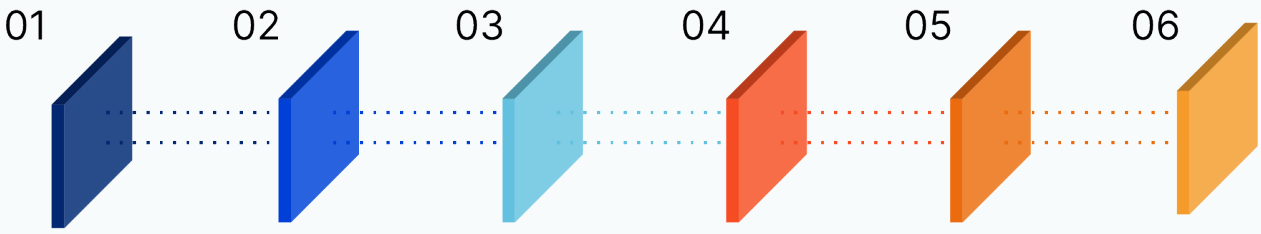
接下來呢？

企業電子郵件入侵可能會為單一組織帶來數百萬美元的直接損失。傳統的電子郵件安全性工具很難識別 BEC，而使用進階偵測技術的電子郵件安全解決方案可以最有效地進行阻止。

Area 1 始終專注於阻止網路釣魚攻擊 — 這是單一、最大型的網路威脅手段 — 包括 BEC 攻擊。我們的雲端原生電子郵件安全平台使用複雜的關聯式分析，在造成損失之前偵測所有類型的 BEC 攻擊。

用於偵測並阻止 BEC 的進階技術

我們使用各種專有技術來偵測全面的進階攻擊，包括 BEC。我們的雲端擴展解決方案可與各種規模的組織整合並提供支援。



結構分析	NLU 模型（自然語言理解）	情緒分析	對話分析	產業模型	信任圖表
標頭、內文、影像、電腦視覺連結、有效負載	寫入模式 類別 運算式	意圖、 語氣、關係、 層次結構	交談 變化 長度	垂直 通用語 業務流程	合作夥伴社交圖表、 傳送歷程記錄、 ATO 探索 合作夥伴 模擬

若要瞭解我們如何偵測並阻止複雜的 BEC 攻擊，請要求示範。