No.: 1-23025-11
出版日期:2023/05/01 v.1

凱舟濾材—數位技術防堵 BEC 詐騙[1]

張敏華　黃子佳　戴佑真[2]

在 2019 年 4 月，凱舟與義大利客戶 Martech 公司在一場交易中，被駭客設局。凱舟員工 Maria 電子郵件遭入侵後，犯罪者註冊多個極為相似的電子郵件地址以假亂真，竄改通訊內容等方式，導致 7 萬歐元的貨款被騙走。

壹、淨水濾材的模範生成為肥羊

凱舟濾材網站、社群 (FB/LinkedIn)、國內外媒體報導皆可搜尋，總經理 Carren 於 2006 年創辦「Caware」品牌行銷全球，致力於製造優質淨水濾材與設備，以滿足世界各地不同水質。2011 年以中東市場的家用飲水為起點，接而從貿易轉向產線建置，也廣布綠能、商業、工業，近年轉以生技醫材專攻歐美市場做為公司第二曲線。

凱舟是一間典型的中小企業，數十年來，以高品質的濾芯研發，提供客戶解決方案。組織現逾七十名同仁，背景領域不乏醫管、材料、工管的博碩士。即便凱舟內部皆是高知識、高學歷的專業人才，銷售經驗遍及六十余國，在高度仰賴資訊科技作為溝通管道，卻從未編列資安預算。每年資安投資不到台幣 5 萬，資安漏洞像蝴蝶效應凸顯一連串的管理破口，造成客戶財損、不信任，員工驚嚇出走、責任推諉、產線出貨收款流程大亂，可謂是成也數位，敗也數位，數位變革勢在必行。

本篇個案角色介紹：

Carren 凱舟濾材總經理，負責公司營運與治理。

Tina 凱舟濾材財務部主管，負責應收帳款對帳及核對。

光華管理個案收錄庫（KMCC）
個案試閱版
http://www.kmcc.org.tw
請勿摘錄已用

---

[1] 本個案摘錄自《中山管理評論》第 31 卷第 1 期，P.171~200，原題目為「凱舟濾材-中小企業透過數位技術防堵 BEC 詐騙」，著作財產權屬於財團法人光華管理策進基金會所有。

[2] 作者張敏華為國立中山大學企業管理學系 DBA 博士生、凱舟濾材股份有限公司創辦人；黃子佳為國立中山大學企業管理學系博士候選人；戴佑真為國立中山大學行銷傳播管理所碩士。

* 本收錄庫所收錄/出版之個案與配套教材，包括文字、照片、影像、插圖、錄音、影音片或其他任何形式之素材等，均由作者獨家授權光華管理策進基金會出版，受到中華民國著作權法及國際著作權法律的保障。所有個案或配套教材的全部或部分內容都不能被複製、影印、掃描、儲存、電子傳輸、分享或公告於任何網站。

** 本收錄庫所發行之個案均為紙本套朱紅色印刷，如發現盜印或任何侵害作者智慧財產權之行為，歡迎備證來信檢舉，電子郵件：kmcccase@gmail.com，查證屬實者，備有獎金酬謝。

***如需訂購光華管理個案收錄庫之個案，歡迎上網查詢。網站位址：http://www.kmcc.org.tw/。

Judy 凱舟濾材業務處主管，綜理客戶服務事項/代理各業務員。

Maria 凱舟濾材業務處經理，處理客戶訂單/出貨/款項追蹤。

Kyle 凱舟濾材業務處經理，同 Maria。

Stanley 凱舟濾材之總管理處經營管理專員，擬訂及執行內部管理辦法、流程制訂/稽核事項。

Yale 凱舟濾材總管理處資訊管理專員，維持內部資訊服務、資訊設備硬體等運作。

Marta 凱舟濾材的客戶，Martech srl 業務經理。Martech srl 主要經營家用電器零配件與耗材買賣。總部位於義大利，以自有品牌「Martech」行銷全歐洲，員工數約莫十人。客戶包含家電經銷商、區域批發商至鄉鎮零售商，其供應商遍集全球，凱舟為其濾芯耗材 ODM[3]代工廠。

莊顧問 凱舟濾材委外資安顧問，協助資訊方案提案建議/遠程資安事項監控/異常狀況查核。

光華管理個案收錄庫（KMCC）
個案試閱版
http://www.kmcc.org.tw
請勿摘錄引用

圖1　凱舟個案人物之間的關係

資料來源：本研究整理

貳、悄悄駭入的不速之客

事情是這樣發生的…，2018 年 10 月 Maria 收到 Microsoft 寄來的電子郵件，說目前的版本需要更新應用程式，於是便點選連結，在頁面上以信箱帳號及密碼登入並安裝。

[3] Original Design Manufacturer「原廠委託設計」從客制化產品設計到生產完成後，交給品牌公司貼他們的 LOGO 出售。

首部曲、電子郵件頻遭退信

2019 年 4 月 8 日，凱舟負責船務同仁，正在準備 10 日要出貨給義大利客戶 Marta (個案人物說明如圖 1)，是價值 7 萬歐元的客制化濾芯訂單。以電子郵件傳送提單[4]給相關同仁時，就會收到業務 Maria 的退信通知。之前，船務同仁還提醒 Maria，問她是不是 Webmail 信箱滿了，請她清理一下垃圾郵件跟廣告信，不然郵件常被退回來。Maria 跟部分凱舟同仁習慣回到家，透過自己的筆電或手機以 Webmail 接收公司的郵件。Maria 在公司用 Outlook 準備寄提單、出貨付款通知給義大利客戶 Marta，同時 cc[5]給其他相關同仁照會時，也會收到退信通知，感覺怪怪的。於是，請負責 IT 的 Yale 來檢查一下郵件伺服器設定。Yale 看完雖覺得無異狀，但也為求安全起見，順便用卡巴斯基防病毒軟體進行掃毒，偵測後並無病毒感染，隨後請 Maria 持續關注，並回報是否還有異常發生。

殊不知此時在看不見的角落，駭客早已虎視眈眈，埋伏監看凱舟與客戶往來的郵件內容。退信問題持續了一周，狀況仍未改善，因此 Yale 打電話問 ISP 業者中華電信，他們提供凱舟 hiBox 企業全能信箱服務，有郵件雙重過濾防護機制，以及專屬、多語系使用管理介面。電信專員建議檢查公司郵件 Webmail 端設定，Yale 進入後臺時發現，Webmail 介面變成簡體中文，而轉信機制也被開啟，且使用許久，Yale 心想可能一開始便是如此，應不屬於特殊異狀。

光華管理個案收錄庫（KMCC）
個案試閱版
http://www.kmcc.org.tw
請勿摘錄已用

二部曲、駭客出手電子郵件交叉發信

監看凱舟郵件已久的駭客眼見時機成熟，準備出手了…。4 月 12 日，登入 Maria 的 Webmail，假借 Maria 名義發信告知義大利客戶 Marta 表示：因為公司兆豐國際商業銀行的帳號，目前稽核中，無法收款，當您要安排匯款時，敬請告知，屆時我們會提供正確的收款銀行帳號。

Marta 不疑有他，回信給 Maria 表示：感謝告知，請提供新的匯款帳號等相關訊息。此時 Marta 是直接「回覆所有人」郵件，殊不知 cc 給凱舟同仁信箱全是假的，但顯示名稱皆相同 (如表 1)，只有 Maria 電子郵件地址不曾被竄改，但駭客早在 Maria 收信前即已轉走郵件。收到信的駭客隨即在西班牙開立新銀行帳戶，並回信給 Marta，信中附上凱舟濾材公司英文名稱、新銀行帳號 IBAN 與 SWIFT CODE 等，並且叮囑 Marta：請確認銀行訊息，需按照指示安排付款，以避免收款時，出現任何問題。

---

[4] 提單（B/L）是對外貿易中托運人運輸貨物的憑證，具有法律效益。證明承運人已收到提單上注明的貨物數量和狀況，便於托運人與收貨人之間的付款，提單也是貨物所有權和交換的憑證，僅在收貨人出示原始提單（B/L）時才會放行這些貨物。

[5] CC 是 carbon copy 的縮寫，副本的意思。寄送郵件給主要收件者時，也同時傳送副本給其他相關人，例如直屬上司、內部其他部門、或者外部協辦人員，同步追蹤進度。