Trend Micro
Research

重新調整作法

2022 年度網路資安報告

內容

網路犯罪集團導入企業經營手法 04

存取權限對駭客至關重要..... 06

受攻擊面正在擴大且修補更新屢屢失效..... 08

發掘藏匿在雲端的弱點..... 14

網路攻擊對業務的衝擊..... 18

應對戰術日益靈活的駭客的防範策略..... 20

威脅情勢..... 21

出版者：
Trend Micro Research

圖片授權：Shutterstock.com

2022 年是政治衝突激烈及經濟不穩定的一年，烏克蘭境內的戰爭以及該衝突所衍生的事件日益升高，在全球造成震盪。許多政府機關、大型企業、甚至是小型企業都面臨了供應鏈中斷、關鍵跨國產業受挫，以及經濟上的衝擊。在這不穩定的大環境下，網路犯罪集團也如同許多企業一樣，試圖重新調整作法以求生存。在去年的資安報告中，我們說明了駭客集團如何為了因應現代化企業資安防護，轉而攻擊更有利可圖的目標，努力開發新的方法來駭入受害者的網路。

以下各節，我們將說明網路犯罪集團採用了哪些企業經營手法以便在營收持續下滑的情況下繼續維持營運。我們將特別深入勒索病毒集團，探討現代化集團在形象經營與企業方案方面如何效法合法企業。

此外，我們也檢視了當前的漏洞情勢，尤其是駭客在 2022 年如何駭入網路。 我們發現存取權限至關重要，不論是哪種類型的駭客，都必須先取得進入受害者網路的存取權限。駭客集團會互相學習，而且經常會採取同樣的動作，只不過最終目的不同而已。2022 年資安界的一件大事就是 Microsoft 決定封鎖 Office 文件中的巨集，禁止巨集執行。我們檢視了這項決定對駭客突破企業防線的手法有何影響，以及犯罪集團如何加以因應。

呼應我們去年發布的 2022 上半年資安總評報告，我們看到企業的受攻擊面仍持續擴大，讓駭客有更多的入侵管道。同時我們也看到企業的修補作業在 2022 年似乎屢屢失效，這也是為何企業老是出現資安問題的另一項因素。為了深入探究企業的資安問題，我們也研究了無伺服器運算的安全弱點，因為許多雲端服務供應商 (CSP) 正在迅速導入這項技術。過去一年，有越來越多駭客攻擊雲端基礎架構以從事虛擬加密貨幣挖礦，試圖掌控更多資源來投入利潤豐厚的挖礦活動。

在全球網路資安專家不足的情況下，這一點顯得格外嚴重，許多企業目前仍在招募具備資安專業能力的人才。根據顧問公司 McKinsey 的一份報告指出，2022 年第 1 季全球仍有 350 萬個網路資安職缺[1]。希望現有的資安團隊、企業領導人等等都能善用這份報告中的資訊來強化自己的網路資安防禦以防範今日的威脅。企業應該將一套完善而全方位的資安策略列為第一要務，因為企業的受攻擊面正在不斷擴大，而駭客也變得越來越精明。

網路犯罪集團導入企業經營手法

從勒索病毒當前的現況[2] 可看出這類集團在面對獲利下滑的情況下，已經迅速擴大了攻擊的範圍。根據近期的報告指出，勒索病毒從受害者收到的贖金越來越少，從 2021 至 2022 年減少了 38%[3]。那麼，這項威脅又是如何存活至今？最近幾年，那些經營得有聲有色的勒索病毒集團很顯然地正在向合法跨國企業取經，引進了一些相同的經營手法。

品牌重塑與形象管理

這些集團有很多在組織架構上就如同合法經營的企業一樣，包括善用已經建立的人脈[4]，並且為受害者提供技術支援[5]。我們看到，這類集團的專業度不斷提升，同時也採取了更細膩的商業手法。這一點在 2022 年尤其明顯，因為我們看到某個最大的勒索病毒集團在遭遇一次形象危機之後，進行了品牌重塑。

Conti 是近年來最活躍也最強勢的勒索病毒家族之一[6]，然而當他們在 2022 年發動一連串高調的攻擊並且疑似與俄羅斯勾結之後，其品牌就被列入了「黑名單」[7]。Conti 集團在 2022 年年中實質上已停止營運，然而，原本的成員卻分散成幾個新集團，打著新品牌的旗幟重新出發，包括：Black Basta、BlackByte、Karakurt 及 Royal。這次的品牌重塑是一項計畫縝密的行動，根據一些報導[8] 指出 Conti 已規劃了一系列的公開攻擊來為其重新化身的小集團製造曝光率。

多角化經營

2022 年，我們看到 Agenda、BlackCat、Hive 及 RansomExx 等幾個勒索病毒集團使用 Rust 程式語言來開發新版的勒索病毒[9]。這個跨平台程式語言讓駭客能針對不同作業系統對惡意程式進行客製化，例如企業常用的 Windows 和 Linux 作業系統。

正如我們在 2022 上半年資安總評報告中指出[10]，勒索病毒集團正在將版圖擴大到 Windows 和 MacOS 之外，開始攻擊 Linux。所以改用 Rust 語言是勒索病毒集團讓自己更容易攻擊 Linux 電腦的另一項技巧。而且 Rust 語言更難分析，也更不容易被防毒引擎偵測，因此對駭客來說更具吸引力。

作業系統	2021 年	2022 年
Linux	3,790	27,602
MacOS	15,154	11,000

表 1：不同作業系統的勒索病毒數量比較。

近年來，我們看到現代化勒索病毒集團紛紛採用雙重勒索技巧[11] 來進一步對受害者施壓，逼迫他們付錢。去年，我們的研究顯示他們開始利用現有的經營架構和工具來開拓新的收入來源[12]。比方說，BlackCat[13] 勒索病毒使用了一個新版的 ExMatter 資料外傳工具以及 Eamfo 這個專門竊取登入憑證的惡意程式。

對勒索病毒集團來說，改用偷來的資料賺錢並非難事，目前許多勒索病毒服務 (RaaS) 已經在好好善用他們手上現有的工具。我們預料未來這些集團將從已經駭入的企業身上榨出更多獲利[14]，例如從事股票詐騙、變臉詐騙 (BEC)、洗錢，以及竊取虛擬加密貨幣等等。

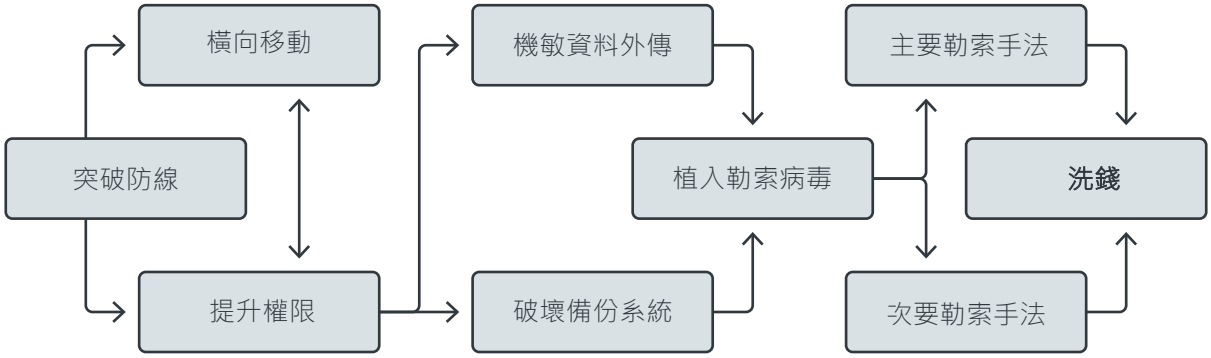

圖 1：勒索病毒最新商業模式範例。

這類集團將逐漸變得樣樣精通，利用原本建立的經營架構和大量工具來開拓新的商業版圖。他們不會固守單一攻擊方式、入侵途徑，或單一營收來源。

> LockBit 3.0 勒索病毒集團率先推出勒索病毒漏洞懸賞計畫。一般來說，通常都是科技公司才會成立漏洞懸賞計畫[15]，目的在透過集體的力量來發掘漏洞，提供獎金給發現漏洞的研究人員，好讓他們幫忙修補自己的漏洞。2022 年，我們看到勒索病毒集團也開始針對其惡意程式採取同樣的作法。
>
> **2022 年勒索病毒新手法**

存取權限對駭客至關重要

不論是哪一種類型的駭客，他們都需要取得存取權限才能進入攻擊目標的環境內部。這一點從 2022 年駭客最常使用的前三大 MITRE ATT&CK 技巧就能看出端倪，這些技巧也反映出大多數駭客的標準作業程序。不論是哪一型駭客，其突破防線的階段在技術上看來都沒有太大差別。

2022 年駭客最常用的三大 MITRE 技巧

遠端服務，技巧 T1021 – 企業 | MITRE ATT&CK®

(橫向移動)

- 駭客可能使用合法帳號來登入某個提供遠端連線的服務，例如：telnet、SSH 和 VNC。接下來就利用已登入使用者的身分從事各項活動。

合法帳號，技巧 T1078 – 企業 | MITRE ATT&CK®

(突破防線)

- 駭客可能掌握了現有帳號的登入憑證，利用該帳號來突破防線、常駐內部、提升權限，或者躲避偵測。已遭外洩的登入憑證可用來避開網路上各種系統資源的存取控管機制，甚至可常態性存取遠端系統以及對外服務。

搜刮作業系統登入憑證，技巧 T1003 – 企業 | MITRE ATT&CK®

(取得登入憑證)

- 駭客可能嘗試搜刮登入憑證來取得作業系統或軟體內儲存的帳號和密碼 (正常來說密碼會以雜湊碼或純文字形式儲存)。接下來，搜刮到的登入憑證便可讓駭客在網路內部橫向移動或存取受管制的資訊。

這前三大攻擊技巧顯示駭客會先透過遠端服務取得存取權限，接著搜刮登入憑證，然後利用合法帳號在環境內部擴大足跡。

2022 年 Microsoft 的一大改動

在過去 7 年當中，最常被駭客用來突破防線的工具就是含有惡意巨集的 Microsoft Offce 文件。這類文件通常隨附在一個含有社交工程訊息的電子郵件，藉此引誘受害者開啟該文件。文件一旦開啟，惡意巨集就會下載並執行能讓駭客進入企業的惡意程式。

然而，2022 年初，Microsoft 突然決定封鎖 Office 文件內的巨集，禁止巨集執行。更確切地說，他們會封鎖從網際網路下載的巨集，包括隨附在電子郵件內的巨集。對駭客來說，光這一個動作，就讓一切完全改觀。由於再也無法使用 Microsoft 巨集，因此駭客開始另闢途徑。

Microsoft 巨集的替代方案

我們所知用來突破防線的替代方案包括：HTML 偷渡 (HTML smuggling)[16] 以及惡意廣告[17]。2022 年末，我們發現有越來越多知名品牌和應用程式的關鍵字遭到挾持，用來顯示惡意廣告。例如，在 Google 搜尋「Adobe Reader」會顯示一個指向惡意網站的廣告。

HTML 偷渡是一種使用電子郵件的突破防線技巧。其基本概念是使用一個惡意的 HTML 檔案作為電子郵件附件。當該檔案開啟時，這個 HTML 檔案會偷渡一個 ZIP 檔案到電腦上，裡面是一個含有 LNK 檔案的 ISO 檔案，這個 LNK 檔案會下載惡意檔案。這是一個相當拐彎抹角的方法，但最後的惡意檔案卻能讓駭客取得首次存取權限。

除此之外，我們也在 2022 年看過網路犯罪集團「就地取材」(利用合法系統和工具) 的案例。確切來說，我們發現像 Cobalt Strike 和 Brute Ratel 這類合法的滲透測試工具被用於惡意攻擊當中[18]。一名熟悉這類滲透測試工具及作業系統內建工具的駭客，能在很短時間內就造成嚴重威脅。

時間	活動
T-0	經由 HTML 偷渡取得首次存取權限。
+16 分鐘	建立幕後操縱 (C&C) 通訊並執行前期偵查。
+5 分鐘	植入 Brute Ratel。
+5 分鐘	使用作業系統內建工具來執行偵查。
+10 分鐘	使用另一項工具來執行 AC 偵查。
+7 分鐘	利用 Cobalt Strike 開始橫向移動。

表 2：使用合法滲透工具的攻擊時間表範例。

受攻擊面正在擴大且修補更新屢屢失效

駭客一直在彼此互相學習，也因此他們的動作和行動方式大致上相同。不過，他們使用的工具和個人偏好還是有所不同 (要看手邊有沒有)，還有就是他們網路環境的設定方式。

2022 年最常被攻擊的漏洞

談到 2022 年最常被攻擊的 Common Vulnerabilities and Exposures (CVE) 漏洞，我們發現原本以 Microsoft 為大宗的情況變成了以 Log4j 為主的情況[19]。這很可能與前一節提到的 Microsoft 重大改變有關。Log4j 是開發人員用來追蹤或記錄系統或應用程式活動的一個 Java 函式庫，在 2021 年底左右被發現了多個相當知名的漏洞[20]，2022 年一開始，駭客便開始攻擊這些漏洞。

2021 年前三大 CVE 漏洞	2022 年前三大 CVE 漏洞
NVD – CVE-2021-26855 (nist.gov) NVD – CVE-2021-27065 (nist.gov) NVD – CVE-2020-0688 (nist.gov) 這些全部都是 Microsoft Exchange 漏洞。	NVD – CVE-2021-44228 (nist.gov) NVD – CVE-2021-45015 (nist.gov) NVD – CVE-2021-45046 (nist.gov) 其中兩個是 Log4j 漏洞，一個相對較不為人知。

表 3：前三大 CVE 漏洞比較 (2021 與 2022 年)。

在檢視 2022 年的三大 CVE 漏洞時，有幾點值得注意：

- CVE 漏洞是駭客可公開攻擊的漏洞，在網路上都能找到各種步驟拆解、說明與分析。
- 這些漏洞都相當嚴重，基本上全都是高風險/重大等級的漏洞，其攻擊途徑可經由網路發動，複雜性低，且幾乎不需要先取得存取權限就能發動攻擊，也無須使用者介入 (意味著攻擊可以自動化)。
- 漏洞已經在新聞上曝光，而且已經成熟可用。此外也有受影響的廠商 (或客戶) 名單，駭客可從這些名單當中挑選目標下手。

駭客通常會立即掌握最新揭露的漏洞，而且深知哪些 CVE 漏洞可以用於他們的行動當中。因此，資安專家和使用者必須隨時搶先駭客一步，在漏洞遭到攻擊之前趕緊先修補。

不同的駭客所使用的漏洞和弱點也許會相似，但動機卻不盡相同。他們的最終目標有可能是為了蒐集資料並將資料外傳、發動勒索病毒攻擊、從事虛擬加密貨幣挖礦，或者其他惡意活動。

除此之外，我們也研究了一下 Trend Micro™ Deep Security™ (DS) 產品一整年偵測到的漏洞相關事件，並看到與我們上半年資安報告類似的結果：dnsmasq 的 CVE-2017-14495 漏洞是偵測事件最多的漏洞，這不令人意外，因為 dnsmasq 是一個熱門的免費軟體，可用來架設 DNS (網域名稱系統)、DHCP (動態主機組態設定協定) 和 TFTP (小型檔案傳輸協定) 伺服器，主要用於路由器和物聯網 (IoT) 閘道當中。

其他偵測數量較高的漏洞就相當多元：CVE-2021-44228 是我們前一節提到的 Apache Log4j 的漏洞，而 CVE-2006-4154 則是另一個 Apache 的漏洞。同樣地，我們看到駭客會攻擊一些使用廣泛且對許多企業相當重要的免費技術。就像 dnsmasq 一樣，Apache 也是一個免費軟體，而且全球有 67% 的網站都用到它[21]。

過濾規則 ID	解決方案	相關 CVE	偵測事件數量
1009667	Deep Security	CVE-2017-14495	149,584,000,000
1011242	Deep Security	CVE-2021-44228	11,766,751,565
1000853	Deep Security	CVE-2006-4154	5,667,326,528
1004398	Deep Security	CVE-2010-2730	1,970,505,793
1010971	Deep Security	CVE-2021-29441	1,936,302,017
1011466	Deep Security	CVE-2022-30522	1,518,554,891
1006027	Deep Security	CVE-2014-0098	871,076,092
1011456	Deep Security	CVE-2022-26134	533,046,544
1011265	Deep Security	CVE-2021-45046	269,500,708
1011492	Deep Security	CVE-2022-30136	169,278,618

表 4：2022 年 Trend Micro™ Deep Security™ 與 Trend Micro Apex One™ 偵測到的漏洞相關事件數量。

Spring4Shell CVE-2022-22965 - CVSS 評分：9.8

CVE-2022-22965 是一個 Spring Framework 的重大漏洞[22]，Spring Framework 是一套用來開發企業級 Java 應用程式的框架。我們最早在 2022 年 4 月看到這個漏洞，研究顯示它能讓駭客執行 Mirai 殭屍網路惡意程式。

Log4Shell CVE-2021-44228 - CVSS 評分：10.0

CVE-2021-44228 是一個 Apache Log4j 當中的重大漏洞，Log4j 是一個使用相當廣泛的 Java 記錄檔函式庫。全世界的國防機構都針對這個漏洞發出了警告[23]，因為網路上已經有攻擊出現。此漏洞在 2021 年首次被通報，但其資安問題一直延燒到 2022 年。

漏洞焦點

ZDI 破紀錄的數字

趨勢科技 Zero Day Initiative™ (ZDI) 漏洞懸賞計畫所發布的漏洞公告數量越來越多，而 2022 年是第三度刷新紀錄的一年，總共發布了 1,706 份公告，是該計畫有史以來最高的數字。

根據我們觀察，漏洞公告發布數量之所以穩定成長，有兩項原因：首先，受攻擊面呈倍數擴大，因此有更多的漏洞可被發掘。另一項因素是，ZDI 本身投資了自動化分析流程，結果就是研究人員有辦法發現更多漏洞。

若比較已通報 CVE 漏洞的嚴重性，我們看到重大漏洞數量從 2021 至 2022 年翻了一倍 (54 至 110)，儘管還未達到 2020 年重大漏洞數量的最高點 (173)。

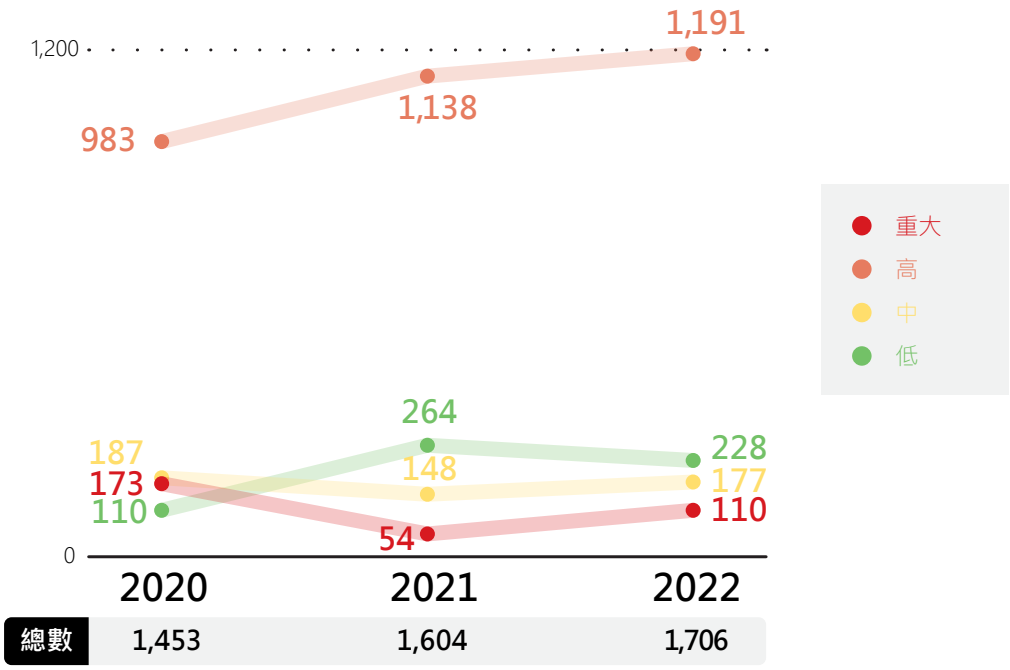

圖 2：漏洞公告數量與嚴重性逐年比較 (2020、2021、2022 年)。

在仔細研究漏洞本身之後，我們並未看到漏洞的類型有太大變化。不過，我們確實看到修補更新失效的情況增加[24]，也許企業並無充分的時間或資源來製作完整的解決方案，只是單純地將緊急修正推播出去，而非解決根本的問題。不僅如此，軟體廠商在發布漏洞警報時所揭露的資訊似乎也不夠詳盡，使得企業和資安領導人在套用修補更新時沒有太多資訊可供參考。

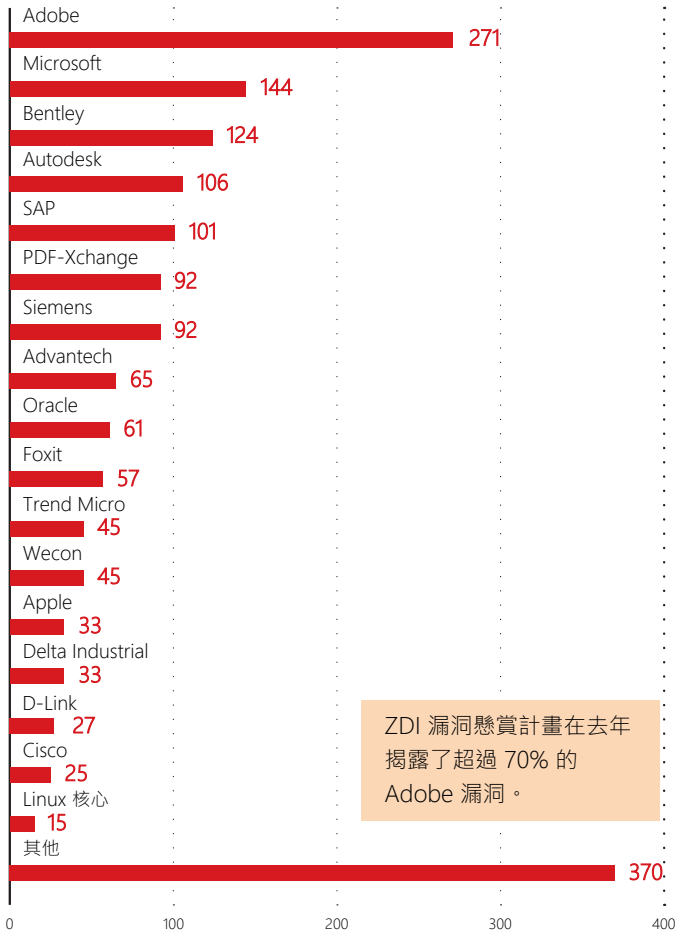

圖 3：2022 年各廠商發布的安全公告數量。

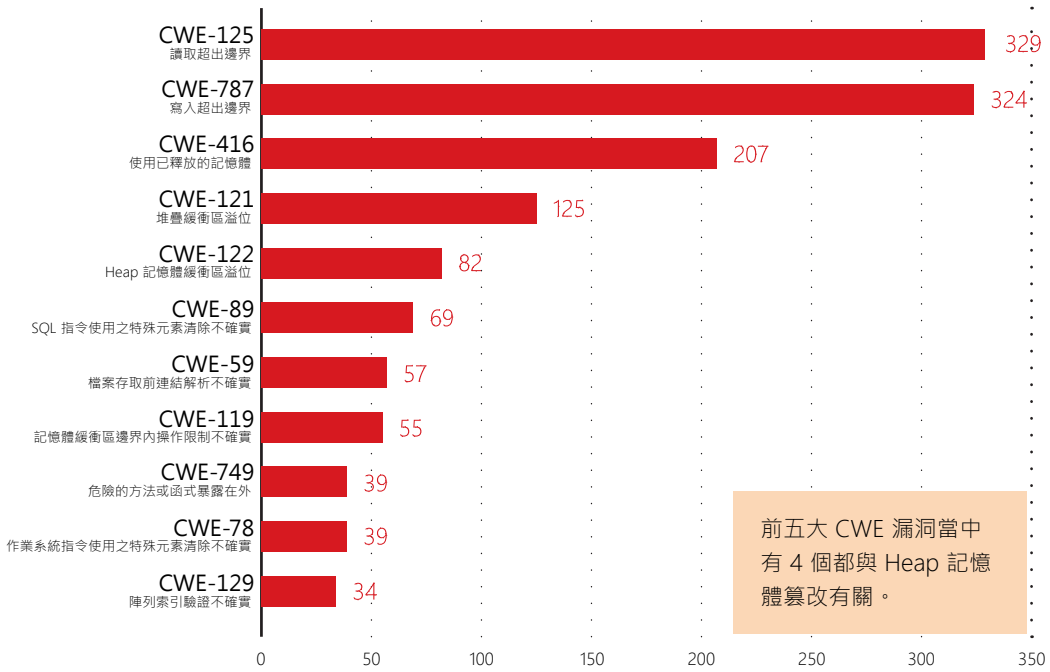

圖 4：2022 年發布的前十大 CWE 公告。

受攻擊面擴大帶來的另一個問題是虛擬私人網路 (VPN) 不斷被人發現漏洞。疫情期間，VPN 的用量突然暴增[25]，因為許多企業都仰賴 VPN 來生存。我們在 2022 上半年資安總評報告當中對於某些 VPN 漏洞的攻擊有詳細說明，而這項威脅仍延續至年底。

其中最常被攻擊的漏洞依然是 Fortinet FortiGate SSL 被發現的路徑瀏覽漏洞 (CVE-2018-13379)，另一個同樣經常被攻擊的漏洞是 Pulse Secure Pulse Connect Secure (PCS) 被發現的任意檔案讀取漏洞。

	Fortinet		Pulse Secure				Citrix Systems	
	CVE-2018-13379	CVE-2022-40684	CVE-2019-11510		CVE-2019-11539	CVE-2021-22893	CVE-2019-19781	
	DV-36087	DV-41863	DV-36089	DV-36241	DV-36095	DV-39636	DV-36876	DV-36927
一月	21,710		8,708	506			1,120	27
二月	21,733		8,204	775			684	15
三月	26,405		10,110	1,940			2,068	60
四月	25,077		14,950	1,483		3	1,134	67
五月	32,590		16,226	1,800	30	1	1,770	76
六月	90,700		48,098	1,765		2	3,361	43
七月	76,897		55,665	2,729	8		4,270	193
八月	123,201		71,423	2,848	4		4,454	140
九月	142,205		78,879	5,606	8	3	3,641	157
十月	163,583	861	89,949	7,762	24	4	10,735	252
十一月	90,505	562	29,600	6,001	12	1	8,273	148
十二月	118,736	1,730	32,881	20,098	16		22,141	122

	F5					SONICWALL
	CVE-2020-5902		CVE-2021-22986			CVE-2021-20016
	DV-37841	DV-38276 (惡意程式)	DV-39360	DV-39352	DV-39364	DV-39727 (惡意程式)
一月	19,339		1,320	173	3,126	
二月	17,581		2,503	446	3,419	
三月	34,507		1,481	313	3,418	
四月	24,881		91	303	3,884	
五月	36,079		12	394	54,692	
六月	62,302		39	241	105,075	
七月	62,756	1	2	216	91,045	1
八月	84,159		1	178	45,099	
九月	109,689			155	44,891	
十月	113,307	27		168	35,872	
十一月	40,429			42	17,013	161
十二月	60,664			99	23,447	160

表 5：已知 VPN 漏洞每月攻擊偵測數量 (2022 年)。

發掘藏匿在雲端的弱點

雲端服務供應商 (CSP) 導入無伺服器運算的腳步飛快，因為這項技術能讓企業執行一些服務而不須負責管理底層的基礎架構。這些服務主要是用來管理業務的運作，例如：內建擴充能力、多區域可用性，以及成本管理性。無伺服器技術可讓開發人員將程式碼上傳至某個服務而不需操心基礎架構的維護、擴充性與可用性問題。

無伺服器在安全上的脆弱環節

2022 年，我們研究了這些無伺服器平台的安全性，並且點出一些可能遭到駭客利用的脆弱環節。企業將這些無伺服器運算服務用來監督複雜的流程與儲存營業所需的資訊。此外，機密與敏感資料的處理與管理，也是服務供應商及使用者都必須擔心的問題。

圖 5：無伺服器平台可能的用途。

駭客已經開始將重心轉向雲端導向服務，因為雲端組態設定錯誤是個普遍存在的問題，所以無伺服器環境很可能是他們的下一個目標。由於無伺服器技術可讓使用者上傳程式碼至服務，因此使用者電腦的安全以及撰寫安全的程式碼，是使用者的責任。所以很重要的一點就是要防範使用者所造成的組態設定錯誤。

除此之外，我們也在總結中提到，雲端服務預設的組態設定從資安角度來看並非最佳狀態。使用者應尋找一些能強化作業系統的解決方案，並看看該採取哪些類似的資安步驟來強化無伺服器環境。

同時我們還提到了另一個無伺服器的安全問題，那就是使用者和 CSP 都沒有做好密鑰與存取令牌的保護。最近有多起駭客集團[26] 搜刮了 CSP 的密鑰進而接管了目標服務或整個帳號的事件。

其中一起事件[27] 是 TeamTNT 集團所為，他們專門竊取 Amazon Web Services (AWS)、Docker 及 Linux Secure Shell (SSH) 登入憑證，駭客在入侵雲端環境之後，會特別尋找某些敏感的環境變數[28]。 另有一起供應鏈攻擊事件[29] 是駭客篡改了某個 Python 函式庫的程式碼來搜刮敏感的變數內容。

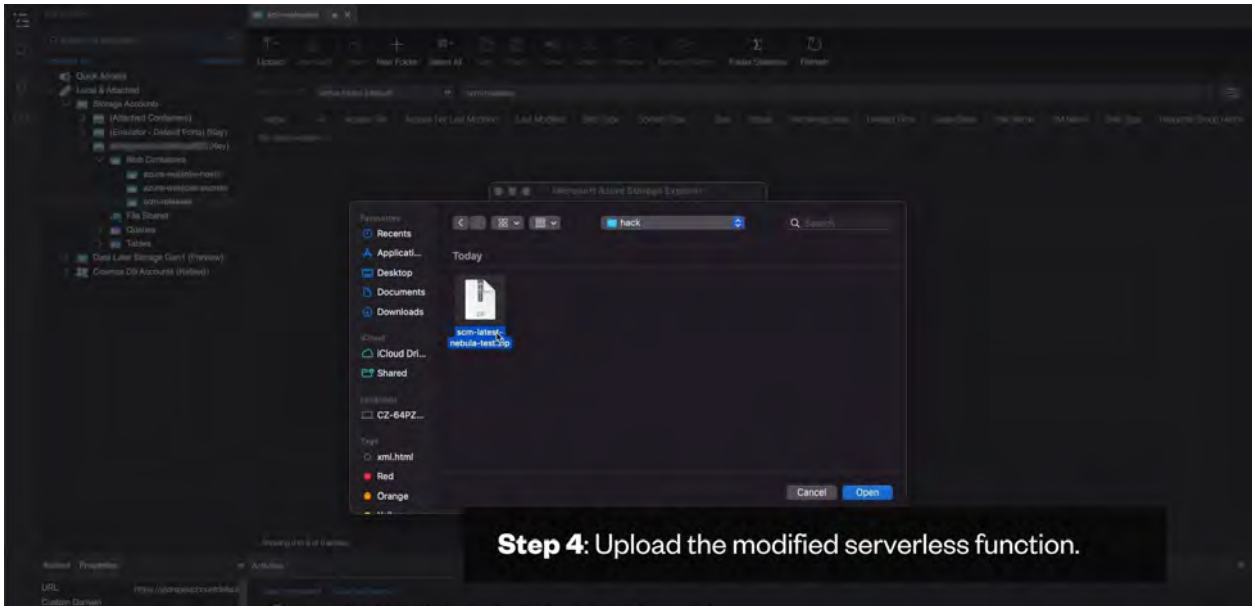

圖 6：趨勢科技報告指出將密鑰儲存在環境變數當中可能如何導致機密意外洩漏[30]。

CSP 的職責是要讓無伺服器服務順利運作，然而將程式碼部署到無伺服器系統上的卻是使用者。在最新的報告中[31]，我們模擬了使用者在市面上的主流 CSP 無伺服器服務上傳的程式碼含有漏洞的情況。根據我們對各家無伺服器環境的評測發現，Microsoft Azure 的資安環境具有一些隱憂，例如：

- Microsoft Azure 環境內含一些敏感的環境變數，這些變數的內容一旦外洩，駭客就能完全駭入整個無伺服器環境。
- 在大多數的 Azure App Service 部署環境中皆有一個預設的執行時期映像使用了一個萬用密碼 (master password) 可讓駭客提升權限。

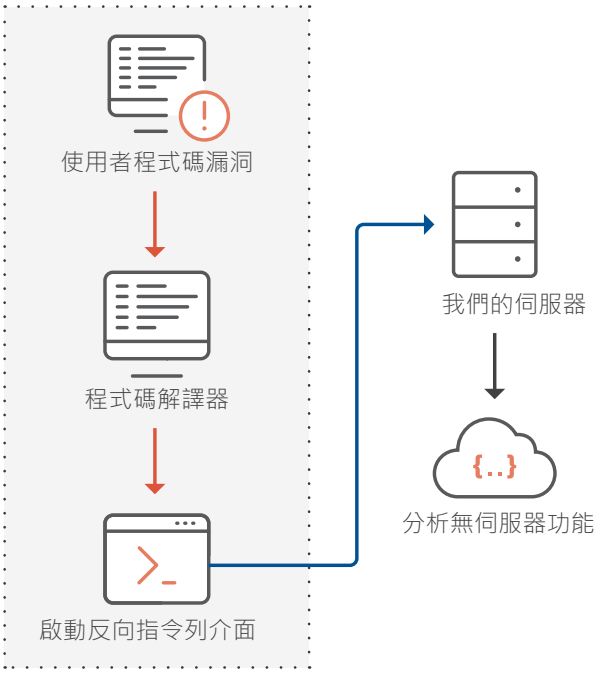

圖 7：模擬針對無伺服器功能的攻擊。

在這裡，我們所看到的一個重點是，使用者可能帶來嚴重的資安風險，一名不熟悉環境的使用者很可能會造成雲端服務組態設定錯誤，進而擴大受攻擊面或上傳了容易遭到漏洞攻擊的程式碼。

雲端虛擬加密貨幣攻擊現況

虛擬加密貨幣的大起大落與挖礦獲利持續下滑[32]，迫使挖礦集團必須另尋其他替代方案與技巧。2022 年，我們看到這類駭客集團將目標轉向入侵雲端基礎架構，不再仰賴獲利不佳的 CPU 挖礦。

這樣的發展早已不是新聞，但 2022 年我們發現隨著新的雲端服務推出與免費供應的速度加快，其攻擊頻率也跟著變高[33]。有時駭客還能即時擴大攻擊規模，因此哪怕只是入侵個幾分鐘或幾小時的時間，就能為駭客帶來相當的獲利。

目前，虛擬加密貨幣挖礦的資源爭奪戰似乎相當激烈，我們曾經看到兩個駭客集團彼此互相爭奪受害者的伺服器控制權[34]，而且控制權在短短一天之內便數度易手。這些集團會使用腳本來協助他們清除競爭對手的挖礦程式，同時也會不斷強化自身的加密編碼能力與常駐機制。

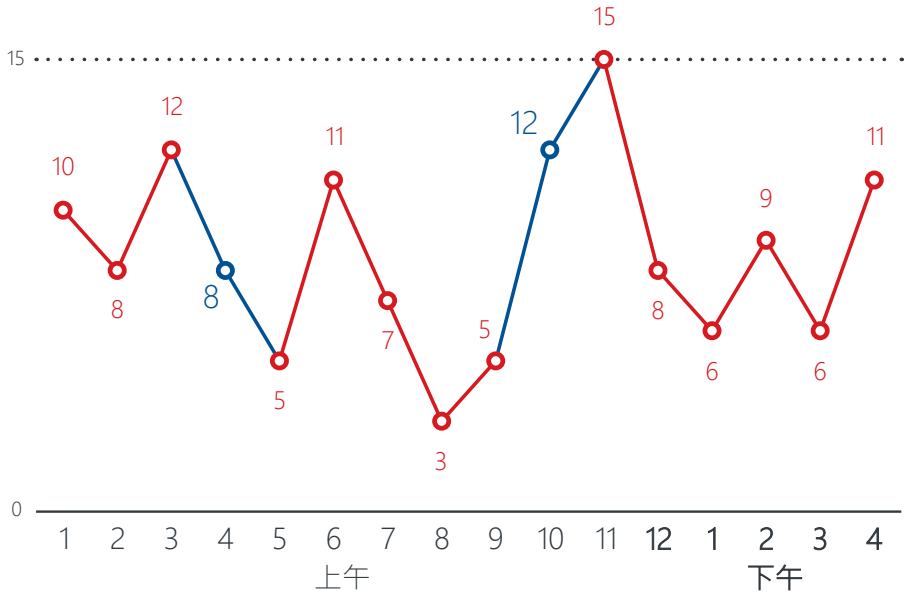

圖 8：Kinsing (紅色) 與 8220 (藍色) 兩大集團在一天當中不斷互相爭奪某個雲端執行個體的控制權，數字代表對內操控連線的數量。

我們看到挖礦集團同樣也呼應勒索病毒集團聚焦 Linux 系統的趨勢，瞄準那些防護較差的目標來獲取暴利。2022 年 11 月我們還攔截了一起使用 CHAOS 遠端管理工具[35] 的虛擬加密貨幣挖礦攻擊，該工具是一個專門攻擊 Linux 電腦的遠端存取木馬程式 (RAT)。

作業系統	2021 年	2022 年
Linux	8,240	13,228
MacOS	1,488	889

表 6：Linux 與 MacOS 虛擬加密貨幣挖礦程式數量比較 (2021 與 2022 年)。

企業應該對虛擬加密貨幣挖礦程式的潛在問題有所認識，當企業的系統上出現虛擬加密貨幣挖礦程式，這通常意味著企業雲端基礎架構存在著更深問題。出現挖礦程式看起來也許不像資料外洩或感染勒索病毒那樣嚴重，但駭客入侵目標系統的方法基本上都一樣。大多數的駭客，不論其動機或最終目的為何，都會先攻擊企業資安上的某個弱點。企業出現挖礦程式不僅會影響雲端基礎架構，同時也是資安狀況不佳的一種指標。

> CPU 使用率從原本的 13% (平均值) 一下子飆到 100%。
> 每個月的電力成本從 20 美元一下子變成 130 美元，成長了 600%，這還只是一個雲端執行個體而已。
>
> 關閉或中斷企業的線上服務。

虛擬加密貨幣挖礦將如何影響雲端服務？

網路攻擊對業務的衝擊

網路犯罪的掠奪本質意味著駭客會攻擊他們覺得容易下手且利潤豐厚的企業或技術。正如前面幾節所說，Linux 威脅正在崛起的主要原因是不安全的物聯網 (IoT) 裝置正在企業及家庭環境內部大量普及[36]，令人垂涎。在此同時，虛擬加密貨幣挖礦集團也正在積極尋找能夠潛入企業雲端基礎架構並暗中吸取資源的方式。

2022 年，我們也看到勒索病毒集團攻擊中小企業環境，這些較小的企業由於 IT 資安的資源較為不足，無法避免或對付複雜的攻擊，因此當遭遇網路攻擊時可能就會遭歹徒挾持。

員工規模	攻擊數量
小 (1-200)	1,213
中 (201-1000)	657
大 (1001 以上)	497

表 7：勒索病毒受害企業規模分布情況 (2022 年)。

另一份趨勢科技的全球調查也指出，52% 的企業都曾經發生某家供應鏈廠商遭遇勒索病毒襲擊的情況[37]。確切來說，軟體供應鏈是問題的核心，企業內使用的各種不同元件和工具都可能成為網路犯罪集團攻擊和濫用的對象。此外，第三方廠商也可能帶來新的軟體必須整合至企業內。網路犯罪集團有眾多途徑可入侵網路，而且只需一個漏洞就足以讓他們存取各式各樣的系統和機敏資料。

軟體供應鏈安全管理的重要步驟之一，就是建立一份軟體物料清單 (SBOM)[38]，也就是一份詳細記載軟體各部分元件與其彼此關係的正式記錄。

圖 9：供應鏈合作夥伴如何影響企業的資安，特別是遇到勒索病毒攻擊的情況。

我們的資料顯示，網路犯罪集團一直聚焦在某些產業，根據我們的研究，製造業是 2021 年駭客的首要目標。但到了 2022 年，威脅分布的情況變得較為平均，而且換成政府機關是駭客的首要目標。

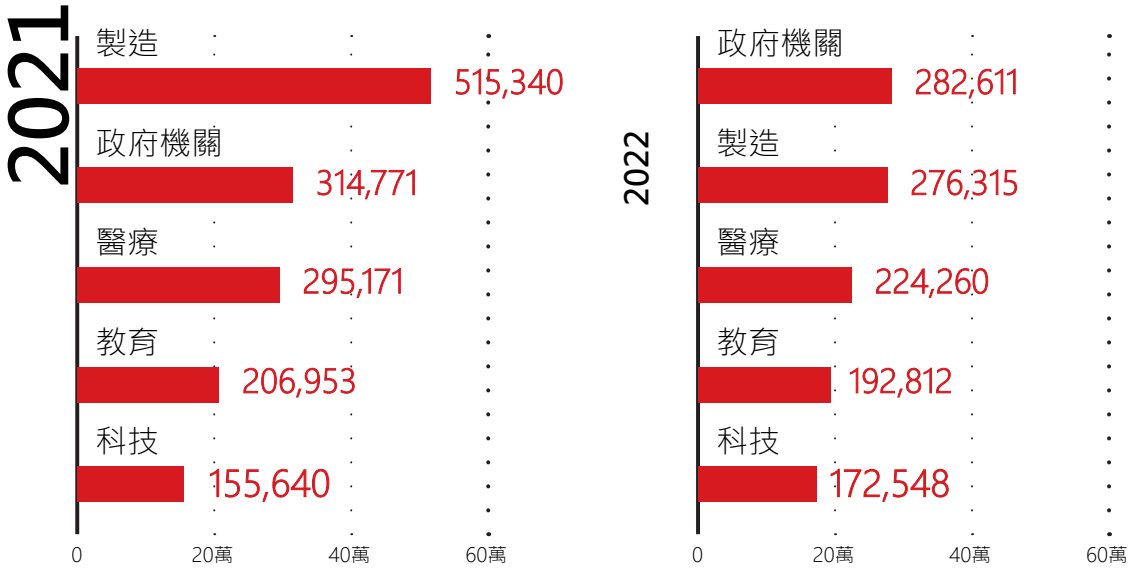

圖 10：受惡意檔案影響最深的五大產業 (2021 與 2022 年比較)。

註：一個惡意程式在同一台電腦上偵測多次只算一台非重複電腦。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

應對戰術日益靈活的駭客的防範策略

數位受攻擊面的擴大，是企業為了在後疫情時代的經濟條件下生存並有效管理遠距上班人力的結果。企業不斷導入新的技術來因應新的混合上班模式、複雜的線上經營及銷售方式、急速擴張的資料儲存需求、資料防護需求等等。正如我們在上半年報告中所言，這意味著企業機構正忙著彌補資安上的漏洞，更別說還有網路資安專家日益短缺的問題。換句話說，許多企業都需要具備適應能力的解決方案和手段，以便採取更有效率的方式來對抗威脅。

目前，駭客正紛紛導入更多合法企業的作法與專業化經營，採用類似的企業方案和策略。他們不僅在工具和攻擊目標上創新，同時也在建立具備韌性的組織架構，而非單純仰賴單一的攻擊方法或特定的目標族群。他們能在單一行動當中同時針對多個面向發動攻擊。

人才的短缺，意味著企業需要一種更有效率、也更全方位的資安解決方案，理想的情況是一套能夠整合多重需求與作業於一身的單一平台。以下是企業應該隨時謹記在心的一些資安實務原則：

- **資產管理。**檢視資產並判斷其重要性、潛在漏洞、威脅活動程度，以及從該資產上蒐集到的威脅情報有多少。
- **雲端資安設定。**確保資安落實到雲端基礎架構設定當中，防範駭客利用已知的弱點和漏洞。
- **適當的資安程序。**將軟體更新列為優先要務以減少遭到漏洞攻擊的情況。此外像虛擬修補這樣的技術，也能協助企業在廠商製作安全更新的期間預先防堵漏洞。
- **受攻擊面可視性。**隨時監控企業內的各種不同技術與網路，以及其相關的資安系統。分散而不連貫的資料來源將造成交叉關聯分析困難。

企業需要一套全方位的解決方案來管理整個受攻擊面，其中，可視性是最重要的關鍵，此外擁有交叉關聯不同指標的能力也相當重要，如此資安團隊才能專心掌握整體情況。一套全方位的平台不僅能提供多層式防護，還有助於減少原本必須花費在多種資安技術上的支出。

威脅情勢

146,408,535,569

2022 年整體威脅攔截總數

2022 年，趨勢科技 Smart Protection Network 全球威脅情報網 (包含行動應用程式信譽評等服務 [MARS]、IoT 信譽評等服務 [IoTRS] 以及 Smart Home Network [SHN] 在內)，總共為客戶攔截了 1,460 億次以上的威脅。我們的年度對照資料顯示，整體攔截的威脅總數較 2021 年增加 55%，此外，已攔截的惡意檔案數量也暴增 242%。在我們攔截的將近 700 億個惡意檔案當中包含了重複與非重複感染的案例，換句話說就是再次感染也計算在內。這一點可能會影響我們偵測到的蠕蟲數量 (如圖 16 所示)。蠕蟲是最難根除的惡意程式，因為它們就是為了常駐在網路內部不斷繁衍而生。此外，大量的病毒與檔案感染器對已攔截檔案數量也有不少貢獻。

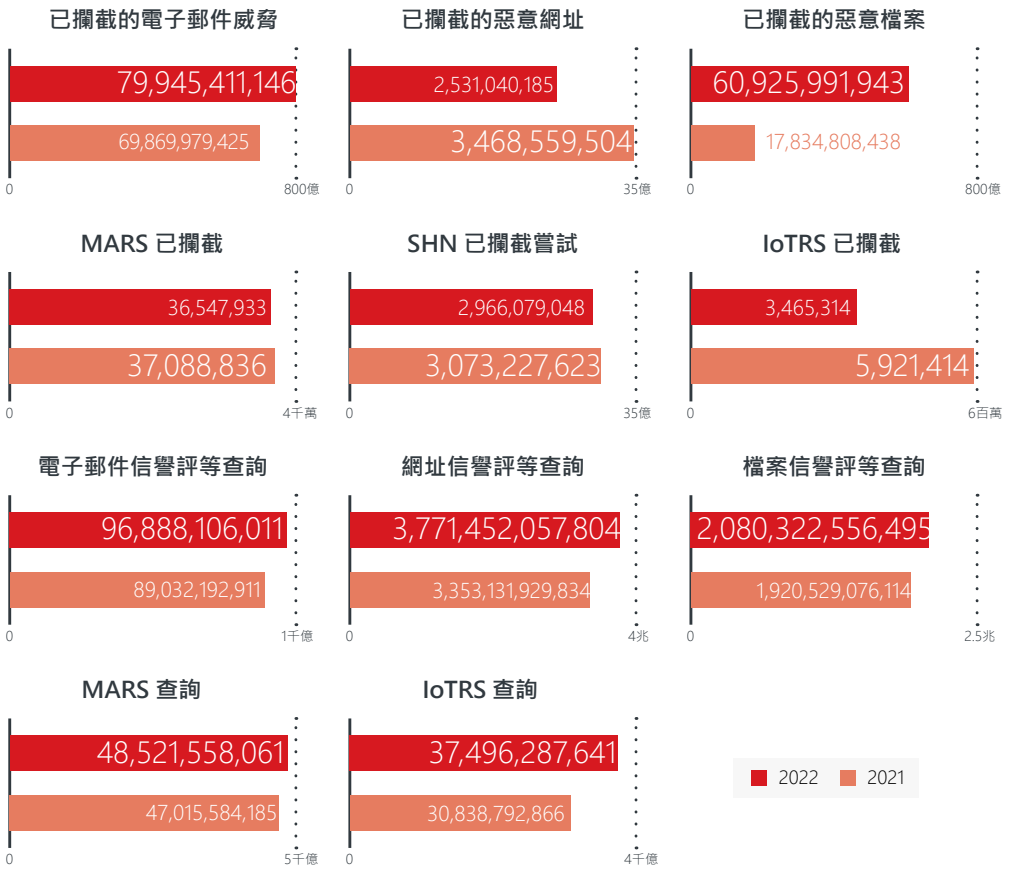

圖 11：已攔截電子郵件、網址及檔案威脅數量比較；電子郵件、網址、檔案信譽評等查詢數量比較；以及已攔截行動應用程式、IoT 及 Smart Home Network 威脅數量比較 (2021 及 2022 年)。

資料來源：趨勢科技 Smart Protection Network (包含行動應用程式信譽評等服務 [MARS]、IoT 信譽評等服務 [IoTRS] 以及 Smart Home Network [SHN] 在內)。

我們所追蹤的威脅在區域分布上呈現出一種有趣的資安版圖，很明顯的是，勒索病毒威脅主要集中在亞洲和美洲地區，變臉詐騙 (BEC) 威脅大多攻擊美洲地區，至於行動安全問題則是亞洲位居第一。

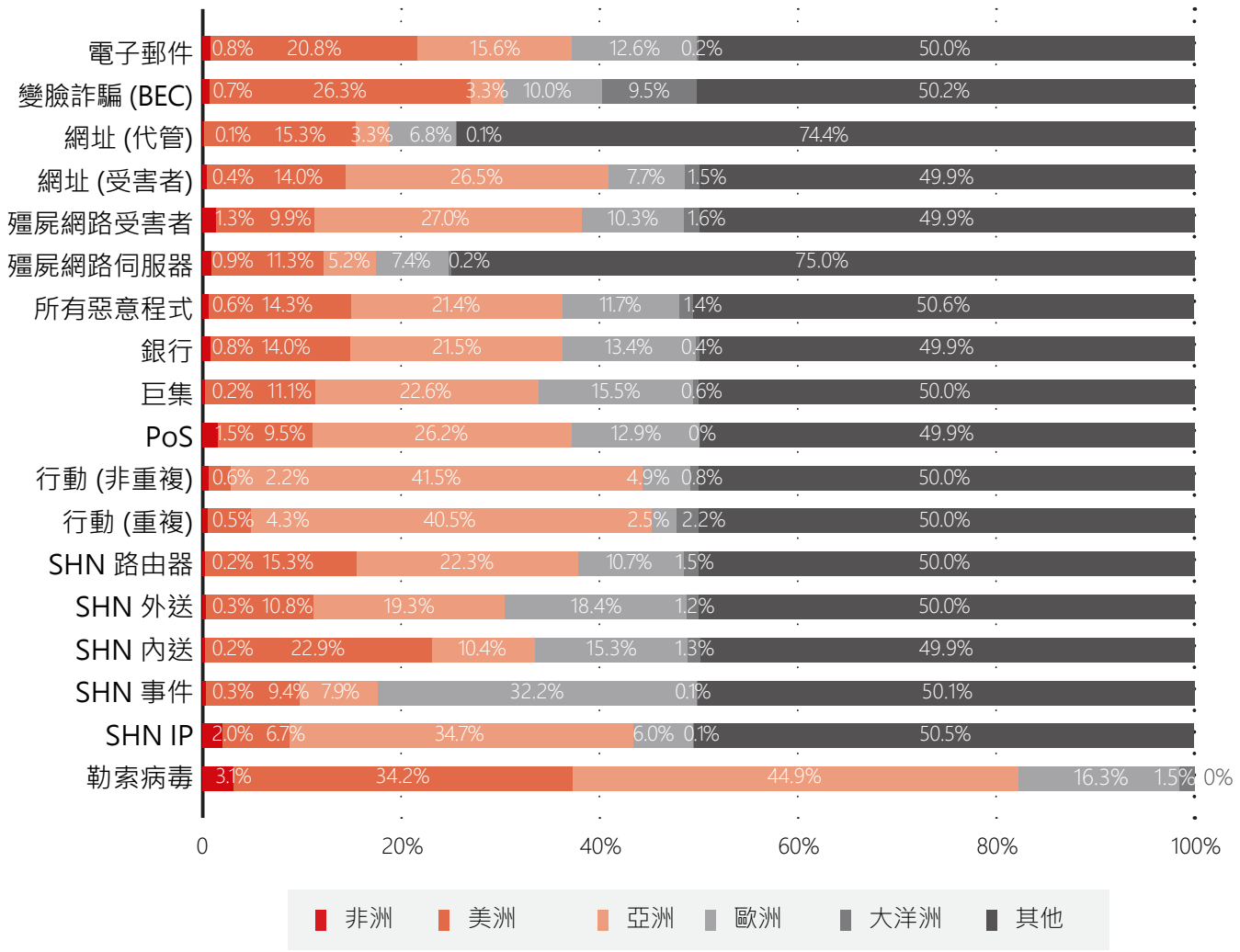

圖 12：趨勢科技 2022 年追蹤的威脅在區域分布上的情況，包括：電子郵件、網址及檔案威脅；已攔截的行動應用程式、IoT 及 Smart Home Network 威脅。

資料來源：趨勢科技 Smart Protection Network (包含行動應用程式信譽評等服務 [MARS]、IoT 信譽評等服務 [IoTRS] 以及 Smart Home Network [SHN] 在內)。

Webshell 是一種可讓駭客入侵網站伺服器並發動攻擊的網站指令列腳本。它們是年度偵測數量最多的惡意程式，Webshell 偵測數量從 2021 至 2022 年暴增 103%。Emotet 偵測數量排名第二，它在 2021 年並未進入十大排行榜，但 2022 卻重新復出。在勒索病毒方面，LockBit 和 BlackCat 是 2022 年最強勢的家族。

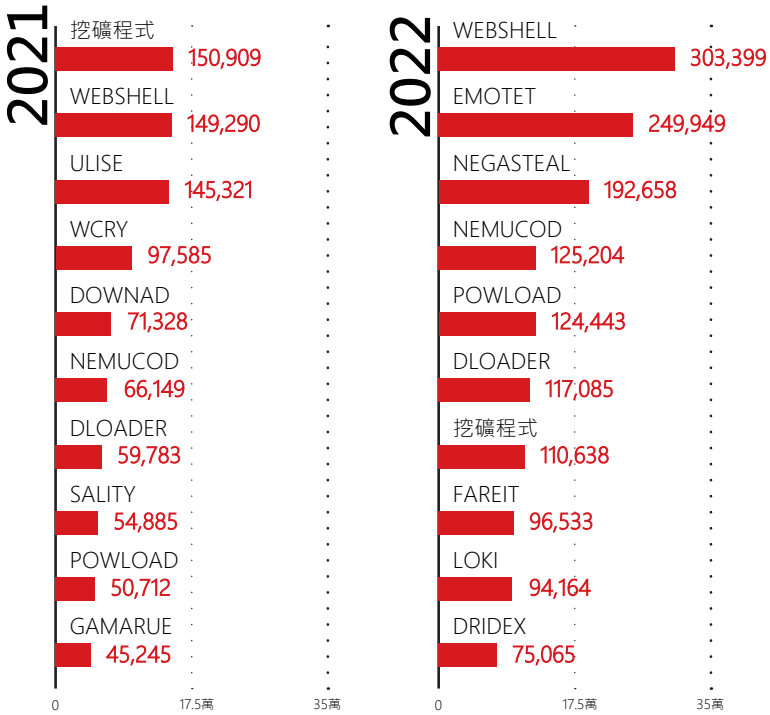

圖 13：偵測數量最高的前十大惡意程式家族比較 (2021 及 2022 年)。

資料來源：趨勢科技 Smart Protection Network。

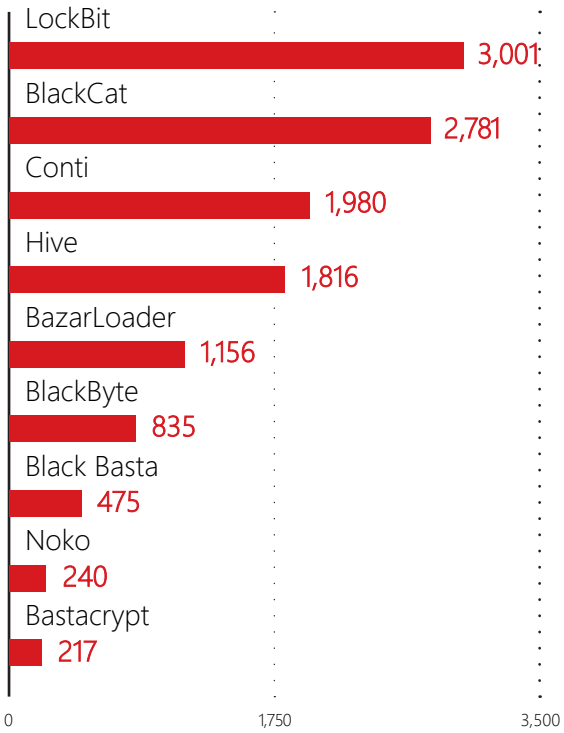

圖 14：勒索病毒家族排行榜 (2022 年)。

資料來源：趨勢科技 Smart Protection Network。

	一月	二月	三月	四月	五月	六月
1	沒有新的家族	沒有新的家族	Ransom.Win32.EXPLUS.A	Ransom.Linux.CHEERSCRYPT.A	Ransom.Win64.KEVERSEN.A	Ransom.MSIL.ZAGREUS.A
2			Ransom.Win32.NOESCAPE.A		Ransom.Win32.STORAGECRYPT.A	Ransom.Win32.LORENZ.A
3					Ransom.MSIL.PALANG.A	Ransom.Win32.EVILNOMINATUS.A
4					Ransom.Win32.BLAZE.A	
5						
總數			2	1	4	3

	七月	八月	九月	十月	十一月	十二月
1	No New Families	Ransom.Win32.USELESSDISK.A	Ransom.PS1.BEBACK.A	Ransom.Win32.GORF.A	Ransom.MSIL.PENTERWARE.A	Ransom.Win32.HMBRAN.A
2		Ransom.Win32.WRLDECODING.A		Ransom.Win32.MIMIKRYPT.A	Ransom.Win32.BEIJIRAN.A	Ransom.Win64.PANDORA.A
3		Ransom.Win32.PLAYDE.A		Ransom.Win32.CRYPTATO.A	Ransom.Win64.VICESOCIETY.A	Ransom.Win.32.SCHOOBOS.A
4		Ransom.MSIL.KANCRYPTER.A			Ransom.MSIL.MALLOX.A	
5					Ransom.Win64.BLOODY.A	
總數		4	1	3	5	3

表 8：2022 年偵測到的新勒索病毒家族。

資料來源：趨勢科技 Smart Protection Network。

2022 年已攔截的惡意應用程式數量較前一年減少 1.5%。

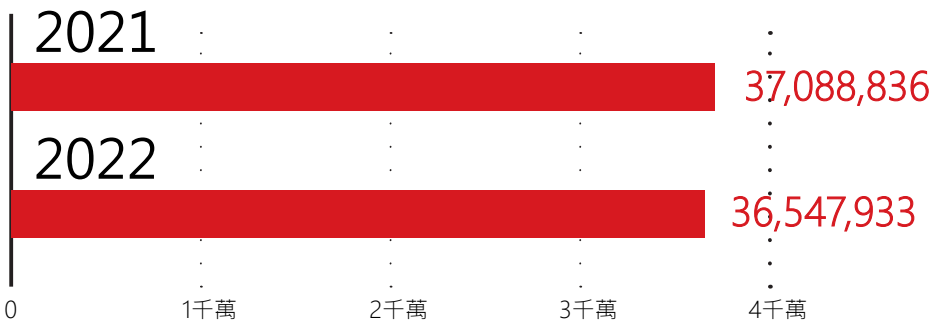

圖 15：已攔截的惡意應用程式數量比較 (2021 及 2022 年)。

資料來源：趨勢科技行動應用程式信譽評等服務 (MARS)。

2022 年惡意檔案偵測數量暴增，在研究過這些檔案之後，我們歸納出以下幾種惡意程式類型。駭客工具的使用情況增加了 11.1%，有可能是因為這些駭客工具被用來植入勒索病毒。2022 年當中使用最廣泛的是 Bloodhound 這個工具，反觀 2021 年使用最廣的工具則是 Mimikatz。後門程式偵測數量大幅增加 86.2%。這些後門程式大多攻擊網站伺服器平台的漏洞。

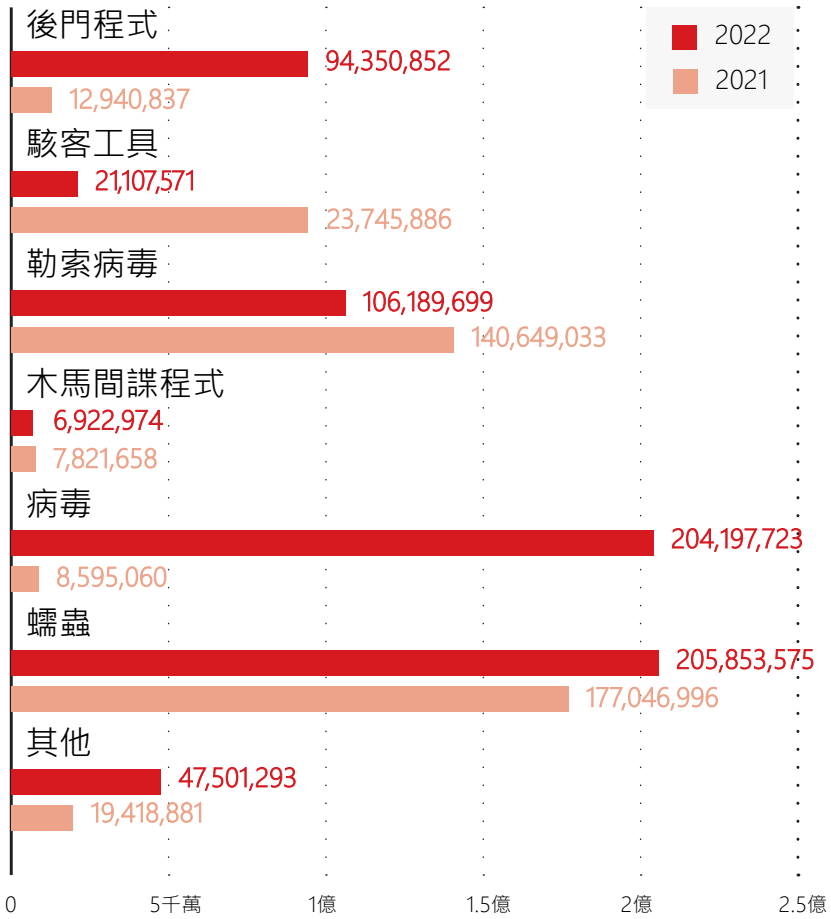

圖 16：已攔截惡意檔案中的惡意程式類型比較 (2021 及 2022 年)。

附註

1 Rami Sass. (Nov. 14, 2022). *Forbes*. "A New Approach Is Needed To Close The Cybersecurity Talent Gap." Accessed on Mar. 1, 2022, at: Link.

2 Feike Hacquebord, Stephen Hilt, and David Sancho. (Dec. 15, 2022). *Trend Micro Security News*. "The Future of Ransomware." Accessed on Mar. 1, 2022, at: Link.

3 Pieter Arntz. (Jan. 23, 2023). *Malwarebytes*. "Ransomware revenue significantly down over 2022." Accessed on Mar. 1, 2022, at: Link.

4 Trend Micro Research. (Oct. 27, 2022). *Trend Micro Security News*. "Ransomware Spotlight: BlackCat." Accessed on Mar. 1, 2022, at: Link.

5 Trend Micro Research. (Dec. 7, 2022). *Trend Micro Security News*. "Ransomware Spotlight: Cuba." Accessed on Mar. 1, 2022, at: Link.

6 Trend Micro Research. (Dec. 1, 2021). *Trend Micro Security News*. "Ransomware Spotlight: Conti." Accessed on Mar. 1, 2022, at: Link.

7 Eduard Kovacs. (May 23, 2022). *Security Week*. "Conti Ransomware Operation Shut Down After Brand Becomes Toxic". Accessed on Mar. 1, 2022, at: Link.

8 Lawrence Abrams. (May 19, 2022). *Bleeping Computer*. "Conti ransomware shuts down operation, rebrands into smaller units." Accessed on Mar. 1, 2022, at: Link.

9 Nathaniel Morales et al. (Dec. 16, 2022). *Trend Micro Research*. "Agenda Ransomware Uses Rust to Target More Vital Industries." Accessed on Mar. 1, 2022, at: Link.

10 Trend Micro Research. (Aug. 31, 2022). *Trend Micro Research*. "Defending The Expanding Attack Surface: Trend Micro 2022 Midyear Cybersecurity Report." Accessed on Mar. 1, 2022, at: Link.

11 Janus Agcaoili et al. (Jun. 15, 2021). *Trend Micro Research*. "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti." Accessed on Mar. 1, 2022, at: Link.

12 Feike Hacquebord, Stephen Hilt, and David Sancho. (Dec. 15, 2022). *Trend Micro Security News*. "The Future of Ransomware." Accessed on Mar. 1, 2022, at: Link.

13 Trend Micro Research. (Oct. 27, 2022). *Trend Micro Security News*. "Ransomware Spotlight: BlackCat." Accessed on Mar. 1, 2022, at: Link.

14 Feike Hacquebord, Stephen Hilt, and David Sancho. (Dec. 15, 2022). *Trend Micro Research*. "Ransomware Business Models: Future Pivots and Trends." Accessed on Mar. 1, 2022, at: Link.

15 Tech Target. (July 2017). *Tech Target*. "Bug Bounty Program." Accessed on Mar. 1, 2022, at: Link.

16 Ian Kenefick, Lucas Silva, and Nicole Hernandez. (Oct. 12, 2022). *Trend Micro Research*. "Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike." Accessed on Mar. 1, 2022, at: Link.

17 Junestherry Dela Cruz. (Jan. 17, 2023). *Trend Micro Research*. "Batloader Malware Abuses Legitimate Tools, Uses Obfuscated JavaScript Files in Q4 2022 Attacks." Accessed on Mar. 1, 2022, at: Link.

18 Ian Kenefick, Lucas Silva, and Nicole Hernandez. (Oct. 12, 2022). *Trend Micro Research*. "Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike." Accessed on Mar. 1, 2022, at: Link.

19 Trend Micro Research. (n.d.). *Trend Micro Research*. "What Is Apache Log4J (Log4Shell) Vulnerability?" Accessed on Mar. 1, 2022, at: Link.

20 Trend Micro Research. (n.d.). *Trend Micro Research*. "What Is Apache Log4J (Log4Shell) Vulnerability?" Accessed on Mar. 1, 2022, at: Link.

21 WP Editorial Staff. (n.d.). *WPBeginner*. "What is: Apache." Accessed on Mar. 1, 2022, at: Link.

22 VMWare. (n.d.). *Spring*. "Spring Framework." Accessed on Mar. 1, 2022, at: Link.

23 Sean Lyngaas. (Dec. 14, 2022). *CNN Politics*. "US warns hundreds of millions of devices at risk from newly revealed software vulnerability." Accessed on Mar. 1, 2022, at: Link.

24 Lily Hay Newman. (Aug. 11, 2022). *Wired*. "Sloppy Software Patches Are a 'Disturbing Trend'." Accessed on Mar. 1, 2022, at: Link.

25 Rae Hodge. (Apr. 23, 2020). *CNET*. "VPN use surges during the coronavirus lockdown, but so do security risks." Accessed on Mar. 1, 2022, at: Link.

26 David Fiser and Alfredo Oliveira. (Aug. 17, 2022). *Trend Micro Research*. "Analyzing the Hidden Danger of Environment Variables for Keeping Secrets." Accessed on Mar. 1, 2022, at: Link.

27 David Fiser and Alfredo Oliveira. (Mar. 9, 2021). *Trend Micro Research*. "TeamTNT Continues Attack on the Cloud, Targets AWS Credentials." Accessed on Mar. 1, 2022, at: Link.

28 Trend Micro. (Feb. 2, 2023). *Trend Micro Research*. "Research Exposes Azure Serverless Security Blind Spots." Accessed on Mar. 1, 2022, at: Link.

29 28. Ax Sharma. (May 24, 2022). *Bleeping Computer*. "Popular Python and PHP libraries hijacked to steal AWS keys." Accessed on Mar. 1, 2022, at: Link.

30 Trend Micro. (Jul. 13, 2022). *YouTube*. "Proof of Concept (POC): When Secrets Stored as an Environmental Variable are (Unwittingly) Leaked." Accessed on Mar. 1, 2022, at: Link.

31 Trend Micro. (Feb. 2, 2023). *Trend Micro Research*. "Research Exposes Azure Serverless Security Blind Spots." Accessed on Mar. 1, 2022, at: Link.

32 George Kalpudis. (Jan 2, 2023). *Coin Desk*. "What Will It Take for Bitcoin Mining Companies to Survive in 2023?" Accessed on Mar. 1, 2022, at: Link.

33 Alfredo Oliveira and David Fiser. (Sept. 10, 2023). *Trend Micro Research*. "War of Linux Cryptocurrency Miners: A Battle for Resources." Accessed on Mar. 1, 2022, at: Link.

34 Alfredo Oliveira and David Fiser. (Sept. 10, 2023). *Trend Micro Research*. "War of Linux Cryptocurrency Miners: A Battle for Resources." Accessed on Mar. 1, 2022, at: Link.

35 Alfredo Oliveira and David Fiser. (Dec. 1, 2022). *Trend Micro Research*. "Linux Cryptocurrency Mining Attacks Enhanced via CHAOS RAT." Accessed on Mar. 1, 2022, at: Link.

36 Liam Tung. (Jan. 17, 2022). *ZDNet*. "Linux malware is on the rise. Here are three top threats right now." Accessed on Mar. 1, 2022, at: Link.

37 Trend Micro. (Dec. 28, 2022). *Trend Micro Research*. "Improving Software Supply Chain Security." Accessed on Mar. 1, 2022, at: Link.

38 NIST. (n.d.). *NIST*. "Software Security in Supply Chains: Software Bill of Materials (SBOM)." Accessed on Mar. 1, 2022, at: Link.

如需更多資訊，請至：trendmicro.com

©2023 年版權所有。趨勢科技股份有限公司及其相關機構保留所有權利。Trend Micro、t 字球形標誌、Apex One 及 Trend Micro Apex Central 是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為該公司的商標或註冊商標。本文件之內容若有變動，恕不另行通知。[REP01_General_Report_Template_A4_221206TW]

如需有關我們蒐集哪些個人資訊的詳細內容和理由，請參閱我們網站上的「隱私權聲明」：trendmicro.com/privacy