

# 管理人週報

HR WEEKLY UPDATES



626.333.1111 哈崗 · 鑽石吧 · 聖蓋博 · 爾灣 · 喜瑞都 · 安大略

## 焦點：勒索軟件攻擊在 2020 年第 4 季達到歷史最高峰

由於 COVID-19 造成的恐慌和混亂，加上遠程工作的過渡，2020 年勒索軟件攻擊激增，為網絡犯罪提供了大量契機。Advisen 的數據顯示，勒索軟件攻擊在 2020 年達到歷史最高峰，尤其是對製造業公司的攻擊。

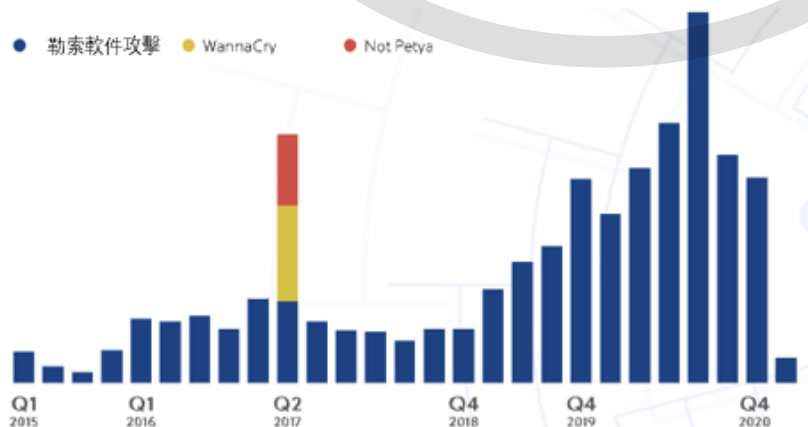
Advisen 的數據庫顯示，在 2020 年第四季達到有記錄以來的最高峰之前，2020 年第三季的勒索軟件攻擊次數與 2017 年第二季遭受全球 WannaCry 和 NotPetya 攻擊的次數相當。2020 年第一季勒索軟件攻擊減少可能是由於數據滯後，並不意味著攻擊頻率的真正減少。隨著數據蒐集工作的繼續展開，這些數字還會增加。

2020 年和 2021 年初，醫療保健、製造業和公共管理領域遭受的攻擊占所有勒索軟件攻擊的一半。這與 2019 年相比發生了變化，當時公共管理和教育服務領域是面臨勒索軟件攻擊的主要行業。根據 Advisen 的數據，2018 年，公共管理和醫療保健領域遭受攻擊的頻率最高。

這些攻擊造成的業務中斷損失可能相當嚴重，導致一些公司不得不支付極高的贖金，使其業務恢復運營。

例如，美國化學公司 Hexion 在 2019 年 3 月遭到勒索軟件攻擊，導致其整個全球網絡被關閉。根據 Advisen 的數據，該公司因該事件遭受了 1700 萬美元的成本損失。

### 勒索軟件攻擊、頻率



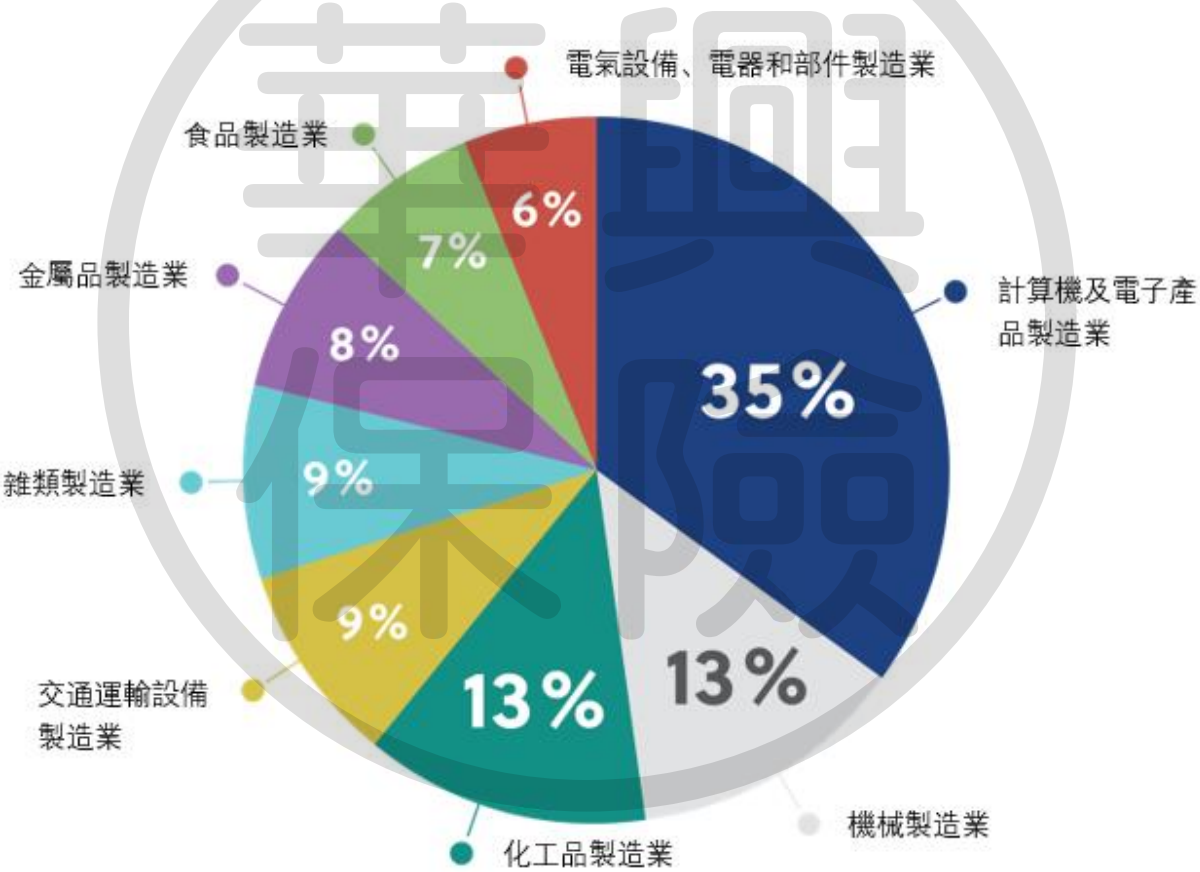
在 Advisen 的數據庫中，2020 年製造業遭受勒索軟件攻擊的高頻率是前所未有的，是之前所有年份所遭受的勒索軟件攻擊的頻率的兩倍以上（包括 2017 年的 WannaCry 勒索軟件攻擊）。

從 2020 年製造業公司遭受的勒索軟件攻擊來看，電腦和電子產品製造業的損失占比最大。該行業包括電子芯片製造商、筆記型電腦製造商和武器製造商等。

例如，根據 Advisen 的數據，國防和通信行業的主要電子產品製造商 Communications & Power Industries (CPI) 因勒索軟件攻擊而離線，被迫支付約 50 萬美元的贖金。CPI 為軍事設備和裝備製造零件，如雷達、導彈引導頭和電子對抗技術。

2020 年，機械製造業和化工品製造業各占剩餘勒索軟件攻擊的 13%。2020 年面臨勒索軟件攻擊的機械製造企業包括鑽孔產品製造商、洗浴用品製造商和工業機器人製造商。根據 Advisen，2020 年面臨勒索軟件攻擊的化工品製造商包括製藥商、醫療技術開發商和一家基因製造公司。

**2020 年製造業面臨的勒索軟件攻擊、頻率**



\* Advisen 的數據來自各種公共資源。我們主要蒐集大案和要案的數據。因此，本文中的數據可能不能完全代表這類案件的所有情況。