電子郵件：謹慎點擊

如何防範網路釣魚、詐欺與其他詐騙

CISCO

目錄

簡介

到去年，垃圾郵件攻擊已超過40 年了。沒錯，早在 1978 年，Digital Equipment Corporation 的行銷經理 Gary Thuerk 為了推銷新產品，寄出了第一封垃圾郵件給原始 ARPANET 上的 393 人。毫不意外，大家對這封訊息的接受度如同今天的垃圾郵件。Thuerk 不僅受到嚴厲譴責，而且被告誡不要再犯。

如果現在也那麼單純就好。四十年來，垃圾郵件日益猖獗，諸如藥品、減肥產品和工作機會等資訊充斥在我們的收件匣。不僅如此，還加入了更危險的親戚：網路釣魚和惡意軟體。網路釣魚最初是在 30 年前構思出來的，惡意軟體也有長達幾十年的電子郵件發送歷史。

如今，遺憾的事實是許多電子郵件都是不需要的垃圾郵件或更糟，而且數量驚人 – 根據 Talos 情報，2019 年四月的所有電子郵件中有 85% 是垃圾郵件。不需要的電子郵件數量也持續增加；垃圾郵件在四月創下 15 個月以來的新高。

寄件者與收件者

電子郵件的結構幾乎可說是詐騙人士的理想形式。電子郵件強迫使用者閱讀和評估他們收到的郵件，然後決定要開啟或是點擊哪些內容。只要有恰到好處的社交工程，就能利用每個人的善良天性，誘騙使用者點選。

社交工程不僅使其成為誘人的攻擊媒介， 也是難以系統性防禦的挑戰。電子郵件傳播的攻擊很少會繞過使用者。雖然從 URL 連結至遭到入侵或使用漏洞攻擊包的惡意網站非常常見，這種方式仍然需要強迫使用者先點選電子郵件中的連結。

這對企業有何意義

難怪電子郵件是令資安長徹夜難眠的的主要挑戰之一。從我們最近的資安長基準研究中，我們得知 56% 的受訪的資安長認為要防範使用者行為，例如點擊電子郵件中的惡意連結，是非常或極度困難的事。這比任何其他受調查的安全隱憂排名都高 – 高於公有雲中的資料，以及行動裝置的使用。

這類攻擊發生的頻率也是引起資安長注意的原因。例如，有 42% 的受訪資安長所處理的資安事件，是由於有人在組織內開啟惡意垃圾郵件所造成的結果。36% 則因為網路釣魚竊取資訊而處理過類似的事件。根據我們的資安長基準資料，資安長認為電子郵件威脅是對組織的首要資安風險。

受思科委託並於 2018 年由 ESG 執行的一項單獨研究中指出，70% 的受訪者回報防範電子郵件威脅變得日趨困難。就電子郵件傳播攻擊的後果而言，75% 的受訪者表示他們的營運受到重大影響，而 47% 的人回報受到嚴重的財務衝擊。

所需的回應

如何保護具有風險的必需品呢？許多組織將移轉到雲端視為解決方案。但是雲端並非防範電子郵件風險的萬靈丹。在多數情況下，這只是權宜之計。安全性問題不會消失，而是繼續存在。

您可以透過多種方式把電子郵件威脅的整體影響降到最低。在本文中，我們將討論目前的威脅趨勢，提供現今最常見的電子郵件攻擊類型概述。分析它們的過程、目標和背後的基礎設施。並討論您可做什麼來保護業務安全，以及如何在使用者遇到電子郵件傳播的威脅時加以辨識。

「我們平均一天會收到大約412,000封電子郵件，其中266,000封訊息甚至無法送到我們的SMTP 引擎，因為 Talos 會根據他們的全球威脅情報封鎖這些郵件。」

紐約州立大學 (SUNY) 舊韋斯特布里學院安全長 Milind Samant

「公司需要在安全性與業務風險和使用者體驗之間取得平衡。一旦取得平衡，您就需要在出現問題時能採取防禦措施和主動回應的計畫。人為錯誤是既定現實，如今有個數億美元的網路犯罪產業就靠這樣的人為錯誤。您應該為錯誤做好準備，並在發生問題時迅速回應。我們每天都會發現網路攻擊透過人為錯誤成功地擊敗安全性防禦，或是發現鎖定資產和軟體漏洞的不肖人士，但是每天我們都能透過主動的偵測與回應，確認自己不僅找到而且遏制了這些攻擊。我正是透過這個方式，所以知道我們有一個功能完備的安全計畫。」

思科資安長 (CISO) Steve Martino

目前電子郵件和網路釣魚的趨勢

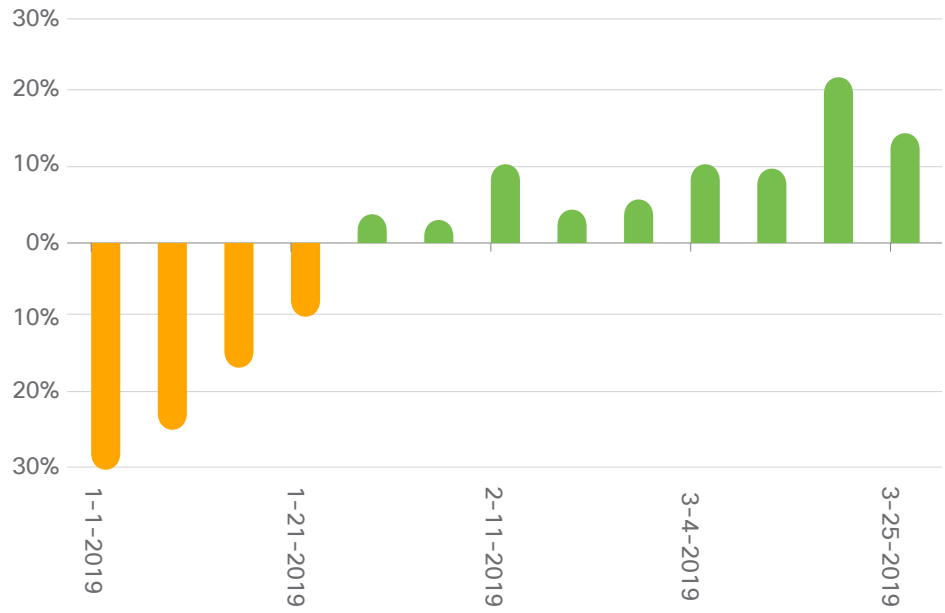
電子郵件帶來的危害有很多。根據思科也有參與的 Verizon 2018 年資料外洩調查報告指出，電子郵件是惡意軟體發送 (92.4%) 和網路釣魚 (96%) 的首要媒介。點擊錯誤的郵件，您可能就是挖礦的受害者，認證遭竊，或是因為落入社交工程騙局而損失大量金錢。如果情況擴展到企業層級，不當的郵件就會造成嚴重破壞。

使用者有多常受到電子郵件詐騙呢？只需問問 Duo Security 的員工。團隊在幾年前建立了免費的 Duo Insight 工具，讓使用者可以自行建立假冒的網路釣魚活動，並在自己的組織內進行測試，看看誰會上鉤。

不幸的是，許多人還是中計了。根據 2018 年 Duo Trusted 存取報告顯示，62% 的網路釣魚模擬活動都至少獲取一組使用者認證。在所有收件者中，幾乎有四分之一的人點擊了電子郵件中的網路釣魚連結。其中一半的人在假冒網站中輸入了認證。

獲得如此的成功，難怪電子郵件是發起網路釣魚活動的熱門選擇。事實上，如果 Cisco Umbrella 發現的新網路釣魚網域數量可作為指標，那麼網路釣魚活動可能持續增加。我們在 2019 年第一季度取每週平均值，然後將每週的數值與該平均值做比較。圖 1 的結果顯示今年雖然起步緩慢， 但是新建立的網域數量持續加速，從季度的第一週到最後一週增加了 64%。

圖 1 每週新的網路釣魚網域與第一季度的週平均比較圖。



資料來源：思科資安防護傘

常見電子郵件攻擊類型

以下是現今最常見的電子郵件詐騙。拿起您的筆記型電腦，開啟您的收件匣，並想像以下未讀郵件正在等待您。

類似的網路釣魚攻擊也發生在其他雲端式電子郵件服務，例如 Gmail 和 G Suite。

Office 365 網路釣魚

電子郵件看似來自 Microsoft。信上寫著由於錯誤或違規，您的 Office 365 電子郵件地址將中斷連線。防止這種情況發生的唯一方法就是透過提供的連結驗證地址。

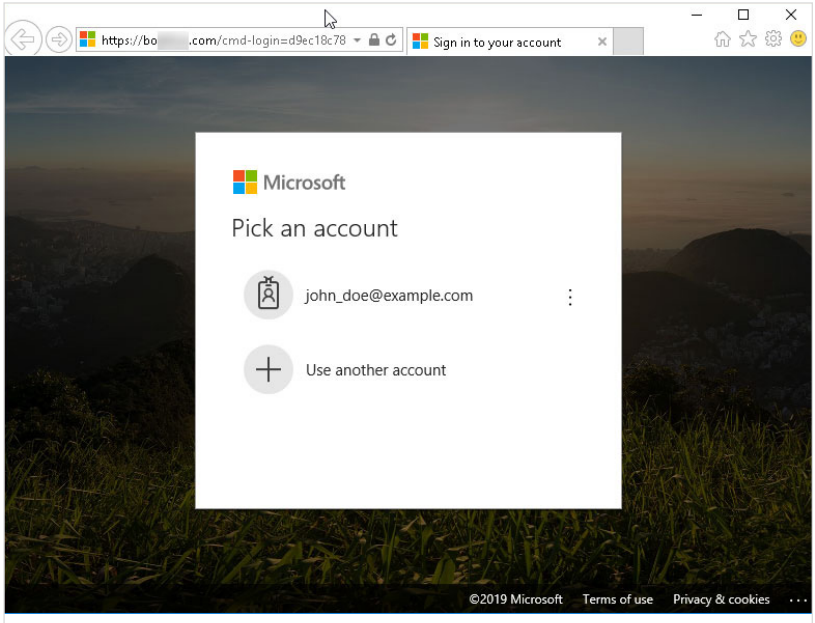
這是企圖竊取您的 Office 365 認證的網路釣魚手法。信上使用的電子郵件和 URL 甚至就像您在 Office 365 中會看到的風格，例如：micros0ftsupport@hotmail.com。如果您點擊連結，將連至看似官方的登入頁面，要求您提供電子郵件地址和密碼。

只不過網站是假的。一旦詐騙人士擁有您的憑證，他們可能會試著登入其他 Microsoft 相關服務，並獲取您的聯絡人資訊。一種常見的技巧是登入您的電子郵件信箱帳戶，並向您的聯絡人傳送包括另一個網路釣魚 URL 的非正式郵件（例如，主旨：參考資訊）。

這種攻擊方式在持續增加中。根據我們的合作夥伴 Agari 在他們 2019 年第 2 季度電子郵件詐欺和身份詐騙趨勢報告中發佈的資料，27% 的進階電子郵件攻擊都是從遭入侵的電子郵件帳戶傳送的。這比 2018 年最後一季度上升了七個百分點，當時僅有 20% 的網路釣魚攻擊來自遭入侵的電子郵件。

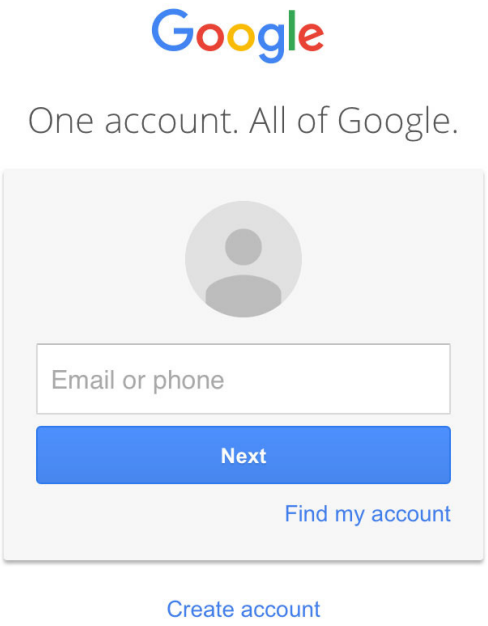
Office 365 不是唯一被鎖定的目標。類似的網路釣魚攻擊也發生在其他雲端式電子郵件服務，例如 Google 的雲端電子郵件產品 Gmail 和 G Suite。由於 Google 帳戶十分普遍且可用來登入網際網路上的各種網站，攻擊者會在這個領域建立網路釣魚網站也就不足為奇了。

圖 2 網路釣魚網站刻意設計的像是 Microsoft 的登入頁面。



***備註：**這樣的 Microsoft 畫面是假冒的，是由網路威脅發動者所發動，並使用它來欺騙觀看者以為這是來自 Microsoft 的合法標誌和訊息。*

圖 3 Google 帳戶登入範例。您能辨別真假嗎？



備註：這樣的 Google 畫面是假冒的，是由網路威脅發動者所發動，並使用它來欺騙觀看者以為這是來自 Google 的合法標誌和訊息。

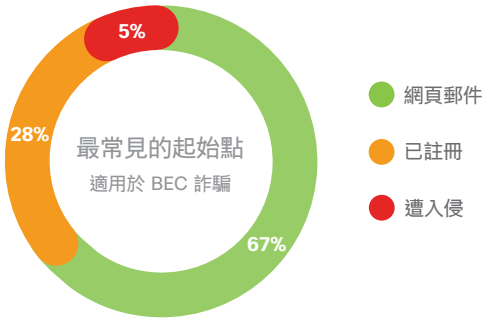
商務電子郵件入侵

這週舉行重要的公司高峰會，除了維護重要功能的少數人之外，所有人都離開了辦公室。您是財務團隊的成員，也是仍在現場的骨幹團隊成員之一。突然間，收件匣出現一封似乎是來自財務長的信，主旨寫著「尚未付款」。信上說明上週有一筆款項尚未付款，所以公司的供應鏈可能會因此中斷。附件是電匯說明。寄件者在文末還說他們會在一小時內電話聯絡您討論此事。

這是商務電子郵件入侵 (BEC) 的典型案例。BEC 詐騙是一種電子郵件詐欺形式，攻擊者偽裝成 C 級或以上的高階主管， 企圖欺騙收件者為非法目的執行業務功能，例如匯錢給他們。有時他們確實會用電話聯絡對方，冒充高級主管。而且似乎有效。根據網際網路犯罪申訴中心 (IC3)，BEC 詐騙在 2018 年造成 13 億美元的虧損。

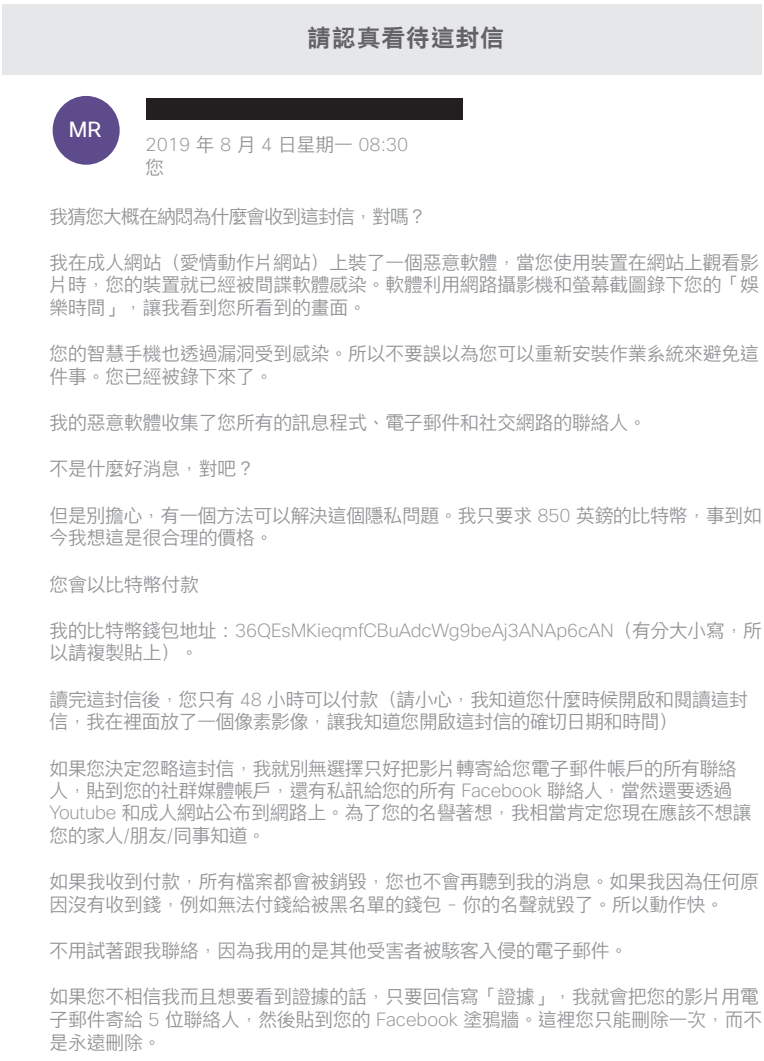
您可能以為攻擊者會利用 BEC 詐騙中遭入侵的帳戶，就像他們在 Office 365 網路釣魚詐騙中所做的一樣。令人驚訝的是，根據 Agari 2019 年第 2 季度電子郵件詐欺和身份詐騙趨勢報告顯示，只有約 5% 的詐欺案這麼做。三分之二的攻擊仍然使用免費的網路電子郵件帳戶發起攻擊，其餘的 28% 則使用註冊網域進行自訂的攻擊。後者的個人化程度甚至擴展到電子郵件內文，Agari 指出每五個 BEC 電子郵件中就有一個包含目標收件者的姓名。

圖 4 BEC 電子郵件起始點。



資料來源：Agari Data, Inc.

圖 5　近期數位勒索範例。



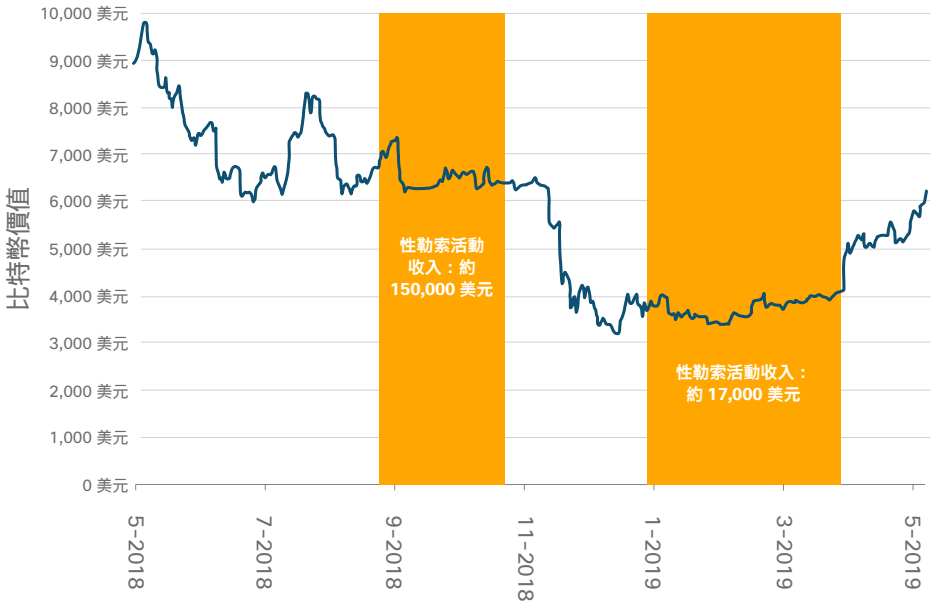
數位勒索

您的收件匣收到一封主旨為**「請認真看待這封信」**的電子郵件。電子郵件的寄件者宣稱已入侵您造訪過的成人影片網站。對方還表示已透過您的網路攝影機錄下您的一舉一動，裡面還有他們聲稱您所觀看的影片。此外，寄件者還說已獲得您的聯絡人資料，而且打算將所有的影片傳送給他們，除非您支付數百美元，甚至是數千美元的比特幣。

這就是數位勒索。這和較傳統的勒索情境唯一不同之處就是所有的資訊都是捏造的。詐騙人士不僅沒有入侵網站，他們也沒有錄影，更沒有您的聯絡人清單。他們只是希望能騙您相信他們有。

我們在「本月威脅」部落格文章「要錢還是要命：數位勒索詐騙」(Your money or your life: Digital extortion scams) 中，涵蓋了這類型電子郵件詐騙的諸多形式。

圖 6 比特幣價值 (USD) 與性勒索活動收入的比較。



來源： Cisco Talos

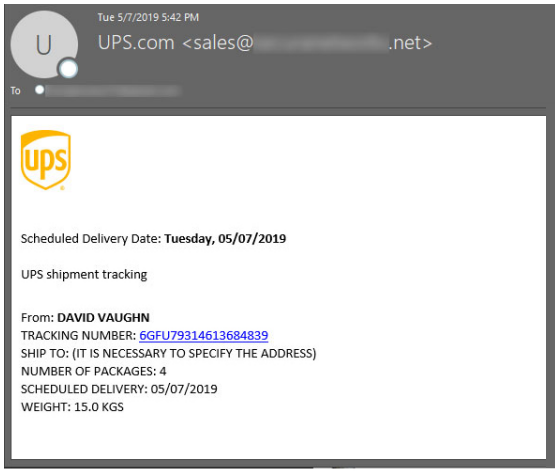
這是一個有趣的騙局，而且對攻擊者來說有利可圖，從數位勒索活動中獲得的利潤在 2018 年年底達到六位數。但是根據思科 Talos 進行的最新分析，涵蓋 2019 年一月至三月的利潤已經下降。利潤的升降與比特幣的價值約略相關，不過跌幅還是相對較大。隨著比特幣的市值回升，我們也想瞭解數位勒索活動款項是否也會增加。

包裝與發票垃圾郵件

「我不記得有訂閱這個手機應用程式」您自言自語地說道。至少電子郵件是這麼說的：例如電影俱樂部的終身訂閱。等一下，發票上列出的地址顯示這是在斯里蘭卡買的，而您甚至不住在斯里蘭卡。「一定是弄錯了」您對自己說，一邊快速開啟附件的 PDF 調查原因。

不幸的是 PDF 包含漏洞攻擊，最終會下載 Emotet 到您的裝置上。詐騙手法包羅萬象，不過通常都包含您未訂購的包裹、未購買產品的發票或您未加入的訂閱或服務月費。可能導致各種不良後果，從被竊取的銀行認證到挖礦。

圖 7 Emotet 詐騙電子郵件，假裝來自 UPS。



***備註：**這樣的 UPS 畫面是假冒的，是由網路威脅發動者所發動，並使用它來欺騙觀看者以為這是來自 UPS 的合法標誌和訊息。*

圖 8 近期預付款詐欺範例。

Christoper A. Wray 先生

CW

聯邦調查局局長 (FBI)
收件者：[redacted]
回覆至：[redacted]

收件人：受益人。

根據辦公室的道德規範，首次聯絡時自我介紹總是十分重要。我是美國聯邦調查局 (FBI) 局長 Christopher A. Wray 先生。本官方備忘錄旨在通知您，替美國政府工作的部分官員試圖利用後門管道轉移您的資金。事實上，我們於今早逮補一名嫌犯後，透過聯邦調查局 (FBI) 政風處的秘密調查員得知此事。

上述嫌犯於今天稍早在杜勒斯國際機場，因企圖攜帶大量資金至美國海外遭到逮補。根據美國洗錢法令，該筆金額無法以現金攜至美國境外且為刑事犯罪，得依照美國 1982 年洗錢法予以懲處。本法令為全球法律，適用於大多數已開發國家以打擊恐怖主義和洗錢活動。

根據本單位收集的資訊，發現該筆資金實際屬於您，但因為負責款項的官員從事某種不法行為，此行為徹底違反任何付款機構的道德規範，所以此款項遭到延遲。目前該筆資金由付款銀行代為保管，我可以向您保證若您和我們誠實以對，資金將順利釋出。此外，我們需要您在各個層面與我們積極合作，因為我們正在密切監控這項交易，以揪出現今社會中的不可信任之人。

我們已於 2019 年 5 月 9 日指示付款銀行的高階管理人員，將該筆資金支付給您作為認證受益人，我們掌握重要真實資訊/紀錄，證明資金確實屬於您。儘管如此，您需要向我們提供下列資訊（用於官方驗證）。

1. 名字、中間名與姓氏。
2. 年齡。
3. 職業。
4. 婚姻狀況。
5. 直撥電話/傳真號碼。
6. 居住地址。

我們期待您立即遵守官方義務，以便收到授權付款銀行支付的款項。

官方蓋章。

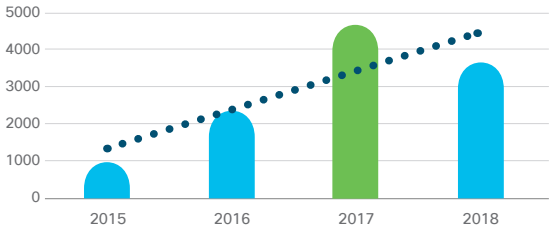
Christopher A. Wray 先生
聯邦調查局局長 (FBI)

預付款詐欺

FBI 發來的郵件不是每天都有。收到通知您有 1050 萬美元待匯款的信就更少見了！您只需要回信，他們就會指示您如何收款。

這是經典的預付款詐欺騙局。顧名思義，詐騙人士會在匯出所承諾的款項前先向您索取費用，但這筆匯款永遠不會出現。這也是舊的電子郵件詐騙手法之一，過去幾年形式稍有變化，從希望分享財富的異國王子到為信用不佳的人審核貸款。不過詐騙依舊屹立不搖，美國商業促進局 (BBB) 每年都會接獲數以千計的電子郵件詐騙投訴。

圖 9 BBB 每年獲報的預付款詐欺騙局。
（預付款貸款、奈及利亞/外幣兌換、愛情、信用修復/債務減免、投資、與旅遊/假期詐騙類別總數。）



資料來源：美國商業促進局

電子郵件中的惡意軟體

大部分的惡意軟體仍然透過電子郵件傳送。過去手法較顯而易見，.exe 檔案直接放在電子郵件的附件裡。但是隨著使用者明白開啟可執行檔不是安全的決定後，惡意攻擊者便改變了策略。

如今，惡意軟體通常都是間接傳送，無論是透過較不可疑的附件，例如常用的業務檔案，或是訊息本文中的 URL – 經常都是透過一般有效的電子郵件通訊傳送的項目。目的是為了避開會攔截和隔離二進位檔案或其他不常見附件的傳統電子郵件掃描。

檢視今年迄今（2019 年一月到三月）所標記的電子郵件附件時尤為明顯。二進位檔案占所有惡意附件不到百分之二 – 不僅是 .exe 檔，還包含所有二進位檔案。相較過去幾年經常遇到可執行檔、Java 和 Flash 檔的日子，這改變相當大。事實上，Java 和 Flash 已經變得相當冷門，就算把它們和二進位檔案算在一起，仍然只會佔附件的 1.99%。

封存檔例如 .zip 檔案，構成將近三分之一的惡意附件，也是攻擊者使用的前十種檔案類型的第四名。

表 1 惡意附件類型。

類型	百分比
Office	42.8%
封存檔	31.2%
指令檔	14.1%
PDF	9.9%
二進位	1.77%
Java	0.22%
快閃記憶體	0.0003%

資料來源：Talos 情報

最常見的附件類型就是每天在辦公室間傳送的附件 – 五個中就有兩個惡意檔案是 Microsoft Office 文件。

那麼攻擊者偏好哪些類型的附件呢？封存檔例如 .zip 檔，構成附件的幾乎三分之一，也是前十種檔案類型的第四名。指令檔例如 .js 檔，構成 14.1%。和我們上次檢視附件類型時相比，指令檔大幅增加，在 2018 年度網路安全報告 (ACR) 中，.js 檔加上 XML 與 HTML 只佔惡意檔案副檔名的百分之一。

這些類型的檔案作為惡意附件的頻率持續增長，從 2018 年的 ACR 上漲近五個百分比。若再加入 PDF 檔案，那麼半數以上的惡意附件都是經常使用的文件類型，在現代工作空間中無所不在。

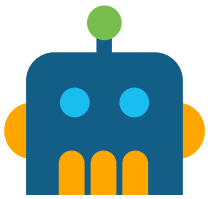
表 2 10 大電子郵件中的惡意副檔名。

副檔名	百分比
.doc	41.8%
.zip	26.3%
.js	14.0%
.pdf	9.9%
.rar	3.9%
.exe	1.7%
.docx	0.8%
.ace	0.5%
.gz	0.5%
.xlsx	0.2%

資料來源：Talos 情報

電子郵件傳輸基礎架構

現在讓我們走到幕後，遠離電子郵件或負載類型，並了解惡意電子郵件的傳播方式。詐騙人士發起發起垃圾郵件攻擊活動的主要方法有兩種：僵屍網路和大量電子郵件工具組。



殭屍網路

垃圾郵件僵屍網路目前是傳送大多數垃圾郵件的主要罪魁禍首。以下是垃圾郵件僵屍網路趨勢中的關鍵角色。

Necurs

Necurs 僵屍網路最早於 2012 年出現，散播從宙斯到勒索軟體等各種威脅。雖然它的活動在過去受到極大關注，但 Necurs 似乎已逐漸退居幕後，至少在新聞報導方面是如此。不過這種僵屍網路依舊十分活躍。事實上，Necurs 僵屍網路是包括數位勒索等各種詐騙的主要傳播工具。

如需有關 Necurs 的更多資訊，請查看由思科 Talos 執行的分析文章「Necurs 僵屍網路的多支觸角」。

Emotet

許多 Emotet 傳送的垃圾郵件都屬於包裝和發票類別。Emotet 是包含垃圾郵件殭屍外掛程式的模組化惡意軟體。由於幕後的攻擊者是利用 Emotet 作為其他威脅的傳播管道來賺錢，因此垃圾郵件殭屍模組傳送的多數垃圾郵件目的都是透過 Emotet 感染更多系統，來進一步擴大惡意傳播管道。

Emotet 會竊取受害者信箱的內容，所以通常能夠作出惡意但看似逼真的對話訊息，讓收件者誤以為是原有對話的一部分。Emotet 還能竊取 SMTP 認證，霸佔受害者的外傳電子郵件伺服器作為輸出垃圾郵件的工具。

如需有關 Emotet 的更多資訊，請閱讀我們先前網路安全報告系列中的威脅報告「防範今日的嚴重威脅」。

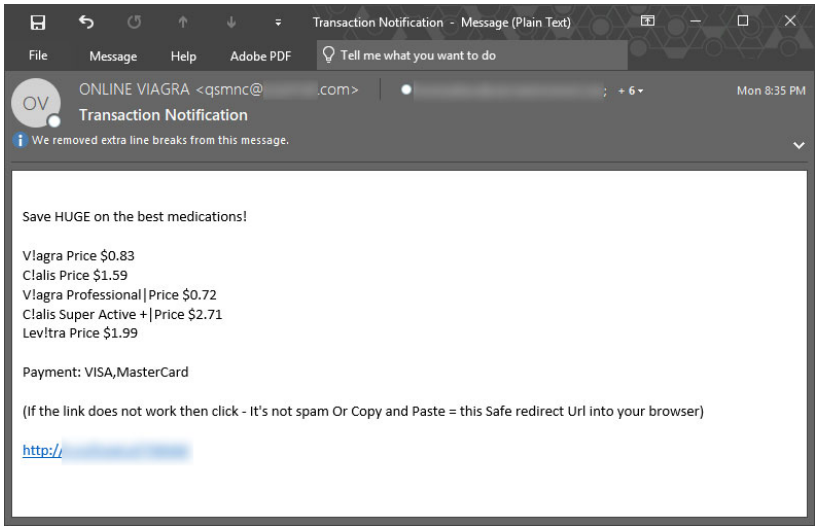
> **「Cisco Email Security 不僅降低偵測花費的時間，更減少約 80% 的垃圾郵件。」**
>
> **佛羅里達州薩拉索塔安全官員**
> **Jacquelyn Hemmerich**

Gamut

Gamut 僵屍網路一直忙於發送約會和親密關係的垃圾郵件，主題大多圍繞著在您附近認識新的人。在其他活動中，僵屍網路背後的攻擊者也會傳送消息兜售藥品或工作機會（見圖 10）。

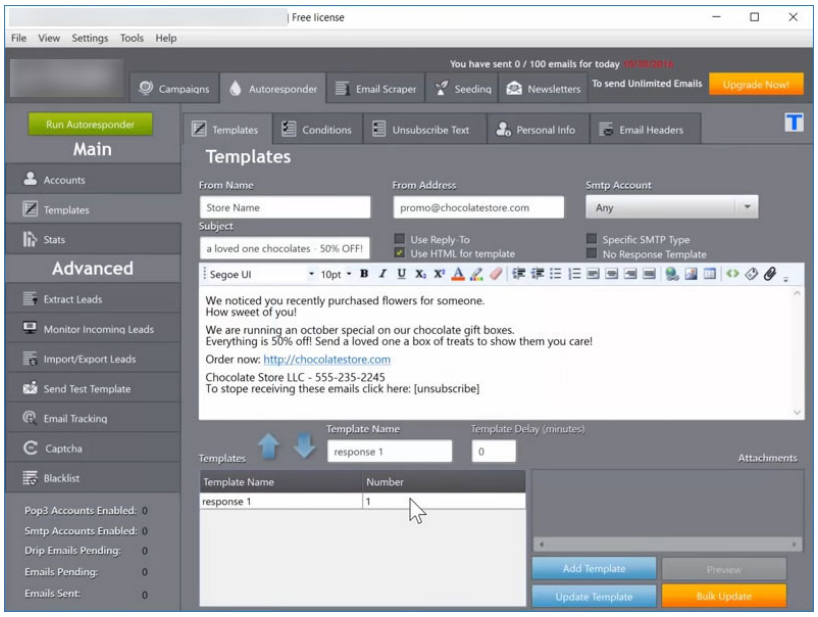
他們註冊了各種網域，雖然基礎架構看似簡單，一個網域下有數個子網域，而且通常指向一個 IP 位址。思科尚未確認他們所提供的服務是否合法，但註冊過程似乎像是網路釣魚試圖竊取個人資訊。

圖 10 Gamut 僵屍網路傳送的垃圾郵件。



備註：這樣的畫面是假冒的，是由網路威脅發動者所發動，並使用它來欺騙觀看者以為這是合法的訊息。

圖 11 垃圾郵件工具組的範例。



備註：這樣的畫面是假冒的，是由網路威脅發動者所發動，並使用它來欺騙觀看者以為這是合法的訊息。

大量電子郵件工具組

許多濫發垃圾郵件者採取的另一種方法，就是購買工具組來傳送大量電子郵件。其中許多工具都是半合法的，代表如果您想銷售自己手工製作的浴簾，技術上您可以使用工具組向自己的電子報傳送大量電子郵件來提高品牌知名度。但是這類工具組的某些功能，例如循環寄件者 IP 位址和自訂附件重建以產生唯一的雜湊值，用於上述情境的機會很低。

思科 Talos 的工程師最近揭發攻擊者偽裝的 Facebook 社團，他們在上面銷售大量電子郵件工具，以及疑似透過資料外洩竊取的大量電子郵件地址清單。這些案例中購買工具的人顯然意圖不軌。

詐欺的方法

如果郵件是最常見的媒介，詐欺就是最常見的方法 – 特別是對於組織犯罪來說。

如果郵件是最常見的媒介，詐欺就是最常見的方法：特別是對於組織犯罪來說。BEC 詐騙幕後的惡意攻擊者企圖騙取公司數千美元。數位勒索者則利用不實資訊欺騙使用者支付他們比特幣。而提到預付款詐欺就更是顧名思義了。

這些都不是新手法。電子郵件只是犯罪分子用來詐欺的最新工具之一。犯罪分子在歷史上總是奮力抓住機會，利用每一代的科技盡可能賺取非法的利潤。

縱觀德國聯邦警察 (Bundeskriminalamt BKA) 和 FBI 的損失紀錄，超過 80% 的有記錄網路犯罪損失都可歸咎於詐欺行為。重點在於「有記錄的」損失，因為可能還有難以準確量化和記錄的無形損失。不過這也表示有記錄的統計資料相當可靠。

因此，詐欺確實是網路犯罪損失背後的原因。事實上，透過檢視兩種 FBI 的統計資料指出的詐欺方法，也就是商務電子郵件入侵 (BEC) 和電子郵件帳戶入侵 (EAC)，我們發現 2018 年的虧損為 13 億美元。相較之下，勒索軟體這個經常被提到和分析的網路犯罪形式，所記錄的等價損失 為 360 萬美元。事實是：每種跡象都表示尚未發現的詐欺造成的損失將繼續增加，因為與 BEC/EAC 相關的損失在 2016 年和 2017 年之間就單獨增加了 78%。

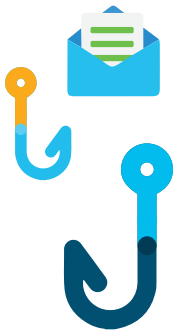
「Cisco Email Security 真的替管理階層分擔了電子郵件安全的工作，讓我們能專注於其他領域。它什麼都攔截得到！知道我們為電子郵件安全做出了最佳決定很令人安心！」

Technology Concepts & Design, Inc.
資深 IT 架構師 Steven Wujek

如需有關詐騙和網路犯罪損失的更多資訊，請參閱我們探討「網路犯罪與詐欺」的部落格系列。

「全面性的資安策略不僅只是安全性產品問題或業務需求。而是關於檢視員工、程序與橫跨整體業務的科技。在思科，我們採取以人為本的方法，專注在個人和他們執行的工作，並協助他們安全地完成工作。方法之一就是提供員工實用的技巧，讓他們在點擊前辨識並通報可疑的電子郵件。」

思科資安長 (CISO) Steve Martino



如何防範電子郵件攻擊

網路釣魚電子郵件的型態

往好的一面來看，透過電子郵件傳播的威脅通常有一些矛盾之處可供辨認，不過您得知道要找什麼。以下是幾個範例。請參閱下頁查看每個範例的詳細內容。

收件者：you@youremail.com

1 寄件者：Amazon 貨運 <amz@123fnord.com>

主旨：尼近期的訂單

您好，

2 感卸您的訂單。訂單詳細資訊如下：

商品：Puppy Food™ 每月寄送訂購方案
品牌小狗食品
每月金額：$121 美元
日期與時間：2019 年五月 3 日 10:21
IP 位址：254.189.234.159.01
購買國家：瓜地馬拉

3 若您不希望繼續訂購，請按照附件中的說明立即取消，或在此輸入您的信用卡資訊：

4

5 http://badphishingsite.com/dontgothere.html

順頌 商祺
Amazon 貨運

檔案

6 不要開啟這是.惡意檔案

備註：這樣的 Amazon 畫面是假冒的，是由網路威脅發動者所發動，並使用它來欺騙觀看者以為這是來自 Amazon 的合法標誌和訊息。

圖 12　Microsoft Office 關於已開啟文件中的巨集警告。

1. **寄件者地址**寄件者地址中的名字是否與電子郵件地址相符？
2. **許多拼字與文法錯誤或模糊的標誌。**如果電子郵件看似隨便拼湊，那可能就是不正當的。
3. **急迫感。**如果電子郵件要求您立即採取行動，或語氣有急迫感或想激起您的好奇心：請抱持懷疑態度。
4. **要求個人或敏感資訊。**切勿回覆不請自來且詢問您個人、財務或敏感資訊的電子郵件。
5. **看似不正當的 URL。**許多網路釣魚電子郵件 URL 只要經過仔細檢查看起來都很不尋常，就不應點擊。如果 URL 隱藏在文字連結中，請在連結上方停留，並查看瀏覽器底部檢查。如有疑問，請勿點擊。
6. **無法辨識的檔案類型。**在大多數專業工作中，僅有幾種檔案類型會透過電子郵件傳送。如果檔案類型看起來很奇怪，請勿開啟。

除此之外：

- **放慢速度。**一般人在行動前會花 8-10 秒的時間快速瀏覽電子郵件。放慢速度並尋找可能表示網路釣魚的線索。
- **如果事情聽起來好得難以置信，那應該就不可輕信。**電子郵件是否提供您數百萬美元？威脅要讓您難堪或傷害您？這可能完全是捏造的。
- **密切注意警告。**如果您確實認得寄件者且開啟了附件，請密切注意關於副檔名的橫幅警告，或需要啟用的巨集 (圖 12)。巨集大多非必要。

攻擊防禦策略

您可以採取多種方法來降低電子郵件威脅造成的風險。

進行定期的網路釣魚練習。您的員工是您防範網路釣魚，尤其是對於那些最特製化的網路釣魚攻擊。學會立即辨識網路釣魚攻擊的員工可以阻止入侵終端的 #1 來源。

為了提高認知，請定期進行公司網路釣魚練習來測試和教育使用者。模擬最新的現實世界技巧，讓員工瞭解他們可能遇到的情況。思科建議每個月進行練習，從容易發現的網路釣魚測試活動開始，然後逐漸提高複雜程度。對於受騙於模仿網路釣魚攻擊的使用者，請立即提供教育（例如傳送更多有關網路釣魚進一步資訊的測試用「惡意」URL）。對於組織中的高風險使用者，如果他們陷入詭計可能會造成重大損害，請進行量身定制的網路釣魚活動練習。

使用多重要素驗證。萬一公司電子郵件帳戶認證被成功竊取，多重要素驗證可以防止攻擊者存取帳戶並造成嚴重破壞。

多重要素驗證的優點在於簡單易用。假設有人設法取得您或您網路上其他人的登入認證，並試圖登入。透過多重要素驗證，系統會自動傳送訊息給認證的所有人，以檢查他們是否試圖登入。在這個情況下，使用者一但發現他們沒有試圖登入，可以直接拒絕請求。這樣就成功地阻止了攻擊。

將軟體保持在最新狀態。在某些情況下，包含惡意 URL 的電子郵件可能將使用者引導到有漏洞攻擊的頁面。將瀏覽器、軟體及外掛程式保持在最新狀態，有助於緩解此類攻擊造成的風險。

絕不匯錢給陌生人。這也適用於預付款詐欺和 BEC 詐騙。如果您對任何要求感到一絲懷疑，請勿回應。對於 BEC，請制定嚴格政策，要求電匯前須經過公司內部高階員工授權，並指定次要簽署人。

請注意登入請求。惡意攻擊者為了竊取登入認證，會竭盡全力使他們的頁面看起來像您熟悉的登入頁面。遇到這類登入提示，請務必檢查 URL 以確保提示來自合法擁有者的網站。遇到彈出式視窗，請展開視窗以確保完整的 URL，或至少讓完整的網域清晰可見。

請確認電子郵件內容是否合理。對於像數位勒索與預付款詐欺的詐騙手法，寄件者通常會創造複雜的故事，試圖說服您郵件是正當的。敘述的情境是否合理？他們的故事是否有任何技術上、財務流程觀點或是其他方面的漏洞？如有，請抱持懷疑的眼光看待問題。

做好準備

電子郵件威脅會用很多不同方法試圖欺騙或誘使您回覆、點擊 URL 或開啟附件。因此使用可以攔截與隔離惡意電子郵件，並過濾垃圾郵件的電子郵件安全軟體有其必要性。

遺憾的是，我們發現了令人擔憂的趨勢：使用電子郵件安全性的組織比例正在減少。根據我們最新的資安長基準研究顯示，目前只有 41% 的受訪者使用電子郵件安全性作為威脅防禦的一部分，儘管研究指出這是讓組織承受風險的 #1 威脅媒介。2014 年有 56% 的組織使用電子郵件安全性服務，相比之下明顯下降。

下降的原因可能很多。移轉到雲端可能是其中之一。在 ESG 代表思科進行的一項近期研究指出，超過 80% 的受訪者回報他們的組織正在使用雲端式電子郵件服務。隨著越來越多的組織選擇將他們的電子郵件服務交由雲端託管，現場專屬的電子郵件設備似乎顯得不太必要，因為有些 IT 團隊認為他們不需要。

儘管許多雲端電子郵件服務能提供基本的安全性功能，分層式防護的重要性依然值得再次強調。事實上，在 ESG 進行的同一份調查中顯示，43% 的受訪者發現移轉到雲端後，還是需要附加的安全性防護來保護他們的電子郵件。最終，還是需要 IT 團隊來制定政策、提高能見度與取得掌控、使用沙箱以及利用外部封鎖功能。

安全團隊目前面臨的另一個問題是因為攻擊面增加，導致有更多的區域需要保護。如果資安預算沒有同時增加，團隊很可能需要減少部分資源以處理更大的攻擊面。

由於電子郵件是最常見的威脅媒介，防範未然的重要性不容低估。在執行任何網路風險評估時，重要的是將最關鍵的進入點列入優先考慮，並提供完備的防禦措施和風險管理系統，然後根據遭攻擊的可能性與遭入侵時對組織產生的風險依序往下評估。接著分配與潛在損失嚴重性相當的資源。

此外，Gartner 建議安全性與風險管理者 (SRM) 採取三管齊下的方法，來改善防範網路釣魚攻擊的防禦措施：

1. 升級安全電子郵件閘道和其他控制措施以改善對網路釣魚的保護。
2. 將員工整合到解決方案中，並培養偵測和回應可疑攻擊的能力。
3. 與業務經理合作，發展處理敏感資料和金融交易的標準作業程序。

如何保護您的電子郵件

我們已經探討網路釣魚電子郵件的型態和攻擊防禦策略。現在，讓我們看看對 2019 年電子郵件安全性技術的期望。

與過去一樣，採取分層方式確保資安，對於保護您的組織免於電子郵件型攻擊至關重要。許多禁得起考驗的電子郵件安全功能至今仍然重要。

例如：

- 仍需垃圾郵件防禦功能以阻擋不需要的郵件和惡意垃圾郵件進入收件匣。
- 電子郵件威脅防禦功能，例如封鎖惡意軟體和 URL 的功能對於封鎖附件中的惡意軟體、魚叉式網路釣魚、勒索軟體和挖礦至關重要，以及能夠對抗電子郵件中惡意連結的 URL 情報。
- 整合式沙箱技術應該自動在背景中進行，以快速瞭解電子郵件中收到的新檔案是否為惡意的。

值得強調的是威脅趨勢持續不斷演進，而惡意攻擊者始終在找尋新的途徑發動攻擊。

除了歷經考驗的措施，以下安全性技術也能協助因應瞬息萬變的趨勢：

- 更進階的網路釣魚防護已經出現，利用機器學習來瞭解和驗證電子郵件身份與行為關係以封鎖進階的網路釣魚攻擊。
- 現在可以啟用 DMARC 網域保護來保護公司的品牌，並防止攻擊者使用合法公司網域進行網路釣魚活動。
- 訊息隔離功能能夠保留訊息，在附件檔案向收件者發佈訊息、移除惡意附件或徹底移除訊息之前分析附件檔案。
- 如果收件者收到的檔案被偵測為惡意檔案，電子郵件修復能讓您從信箱中回去隔離附有惡意檔案的訊息。
- 電子郵件安全性產品現在經常使用 STIX 中的外部威脅摘要，因此組織若希望獲得原生威脅情報以外的資訊，也可以在產品中使用垂直聚焦威脅摘要。
- 具備更廣泛安全性產品組合的電子郵件安全整合也越來越常見，可用於瞭解環境中的進階惡意軟體或訊息是否已經傳送給特定使用者或收件匣。

「思科是 2019 年 Forrester Wave 企業電子郵件安全的領導者，在部署選項、攻擊防護與電子郵件驗證、效能與營運（包括擴充能力和可靠性），以及科技領導方面都榮獲最高評等。」

2019 年 第 2 季度 The Forrester Wave™：企業電子郵件安全

思科網路安全系列

綜觀過去十年，思科已經發佈許多明確的資安與威脅情報訊息，提供給對於全球網路安全領域感興趣的專業人士。這些內容充實的報告對於威脅趨勢及其組織性影響提供了詳細的陳述，同時還提供最佳做法以抵銷資料外洩所產生的不良影響。

思科資安在思維領導方面採用全新做法，就是在思科網路安全系列的橫幅下方，發布一系列以研究為基礎之資料導向出版物。我們增加了標題數量，以便為具有不同興趣的資安專業人士納入不同的報告。號召具有深入且廣泛專業知識的威脅研究人員與資安產業創新人員共襄盛舉，2019 年度系列的報告集合內容包含資料隱私權基準研究、威脅報告與思科基準研究，而且終年都會推出其他豐富內容。

如需詳細資訊、存取所有報告及封存副本，請造訪 www.cisco.com/go/securityreports。

美國總部
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
新加坡

歐洲總部
Cisco Systems International BV
荷蘭阿姆斯特丹

思科在全球各地擁有超過 200 間分公司。各分公司地址、電話及傳真號碼皆列於思科網站上，網址為 www.cisco.com/go/offices。

2019 年 6 月出版 THRT_02_0519_r1