2026
第三季電子郵件安全觀察



ASRC

Spam Mail
Virus Mail
Malicious Mail

Oct 2026 released.

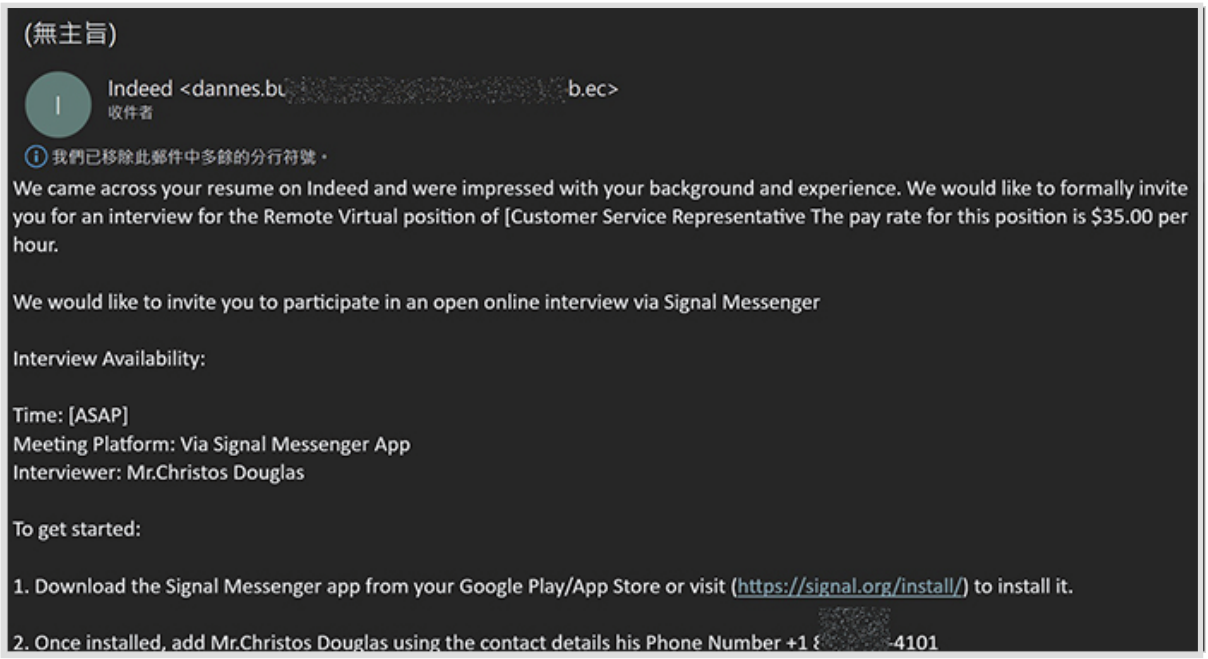
2026 年第三季，電子郵件安全威脅呈現出顯著的攻擊手法演進。自第二季末起，針對郵件伺服器的阻斷服務（DoS）攻擊大幅增加，持續消耗企業郵件系統資源。同時，社交工程攻擊與進階規避技術的結合成為主流。攻擊者大量轉向「雲端寄生」（Living off the Cloud, LotC）策略，並濫用 VHDX 虛擬硬碟格式等新興威脅載體（Threat Vector）進行惡意軟體派發。這些演進顯示駭客正積極發展能繞過傳統端點防護與靜態網址掃描的進階防禦迴避（Defense Evasion）技術，企業需重新評估現有的郵件安全邊界。

2026 Q3 關鍵攻擊樣本與手法剖析

求職詐騙，假職缺郵件的社交工程陷阱

攻擊者持續鎖定求職網站，利用履歷上的聯絡方式發送夾帶優渥待遇的假職缺郵件，並以急迫語氣要求透過加密通訊軟體進行遠端面試。此手法利用求職者急於謀職的心理，設下騙取個資、匯款手續費、假支票詐騙或植入後門的陷阱，令人防不勝防。實務上，攻擊者常在攻擊準備階段利用公開來源情報（OSINT）與求職平台（如 CareerBuilder）進行目標探勘與前置作業。

與真實求職信相比，此類詐騙郵件通常不揭露具體公司資訊，缺乏詳細職務說明，對目標背景描述模糊，且多使用非正式通訊管道發送。為躲避過濾系統，攻擊者亦可能偽冒合法寄件者，或利用遭入侵的郵件系統發送。這些郵件排版通常較不正式，不採用企業標準面試排程工具，而是私下要求使用私人加密軟體進行面試或聯絡。若擔心錯失真實面試機會，應透過親自查證過的官方聯絡方式核實，切勿直接回覆或點擊郵件中的私下聯絡連結。


(無主旨)

Indeed <dannes.bu[redacted]b.ec>
收件者

我們已移除此郵件中多餘的分行符號。

We came across your resume on Indeed and were impressed with your background and experience. We would like to formally invite you for an interview for the Remote Virtual position of [Customer Service Representative The pay rate for this position is $35.00 per hour.

We would like to invite you to participate in an open online interview via Signal Messenger

Interview Availability:

Time: [ASAP]
Meeting Platform: Via Signal Messenger App
Interviewer: Mr.Christos Douglas

To get started:

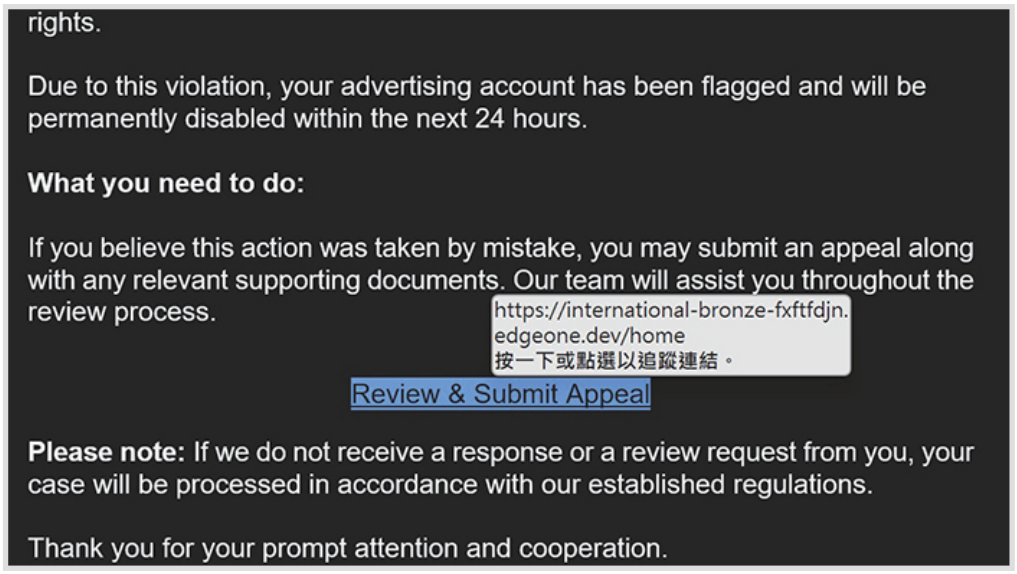
1. Download the Signal Messenger app from your Google Play/App Store or visit (https://signal.org/install/) to install it.

2. Once installed, add Mr.Christos Douglas using the contact details his Phone Number +1 [redacted]4101

求職詐騙郵件，要求私下以加密通訊軟體進行遠端面試

濫用合法雲端服務，規避釣魚偵測的雲端寄生手法

這一季，我們發現大量釣魚郵件連結濫用合法的雲端服務，此手法稱為「寄生雲端」（Living off the Cloud, LotC）或「濫用信任網站」（Living off Trusted Sites, LOTS）。由於傳統釣魚網站易被 AI 或安全瀏覽器偵測攔截，駭客正大規模向合法雲端平台轉移，現今約有近 50% 的釣魚網站濫用合法雲端服務來規避過濾系統。許多「釣魚即服務（PhaaS）」套件也預設支援將惡意頁面部署於此。



寄生雲端（Living off the Cloud, LotC）成為釣魚網站的重要趨勢

這些雲端寄生網站讓攻擊者能以極低成本獲取合法網站憑證與瀏覽器信任，並利用服務自帶的 CAPTCHA 驗證碼阻擋資安系統的自動掃描。此外，攻擊者可利用手機版 Google App 或 Chrome 瀏覽器的「分享（Share）」功能，將惡意網址自動轉換為 https://share.google/ 開頭的隨機亂碼格式。這種透過合法分享機制進行的攻擊加工，能有效規避多數針對網址的靜態掃描。



透過合法的「分享」，對惡意超連結進行隱蔽的攻擊

VHDX「虛擬硬碟」夾帶惡意程式，以多重封裝技術繞過檢測

本季也觀察到利用 VHDX（Virtual Hard Disk v2）檔案格式進行的惡意攻擊樣本。攻擊者先透過 Google Sites 打造看似合法的靜態網頁，誘騙受害者點擊縮址連結，下載一份標示為訂單資料、實則高達 164MB 的虛擬硬碟檔案。

此攻擊利用異常龐大的 VHDX 檔案體積，且內部包裝了一層 .img 映像檔，藉由多重封裝技術成功繞過防毒軟體的容量與格式檢測限制。當受害者遭誘騙將其掛載為虛擬磁碟後，才會暴露出內藏的惡意 JavaScript 攻擊本體；一旦執行，電腦極可能遭植入後門。此攻擊鏈結合了社交工程與進階防禦迴避，反映出威脅載體已從傳統惡意巨集文件，演進為能利用作業系統內建掛載功能的虛擬磁碟映像檔。



假的物流通知信



利用 Google Site 打造出的靜態頁面



導向縮址網站，下載大小約 164MB 的虛擬硬碟

防禦建議

攻觀察第三季的攻擊手法，攻擊者正極大化地利用「合法掩護非法」的策略，無論是濫用合法雲端平台（LotC）或利用作業系統原生支援的掛載檔案格式（如 VHDX、IMG），其核心皆為防禦迴避（Defense Evasion）。

針對上述趨勢，建議採取以下防範措施：

1. 落實電子郵件身分驗證

企業應全面配置並嚴格執行 SPF、DKIM 與 DMARC 等電子郵件安全協定，以防範網域偽冒與商業電子郵件詐騙（BEC），並驗證外部寄件者身分。

2. 動態與沙箱分析升級

針對 VHDX 或 ISO 等可掛載的映像檔格式，傳統防毒軟體常因檔案過大而略過掃描。企業應於郵件閘道端阻擋非業務必要的虛擬硬碟副檔名，或設定規則將異常檔案導入沙箱進行深層拆解分析而非依據檔案大小判定是否深度檢查；同時評估透過群組原則（GPO）限制一般使用者自動掛載映像檔或隨身碟的權限。

3. 依循零信任架構（Zero Trust）與網頁隔離

鑑於合法雲端服務遭到廣泛濫用（LOTS），單純依賴網域信譽評等（Reputation）的靜態黑名單已不足以防禦。建議導入遠端瀏覽器隔離技術（RBI）、加強網頁內容過濾，或以企業專屬的郵件政策進行限制，將來源不明、非業務用途的雲端分享連結視為不可信流量進行阻擋。

4. 資安意識培訓（Security Awareness）

個人對於要求跳脫企業正規流程（如使用私人通訊軟體面試）或帶有強烈急迫性的訊息，應培養「預設懷疑」的查證習慣，以阻斷社交工程的攻擊鏈。

關於ASRC 垃圾訊息研究中心

ASRC 垃圾訊息研究中心 (Asia Spam-message Research Center)，長期與中華數位科技合作，致力於全球垃圾郵件、惡意郵件、網路攻擊事件等相關研究事宜，並運用相關數據統計、調查、趨勢分析、學術研究、跨業交流、研討活動..等方式，促成產官學界共同致力於淨化網際網路之電子郵件使用環境。

更多資訊請參考 www.asrc-global.com



ASRC垃圾訊息研究中心

© 2026 Asia Spam-message Research Center. All Rights Reserved.