知已知彼！深入剖析疫情衝擊下的資安威脅及攻擊手法

全球新冠肺炎疫情仍未趨緩，儘管台灣防疫成效看似較佳，但仍可發現到許多企業方針逐步向數位辦公、遠距辦公靠攏。在這樣的情況下，企業該如何在疫情與資安雙重風險的威脅下，達到危機應變與永續營運的目標。網擎資訊整理了全球與台灣本土的企業資安威脅趨勢與大數據分析，提供企業在後疫情時代守護資訊安全的建議。

關鍵字：新冠疫情、企業資安、郵件威脅防護

作者：張峰銘

目次

前言

根據 Gartner 在 2020 年發布的《Remote Work After COVID-19》報告顯示，在疫情爆發之前，約有 30% 企業員工曾有過遠端工作的經驗，而在疫情爆發之後，至少有 48% 企業員工透過遠端的方式工作。對大部分企業而言，郵件系統是組織成員最倚重的溝通工具，可視為企業運營中最重要的基礎建設。在疫情驅動之下，加速了企業將工作平台轉移到雲端的速度。因此，雲端郵件防護也顯得格外重要。OSecure 資安研究團隊將 2020 年 7 月-12 月期間，在企業用戶環境中實際觀察到的威脅攻擊，加以統計歸納，整理出 OSecure 資安威脅報告書提供讀者作參考，本報告可分為三個部分：

1. 威脅信件來源統計與類型
2. 郵件攻擊手法解析
3. OSecure 進階威脅防護實測報告

期望您在閱讀本報告之後，能了解新的攻擊手法並建立正確的資安防護觀念。

OSecure 郵件威脅報告

OSecure 資安威脅報告說明

日期區間：2020/07/01-2020/12/31

資料來源：OSecure 郵件安全防護服務

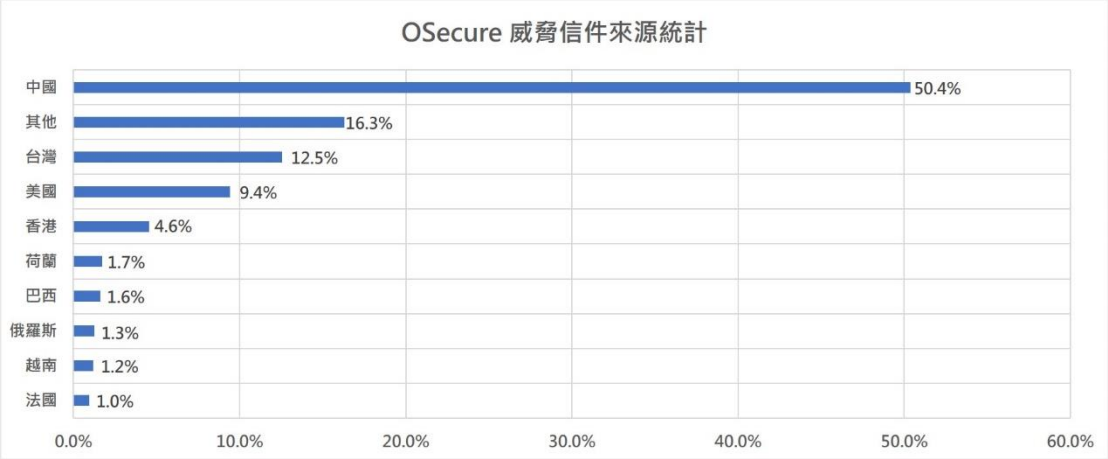
組織規模：200-2000 人之企業用戶

後端郵件服務：Microsoft 365、G-Suite 及 MailCloud 等企業郵件信箱

取樣方法：隨機抽樣 200 個網域，共 350 萬封中高風險等級信件，將信件欄位去識別化統計，包含垃圾信（Spam）、釣魚信（Phishing）、BEC 詐騙信（BEC Scam）、病毒信（Malware）以及 APT 進階威脅攻擊（Advanced Persistent Threat）等信件。

1. 威脅信件來源常跨國變動，需透過全球情資網路完整防護

威脅信件定義：經 OSecure 威脅情資判定為釣魚信、勒索信、詐騙信及垃圾信，此統計數據不含 RBL、SPF 及 DMARC 驗證失敗等信件。



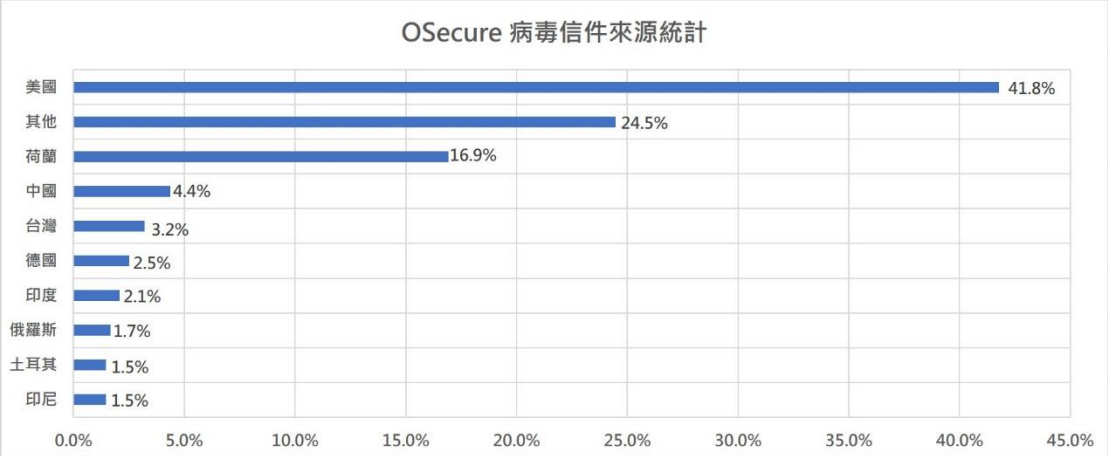
【圖 1. 威脅信件來源統計，N=2,732,445】

自 2020 年 7 月到 12 月期間，從 273 萬封威脅信件之 IP 位址反查來源國家，得到圖 1 統計表。由圖 1 可得知威脅攻擊來源前 5 名依序是中國（50.4%）、台

灣（12.5%）、美國（9.4%）、香港（4.6%）及荷蘭（1.7%）等地區。OSecure 威脅情資中心也觀察到，相同內容的釣魚信攻擊，經過 2-3 天左右，會跳轉到不同地區 IP 位址或雲端服務發送，例如：9 月 1 日偵測到從美國 IP 位址發送的釣魚信件，到了 9 月 3 日攔截到相同內容的信件，但發信的 IP 位址卻從美國變成荷蘭。由此可證實網路攻擊是跨國性的，需掌握全球威脅情資才能完整防護。OSecure 郵件防護服務整合 Cyren RPD（Recurrent Pattern Detection）技術與全球最大的 Cyren GlobalView 網路系統，佈署超過 50 萬個威脅情資誘捕系統（honeypot），可於第一時間偵測最新的惡意來源 IP、釣魚網址及大量散布的病毒攻擊，有效阻擋威脅郵件。

2. 網路罪犯用免費信箱寄送病毒信，造成安全破口

病毒信定義：經 OSecure 進階威脅防護引擎判定，內含高風險附檔之信件，例如：帶有惡意巨集之 Office 文件、內含病毒或 Trojan 木馬程式之壓縮檔等。

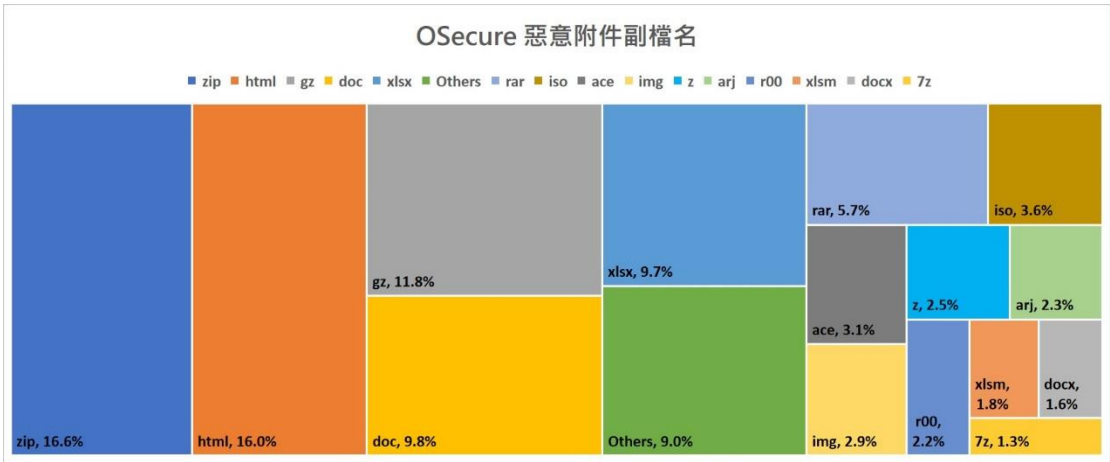


【圖 2. 病毒信件來源統計，N=302,599】

自 2020 年 7 月到 12 月期間，從 30 萬封病毒信之 IP 位址反查來源國家，產出圖 2 統計表。由圖 2 可得知病毒信攻擊來源前 5 名依序是美國（41.8%）、荷蘭（16.9%）、中國（4.4%）、台灣（3.2%）及德國（2.5%）等地區。來自美國的病毒信攻擊佔了將近 4 成，其主因在於網路罪犯利用 Yahoo 及 Outlook 等免費信箱，寄送惡意附檔。攻擊者可透過自動化工具在短時間內註冊大量帳號，進而發動攻擊。這些免費服務為了方便使用者寄送信件，未針對內寄外（Outbound）

信件制定嚴謹的防護政策，只有基於特徵值的（Signature-based）防毒掃描機制。如果帳號密碼被盜，信箱被當成散布惡意程式的跳板，就可能危及往來的商業合作夥伴，進而造成郵件安全的破口。建議企業用戶導入信箱服務時，必須導入第三方郵件安全閘道（Secure Email Gateways），除了要同時檢查接收與外寄的新信外，還須具備動態沙箱分析（Sandbox Analysis）等 APT（Advanced Threat Persistent）防護功能，才能保護企業自身與合作夥伴的安全。

3. 惡意附檔約一半為 zip 等壓縮檔格式，試圖規避偵測

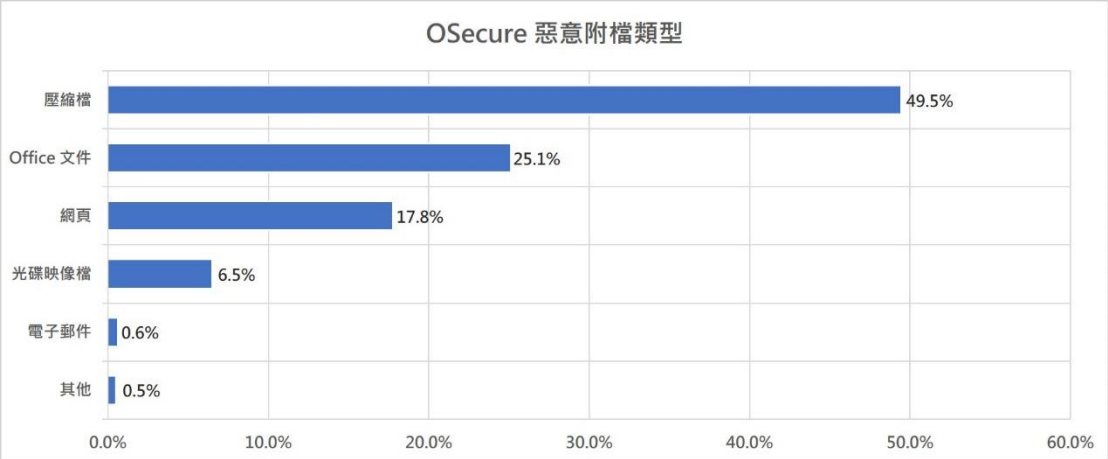


【圖 3. 惡意附件副檔名，N=302,599】

將 30 萬封病毒信樣本附件抽出，並統計惡意附件之副檔名（File Extension）得到圖 3 統計表。由圖 3 可得知，副檔名數量的前 5 名，依序為 zip（16.6%）、html（16.0%）、gz（11.8%）、doc（9.8%）及 xlsx（9.7%）等。若依下表分類統計，則可獲得圖 4 之分類統計表，前 5 類依序為：壓縮檔（49.5%）、Office 文件（25.1%）、html 網頁（17.8%）、光碟映像檔（6.5%）及電子郵件（0.6%）。

類型	副檔名
壓縮檔	7z, ace, arj, bz, cab, gz, jar, lha, lzh, r00, r01, rar, tar, tbz2, uu, zip
Office 文件	doc, docx, docm, ppt, pptx, pps, ppsx rtf, xls, xlsx, xlam, xlsm
網頁格式	htm, html, shtm

類型	副檔名
光碟映像檔	img, iso
電子郵件	Eml



【圖 4. 惡意附檔類型，N=302,599】

最常見的是以變造副檔名的攻擊方式，例如將 html 網頁偽造成 doc 文件、將病毒檔用 zip、7z 等不同格式壓縮多次，藉以規避防毒引擎檢查。專業的郵件安全閘道，如 OSecure 郵件防護服務，內建 TFT（True Format Type）技術，除了可精準判定副檔名稱，防止偽造副檔名攻擊之外一旦系統偵測到壓縮檔，會將檔案自動解壓縮並加以分析，檢查是否有惡意檔案，不會錯漏此類風險。

2020 年郵件攻擊手法解析

上一段是分析 OSecure 所防護之 Microsoft 365 等雲端郵件信箱在半年內共 350 萬封惡意信件的統計，本節則提出其中常見、經典的攻擊手法加以解析，希望有助於讀者了解威脅來源，知彼知己後更能教育使用者防範未然：

1. 盜取 HiNet 信箱由官方主機發出釣魚信

【圖 5.來自 HiNet 服務之釣魚信】

偽造通知信是常見的攻擊手法之一，舉凡密碼過期、授權不足或郵件空間已滿等通知信都可能是詐騙攻擊的前奏。一般而言，要分辨通知信的真假，會比對寄件者網域是否與通知信內容一致，如果不同就有極高的機率是偽造信。然而，如果釣魚信的寄件網域與通知信一樣時，就幾乎真假難辨。圖 5 是 MailCloud 防詐騙智慧分析中心收到的回報信件，郵件內文宣稱是來自 HiNet 的通知信。經分析後發現，該信件有通過 SPF 驗證，確實是從 HiNet 主機寄出的信件，信件內容也幾乎與 HiNet 官方通知信一致，唯一不同的是，當收件者點擊連結後會跳轉到釣魚網站頁面，由於網址是隱藏在信件原始碼中並未直接顯示，若使用者沒

有看出目的網址並非 HiNet，在以假亂真的釣魚網站誘騙下，就可能輸入帳密、將寶貴的個資拱手送出。此為帳號接管攻擊（Account Takeover Attack），研判駭客是先盜取 HiNet 的信箱帳密後，精心編撰專屬於 HiNet 用戶的釣魚信件，再透過官方主機發送，如此就可躲過偽造寄件人等檢查機制，若不仔細觀察隱藏的外連的網址，十分容易上當受騙。

2. 連往釣魚網站的圖片偽裝成附檔掩人耳目

【圖 6. 偽裝成 PDF 附檔的圖片】

近年來資安意識提升，無論是政府單位或企業組織，都不斷地加強宣導資安觀念，教育使用者不要點擊未知信件中的附檔與 URL 連結。如果信件已被防毒軟體掃描過，相信大部分的使用者就會放心地開啟附檔，而網路罪犯為了誘導使用者點擊，可說是無所不用其極。圖 6 是一封來自日本企業的商務信件，乍看之下會以為信件附加一個 PDF 檔，但實際上是帶有 URL 連結的圖片，使用者點擊後，會跳轉到類似 Microsoft 365 的登入頁，藉以騙取帳號密碼。

圖 7 也是利用相同的手法，攻擊者將 Excel 圖片附加在信件底部，讓使用者誤以為是 Excel 文件，一旦使用者點擊，就會跳轉到釣魚網站。此類攻擊主要利用「信件其實沒有惡意附檔」可被偵測的特點，以圖片偽裝成檔案誘使點擊，再配合偽裝為知名服務的釣魚網站，需要使用者警覺連往的網站與各大服務的真正網址不同，才能避免受騙上當。此外，該信件的標題還特別編撰為「Re: new Order」，企圖讓收件者認為是一封曾經往來的信，藉以降低其戒心。

【圖 7. 偽裝成 Excel 附檔的圖片】

3. 免費雲端儲存空間被濫用，成為檢查機制死角

【圖 8. 利用 OneDrive 繞過檢查機制】

攻擊者為了躲避各種郵件安全檢查機制，有時會將病毒檔放置在 Dropbox 或 OneDrive 等雲端服務，因這些免費雲端儲存空間容易取得，且通常只有簡易的防毒掃描，可能無法偵測到最新型的惡意程式，一旦防毒引擎沒掃描到，攻擊者就可建立分享 URL 連結，再透過電子郵件廣為發布，因為在正常的情況之下，沒有任何一家郵件安全廠商，會將 OneDrive 與 Dropbox 等網域的連結設為黑名單。圖 8 是由 OSecure 用戶回報的信件，信件內容看起來像正常的訂單，然而信件中的 PDF 檔實際上是圖片，點擊後會直接從 OneDrive 雲端服務下載病毒檔。此類手法必須依靠各大雲端儲存空間更積極偵測之外，郵件防護系統及端點防毒，都有機會透過 APT 等進階防禦機制攔阻這類刁鑽的攻擊。

4. 植入木馬病毒的 Office 文件，典型卻依然橫行

【圖 9. 內含 Trojan 木馬程式的商務信件】

圖 9 是非常典型的病毒信樣板。首先，攻擊者利用信件標題誤導收件者為往來信件，並於信件內文請收件者確認訂單或匯款資訊，進一步誘導收件者點擊附檔。附檔內含 Trojan 木馬程式的 Office 文件，一旦使用者開啟 Office 文件就會被植入後門程式。這類病毒信之所以成為經典樣板，主因在於一般使用者認為 Office 檔案只能拿來處理文書，因而掉以輕心。實際上 Office 文件除了文書處理之外，還可編寫巨集，執行複雜的指令。唯有每一位使用者建立正確的資安觀念，才能真正降低整體資安風險。

5. 將病毒檔包入加密壓縮檔，以繞過檢查機制

【圖 10. 加密病毒信】

圖 10 是在 2020 年 10 月期間，MailCloud 防詐騙智慧分析中心收到用戶回報的病毒信件，雖然這封信的顯示名稱（Display Name）是電子郵件地址「wanghw@sinolines.com」，但是比對寄件者欄位（Mail-From）卻是「vanzari2@citgrup.ro」，是顯示名稱詐騙的特徵，透過 BEC 郵件安全政策可偵測到此異常部分。而進一步分析可發現，攻擊者為了繞過防毒引擎檢查，將病毒打包成 zip 壓縮檔、刻意以加密保護，並在信件內文附上解壓縮的密碼。如果收件者依指示輸入密碼解壓縮附檔，將會出現一個 doc 類型的病毒檔。這類的加密病毒信在日本地區很常見，壓縮檔格式大部分是 zip，少部分會有 7z 或 rar 等類型。雖然此類攻擊需要使用者手動輸入密碼、解壓縮並點開其中檔案才會受害，但在信件內容經過社交工程設計後，情境及用語若十分符合，就如同各種常見詐騙案例，仍然可能會誘騙成功、讓被害人完成許多步驟而後遭植入病毒詐騙。

OSecure 如何協助企業免於郵件攻擊

Openfind Secure（OSecure）雲端資安服務聚焦在智慧溝通、資安防護及雲端安全等三大方向，提供多雲、混合雲的智慧服務，並整合 Cyren 及 Sophos 等資安國際大廠之核心技術，提供多重防護機制，保護企業免於郵件威脅，以下介紹 OSecure 企業用戶之實際測試數據，比較各項防禦效果供佐證參考。

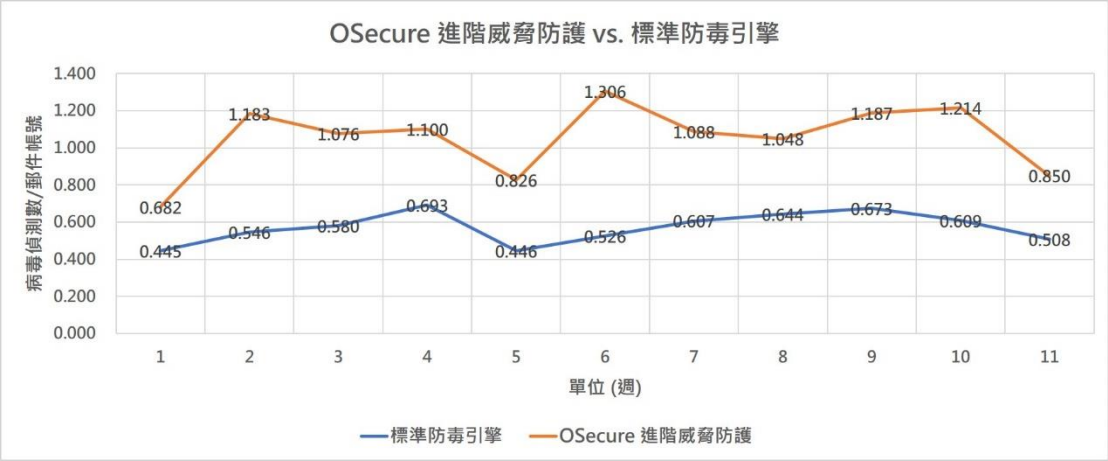
1. OSecure 進階威脅防護與標準防毒引擎之比較

為了驗證 OSecure 進階威脅防護與標準防毒引擎的差異，我們邀請 MailCloud 企業客戶試用 OSecure 進階威脅防護服務，測試說明如下：

測試區間：9 月-11 月，共 11 週。

偵測數量：共偵測到 713,142 封病毒信。

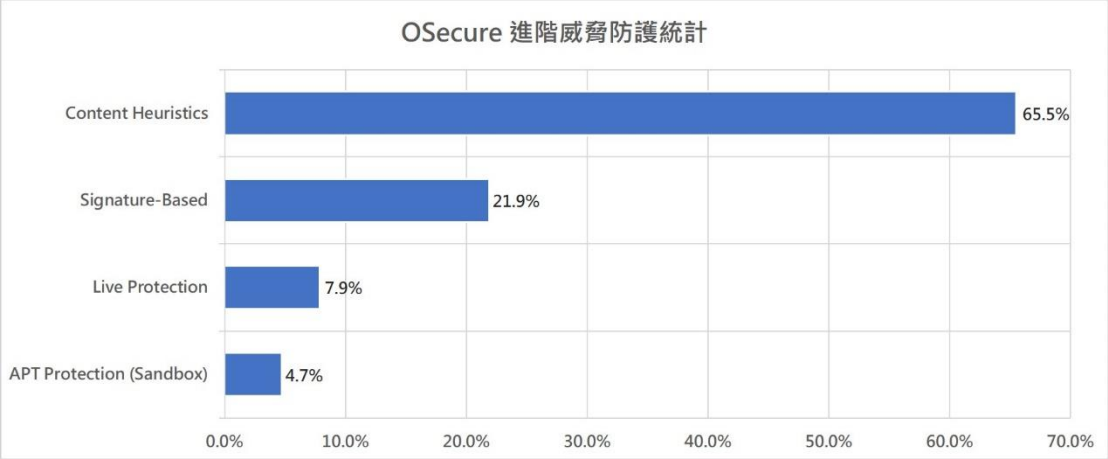
方法說明：將 MailCloud 企業用戶之信件附檔抽出、去識別化，串接 OSecure 進階威脅防護機制判讀，並與標準防毒引擎比較偵測率，為了避免因企業組織規模大小造成的誤差，我們將偵測的病毒信數量正規化：將同一企業收到的病毒信總量均分給所有帳號，呈現各企業平均單一帳號每一週偵測到的病毒信量，結果如圖 11 所示。



【圖 11. OSecure 進階威脅防護 v.s. 標準防毒引擎，N=713,142】

由圖 11 可得知，在測試期間 OSecure 進階威脅防護的偵測率，是標準防毒軟體的 1.5 至 2.4 倍，而在第 6 週時 OSecure 進階威脅防護的偵測率甚至高達 2.48 倍，攔截效果十分顯著。由以上測試結果，可觀察到病毒變種速度非常的快，如果只採用標準防毒軟體，很可能無法阻擋新型病毒的攻擊，建議企業用戶可導入進階郵件防護服務，打造完善的郵件防禦體系。

2. OSecure 進階威脅防護統計



【圖 12. OSecure 進階威脅防護統計】

此外，我們將不同的偵測機制分別統計，在圖 12 可觀察到 OSecure 於 2020 年 9 月至 11 月間約 71.3 萬封惡意信件是由何種過濾機制攔截：進階內容防護（Content Heuristics）（65.5%）、特徵值防護（Signature-Based）（21.9%）、雲端即時防護（Live Protection）（7.9%）以及沙箱分析（Sandbox Analysis）（4.7%），下表說明各偵測機制之運作原理。

編號	偵測機制	功能說明	比例
1	Signature-based 特徵值防護	比對病毒資料庫中已知惡意程式特徵值。	21.9%
2	Content Heuristics 進階內容防護	透過 TFT（True File Type）技術偵測檔案類型、結合大量機器學習模型與靜態程式碼分析技術，可於短時間內判定威脅檔案。	65.5%

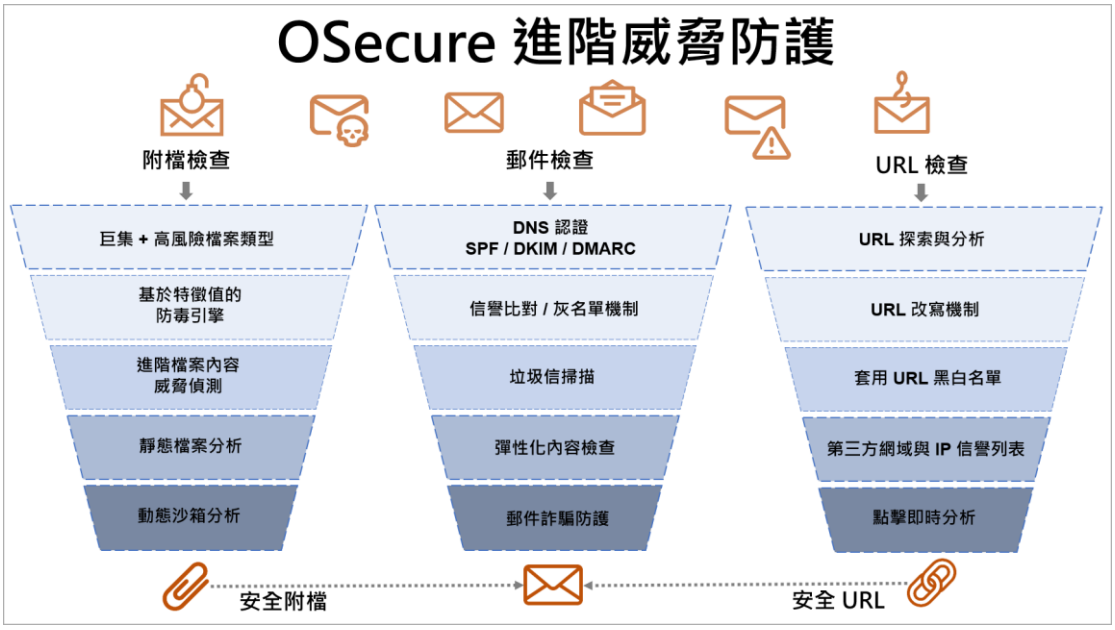
編號	偵測機制	功能說明	比例
3	Live Protection 雲端即時防護	即時比對 OSecure 雲端病毒資料庫中可疑檔案特徵值。	7.9%
4	Sandbox Analysis 動態沙箱分析	將檔案提交至沙箱（Sandbox）環境引爆，透過全系統模擬（Full-system Emulation）技術可阻擋零時差攻擊（Zero-Day）、勒索病毒（Ransomware）及未知惡意程式。	4.7%

由上表可知，進階內容防護結合大量機器學習模型與靜態程式碼分析技術能夠有效判定未知的威脅檔案。反之，若缺乏進階技術保護使用者之信箱，會有大量快速變形的惡意內容，造成許多資安風險。

結語

導入第三方郵件防護服務，是建立雲端工作平台的第一步

企業如果採用雲端郵件服務，IT 人員需思考如何確保電子郵件安全性與彈性。雖然許多大型的雲端郵件服務，例如 Microsoft 365 提供了垃圾郵件過濾（Spam Filtering）與基於特徵值的（Signature-based）病毒防護等功能，但這些基礎的防護機制，並未能保護企業用戶免於針對性攻擊威脅。因此，以進階威脅防護加強電子郵件安全應是 2021 年後企業資安防護首要任務。建議企業可評估導入專業之第三方防護服務，攔阻 APT 及勒索病毒或詐騙等威脅，改善工作平台之安全性。



【圖 13. OSecure 進階威脅防護】

關於 OSecure 進階威脅防護

- 整合 Cyren RPD（Recurrent Pattern Detection）技術（美國專利技術 U.S. Patent #6,330,590），與 Cyren GlobalView 威脅情資網路系統，在全球佈署超過 50 萬個威脅情資收集據點。

- 即時查詢全球威脅情資（Threat Intelligence），包含 IP 位址、URL 連結、圖片、附檔、內文樣式（Body Pattern）與郵件指紋（Email Fingerprint）。
- 整合 SophosLab 實驗最新病毒偵測技術及動態沙箱分析系統，有效阻擋未知惡意程式及零時差攻擊。
- 整合 MailCloud 防詐騙智慧分析中心情資，每天分析大量釣魚 URLs 連結及中文語系詐騙信件。

Reference

[1] Gartner – Remote Work After COVID-19

[2] Sophos 2021 Threat Report

如有任何問題或需要更進一步的資訊，歡迎與我們聯絡

網擎資訊軟體股份有限公司

Openfind Information Technology, Inc.

地址：10359 台北市大同區重慶北路二段 243 號 7 樓

網站：https://www.openfind.com.tw/

聯絡信箱：info@openfind.com.tw

聯絡電話：(02)2553-2000 分機 716 許小姐