



SONICWALL®

2024

SONICWALL  
網路威脅報告

## 執行摘要

2023 年，隨著威脅行為者繼續加大其攻擊並使其攻擊多樣化，幾乎所有追蹤計量上的網路攻擊都增加了兩到三倍。為了向世界各地的防禦者提供對抗不斷激增的網路犯罪所需的可付諸實踐的威脅情報，我們將我們的研究成果彙編到這份報告中。以下是今年最重要的調查結果預覽。

## 2023 年趨勢與發展

在 2023 年快速變化的威脅環境中，SonicWall Capture Labs 威脅研究人員觀察到了幾種全新戰術、技術和程序 (TTP)，包括使用 Microsoft OneNote 檔案作為初始媒介。還揭示了針對 WinRAR 和 MOVEit 漏洞的大規模活動，以及新的嚴重零時差漏洞，[會影響 Apache OFBIZ](#)。研究和發布這些發展是我們許諾的內容，要為我們尊貴的合作夥伴和互聯的網路安全社群賦能。

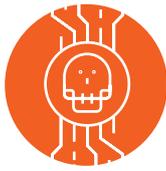
▲ 11%



### 惡意軟體

2023 年，惡意軟體攻擊數量增加 11%，達到 60.6 億次，這是自 2019 年以來攻擊量最高的一次。北美和拉丁美洲的攻擊分別增加了 15% 和 30%，抵消了亞洲和歐洲的小幅下降。

超過  
原來  
兩倍



## 加密威脅

2023 年加密攻擊增加了 117%，總數幾乎相當於 2021 年和 2022 年的總和。這一躍升由全球範圍內的增長推動：北美的攻擊增幅最小，增長 30%，而歐洲、亞洲和拉丁美洲記錄到分別激增 182%、462% 和 527%。

第3

高的  
年份  
有史以來



## 勒索軟體

2023 年夏季，勒索軟體猛增，幾乎超過了 2021 年的最高點。而 2023 年其餘時間的攻擊量較少，致使勒索軟體攻擊與去年同期比較減少 36%，但夏季激增的攻擊量足以使 2023 年成為勒索軟體攻擊第三嚴重的一年。

「以 32 年的豐富歷史為基礎，SonicWall 繼續發布網路威脅報告以提供威脅情報，不僅為了提供可付諸實踐的見解，還為了推動我們的路線圖並構建產品，以幫助我們的合作夥伴，他們需要基於最新威脅情報的經過驗證的解決方案和主動式策略。這就是為何 SonicWall 繼續發布威脅情報（含可付諸實踐的見解），以盡可能建立最強大的防禦。」

-SONICWALL 總經理兼執行長 BOB VANKIRK

下載報告

加入我們的旅程，讓世界各地的組織保持成功與安全：[sonicwall.com/partners](https://sonicwall.com/partners)

### 關於 SonicWall

SonicWall 是網路安全先行者，擁有 30 餘年專業經驗，並且持續關注其合作夥伴。憑藉跨越雲端、混合和傳統環境即時構建、擴展和管理安全的能力，SonicWall 可以快速、經濟地為全球任何組織提供專門構建的安全解決方案。SonicWall 基於其自身威脅研究中心的資料，提供無縫防護，防範十分隱蔽的網路攻擊，並向合作夥伴、客戶和我們的網路安全社群提供可付諸實踐的威脅情報。

作為最佳做法，SonicWall 會定期優化其資料收集、分析和報告方法。這包括資料清理改進、資料來源變更以及威脅摘要整合。可能會跨越不同時間段、地區或行業調整以往報告中公佈的數據。

SonicWall, Inc.  
1033 McCarthy Boulevard | Milpitas, CA 95035



SONICWALL®

© 2024 SonicWall Inc. 著作權所有。

SonicWall 係 SonicWall Inc. 及/或其關係企業在美國及/或其他國家/地區之商標或註冊商標。所有其他商標與註冊商標均係其各自擁有者之財產。本文件中之資訊係根據 SonicWall Inc. 及/或其關係企業之產品而提供。未透過本文件或根據 SonicWall 產品銷售情況，以禁反言或其他方式向任何智慧財產權予以任何明示或默示之授權。

10.24 - 2024 SonicWall Cyber Threat Report - Executive Summary