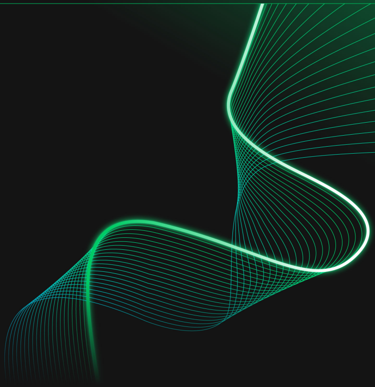
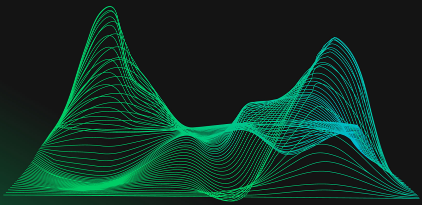
全球攻擊範圍現狀

分析觀察到的掃描數據而非自我報告調查的 5 項重大發現





現代化攻擊範圍的本質

現代化攻擊範圍本質上會持續不斷變動。攻擊範圍具有獨特、持續和不斷擴大的特性—新問題不斷在各個產業出現。

雖然這感覺像是艱苦的戰鬥，不過強化 SecOps 彈性有助於了解您面臨的挑戰。

全球攻擊範圍分析的 5 項發現

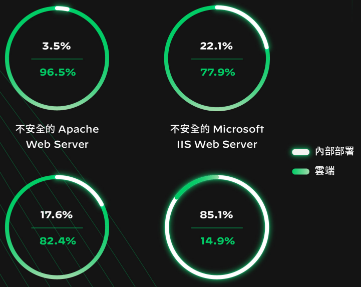
1

攻擊回應需要明確掌握部署現況

雲端可能很容易部署，不過卻對安全性帶來新的挑戰。重要的是如果沒有完整且持續的可視性，企業就無法做出回應。

關於雲端與內部部署之間的四種最近問題類型*，安全弱點的等級取決於您的伺服器。

內部部署與雲端安全問題 (依伺服器)



F5 BIG-IP TMUI

不安全的 Microsoft
Exchange Servers

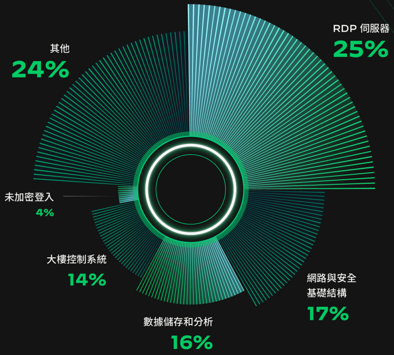
2

由於企業關注弱點，暴露更容易遭到利用

企業經常無法保護許多可防範的暴露。攻擊者只需要在網際網路上掃描遭到暴露或設定錯誤的資產或服務。

常見的攻擊範圍風險：
- 暴露的 RDP 伺服器
- 暴露的系統管理登入入口網站
- 未加密的登入頁面
- 執行達到使用壽命 (EOL) 的軟體
- 執行未修補的軟體版本

全球攻擊範圍的風險分佈



3

各個產業風險最高的暴露

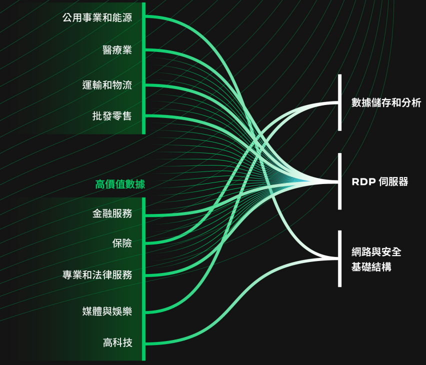
營運中斷

每個企業都有獨特的暴露

攻擊者可能以某些企業為目標的一般原因有兩個：

- 營運中斷
- 竊取高價值數據

了解最常見的風險有助於專注處理。全面了解您的產業所面臨的風險可以建立全面的潛在暴露目錄。



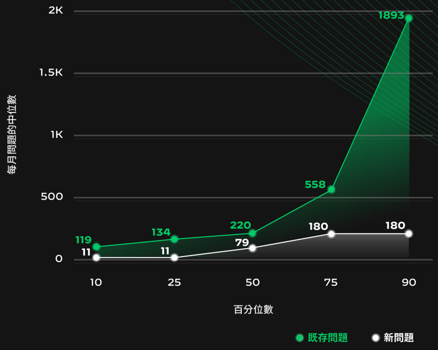
4

沒有一種產業可以免於遭受攻擊

對於安全從業人員來說，工作永遠沒有完成的一天。

做不完的工作會變成不斷累積的問題和暴露，最後造成不受管理的攻擊範圍更加擴大。

醫療業中各公司每月不安全的 Apache Web Server 既存問題和新問題的中位數



我們的研究顯示，無論哪種產業，新問題都會持續存在，並且根據我們的研究，沒有任何一種產業能成功縮小其攻擊範圍。

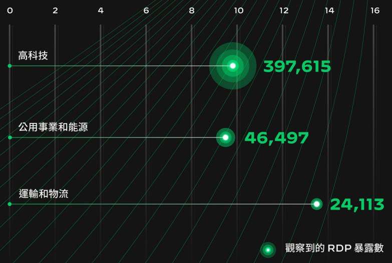
5

重大票證：RDP 暴露會增加網路攻擊風險

根據 2022 Unit 42 勒索軟體威脅報告，主要針對 RDP 的暴力破解攻擊是所有案例數據中排名前三的初始存取途徑之一。

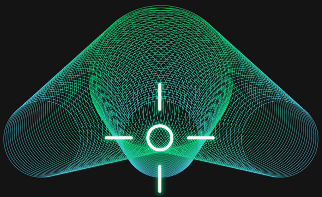
在網路安全性中，攻擊者只需要成功一次，因此即使暴露個幾天也是很大的風險。

RDP 暴露在公用網際網路的平均天數



觀察期間內暴露在公用網際網路的 RDP 執行個體數量，以及在任何特定月份中暴露的 RDP 執行個體發生平均天數。任何一天的暴露都可能導致毀滅性的後果。

*在我們的 2021 年全球攻擊範圍初始研究中，我們著重在數個聯邦顧問所提及並經觀察曾遭到大肆入侵的四種特定弱點上：
- 不安全的 Apache Web Server
- F5 BIG-IP TMUI
- 不安全的 Microsoft Exchange Server
- 不安全的 Microsoft IIS 網路伺服器



先暴露，後弱點

導致產業暴露的問題並不侷限於零時差弱點。我們的分析顯示，廣泛使用的軟體和服務 (例如 RDP) 或暴露的管理員登入入口網站中常見的暴露會導致企業暴露。

真正的重點是設法支援 SecOps 團隊，因為這些人必須盡力達成持續變化的目標。

了解如何深入探究全球攻擊範圍的現狀來縮小攻擊範圍並且增強 SecOps 團隊的能力。

閱讀 2022 年 Cortex Xpanse 攻擊範圍威脅報告

關於全球攻擊範圍現狀的重大發現是根據觀察到的掃描數據，而不是自我報告的調查。我們監控針對與 100 多家全球企業有關的 5000 萬個 IP 位址 (超過整個網際網路的 1%) 進行的掃描。我們收集 2021 年 3 月至 2021 年 9 月以及 2021 年 12 月至 2022 年 6 月的數據。