Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-22-001

Openfind 郵件安全威脅與潛在資安風險通報

Openfind 專注於郵件安全領域已經有 20 年以上的豐富經驗，致力提供客戶穩定、安全、可靠的郵件安全系統與服務。為提昇客戶郵件安全意識與避免潛在資安風險擴大，Openfind 郵件安全研究團隊將不定期提供客戶有關郵件安全威脅的即時訊息，以及潛在資安風險的警示通報。

如果您在使用 Openfind 各項產品時，有發現任何郵件安全威脅或潛在資安風險，也歡迎您透過 support@openfind.com.tw 與我們聯繫。Openfind 技術團隊將提供您即時的資安諮詢與更新服務。

公告日期：2022 / 03 / 16

威脅類別：Emotet 加密病毒信

威脅程度：0 (分數 1~5，5 代表資安事件威脅程度很高)

影響產品版本：Openfind 全產品皆不受影響

事件摘要：

近日，Openfind 資安團隊觀察到了一波 Emotet 加密病毒信攻擊。攻擊手法是將帶有惡意巨集的 Office 檔案，打包成 ZIP 加密壓縮檔，並在內文附上密碼，誘導使用者開啟。由於附檔被 ZIP 加密，防毒引擎無法掃描內容，攻擊者可藉此繞過檢查機制。將 ZIP 加密檔解開後，可發現內含副檔名為 .xlsm 的 Excel 檔，該檔案內含舊版 Excel 4.0 巨集。啟用巨集後，它會下載兩個階段的 PowerShell 以執行惡意程式。

面對 Emotet 病毒猛烈的攻擊，Openfind 資安團隊建議 Mail2000 用戶可導入內嵌式 Sophos 防毒引擎加強防護。Sophos 防毒引擎內含靜態程式碼分析及人工智慧比對技術，可主動偵測 Office 文件內惡意巨集、攻擊腳本（Shell）及 Windows 執行檔等。而針對 Emotet 加密病毒信，可採用 MailGates 解決方案，將 ZIP 加密附檔留置隔離區或將信件標題、內文加上警語，提醒使用者勿輕易開啟來源不明的加密檔，以確保企業組織安全。

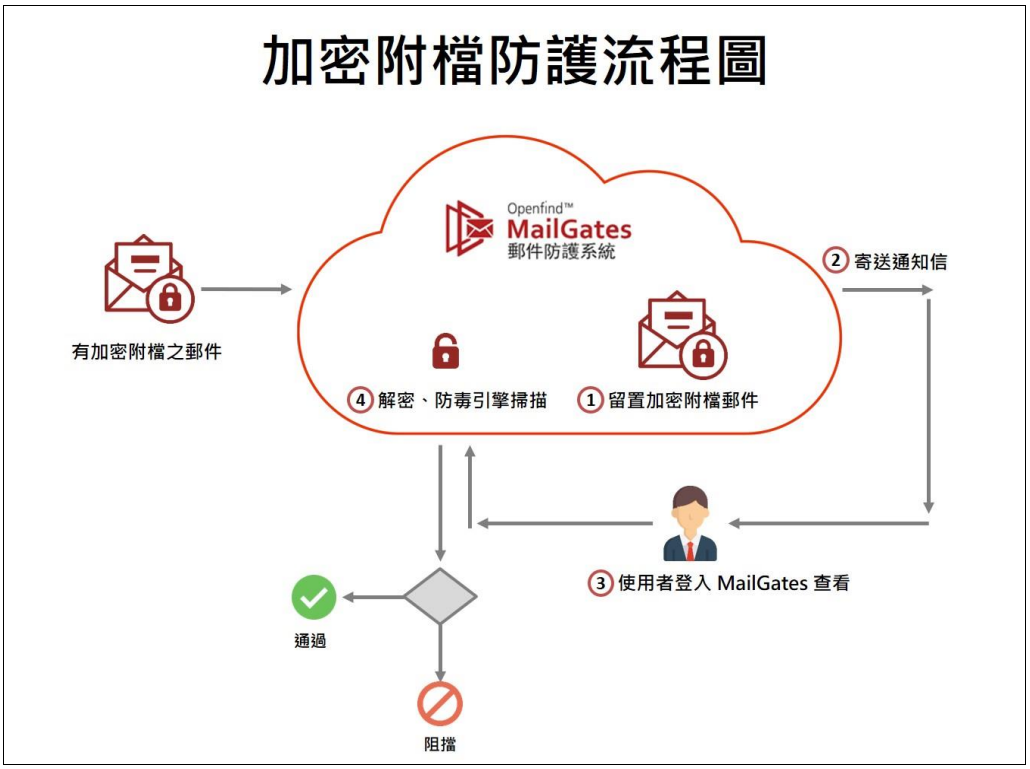
建議措施：

1. 升級到 MailGates 5.2.10 標準版，啟用「加密附檔政策」，設定步驟如下：
   - 切換至管理者模式，點選「威脅管理 > 威脅政策 > 加密附檔」。
   - 選取「啟用」，附檔大小建議值設定為「< 100 KB」。
   - 設定處理動作：選取「留置系統加密附檔隔離區」，小於 100KB 的 ZIP 加密信會被留置隔離區。
   - 設定例外動作：若 ZIP 加密信大於 100KB，可設定信件標題/內文警語提醒收件者。
2. 停用 Microsoft Office 巨集（包含 Word、Excel 及 PowerPoint）。

【圖 1. 加密附檔設定】

MailGates 加密附檔防護流程：

1. 管理者制定加密附檔政策，系統若偵測到加密附檔，就會將該信件留置於隔離區。
2. 若有信件被留置在隔離區，MailGates 系統將發送隔離通知信給使用者。
3. 使用者點擊通知信連結登入隔離區，可檢視信件內容，並輸入密碼解壓縮。
4. 如果解壓縮成功，防毒引擎會即時掃描壓縮檔內所有檔案是否安全。



【圖 2. 加密附檔流程圖】

關於 Openfind 電子郵件威脅實驗室

隨著資訊安全威脅日益升高，所有資訊系統都面臨相當嚴峻的挑戰。其中，電子郵件系統更是諸多資安威脅中首當其衝的主要標的。由於資訊安全的範圍相當廣泛與多元，在實際的案例中，客戶只需要定期更新 Patch 與升級系統，結合 Openfind 主動式安全偵測服務，便可避免暴露於風險之中。Openfind 本著服務客戶的精神，不但會繼續強化產品在資安上的防護與感知能力，也會持續嚴格監控產品的安全。Openfind 電子郵件威脅實驗室也會不定期更新網路上重大的電子郵件安全威脅訊息，幫助管理者掌握最新的資安趨勢與脈動。