Radware DDoS 防護解決方案-政府部門

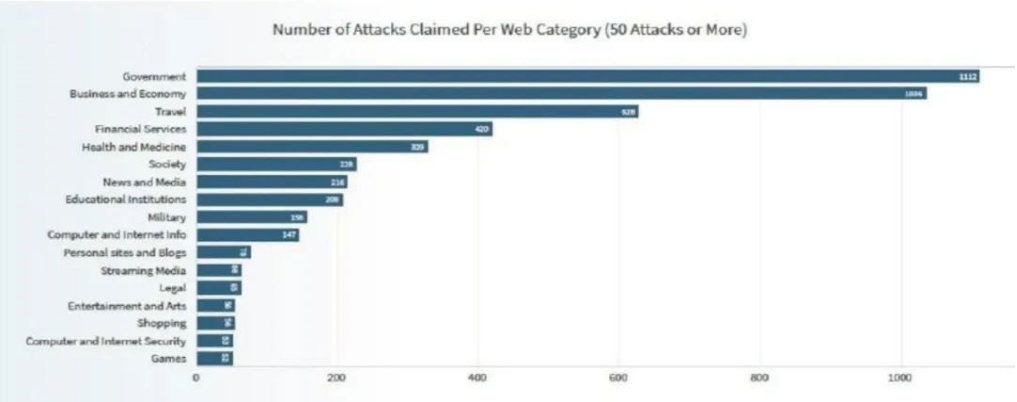
隨著政府服務日益數位化，與 DDoS 防護相關的挑戰和擔憂也逐漸加劇。DDoS 攻擊造成的中斷可能會阻礙公眾訪問政府資源，阻礙應急回應系統，並破壞公眾對政府提供可靠服務能力的信任。

因此，為了維護民主進程的完整性，保護關鍵任務系統的可用性，政府部門需要面對複雜的挑戰，來抵禦日益複雜和持續的 DDoS 威脅。

針對政府部門的 DDoS 攻擊

近年來，DDoS 攻擊目標已擴大至政府部門、民用基礎設施和非營利組織。

根據 Radware 發佈的 H1/2023 威脅分析報告顯示，在 2023 年上半年，僅政府和國家機構就遭受了 1000 多次駭客組織的 DDoS 攻擊。



- **關鍵服務中斷：** DDoS 攻擊可以使政府網站、通信管道和線上服務超載，造成嚴重的中斷。
- **阻礙應急回應:** DDoS 攻擊會阻礙應急回應系統的運作，阻礙政府在危機、自然災害或安全事件期間提供援助的能力。
- **破壞公眾信任：** 政府網站或線上服務的中斷，會削弱公眾對政府提供基本服務的可靠性和能力的信任。
- **對資料安全的威脅：** DDoS 攻擊可以轉移注意力，讓網路犯罪分子利用漏洞破壞政府系統。
- **國家安全風險：** 針對政府部門的 DDoS 攻擊會對國家安全造成深遠的影響。通信管道中斷和資料受損可能會阻礙政府部門之間的協調，並阻礙國家對於國際威脅的反應。

Radware DDoS 防護解決方案

Radware 為政府部門提供全面且量身定制的 DDoS 解決方案，以下是 Radware DDoS 防護解決方案的主要優勢:

- **精准識別並緩解 DDoS 攻擊**：Radware 解決方案提供已知和零日 DDoS 攻擊的即時檢測和風險緩解，確保政府部門的網路和服務保持可訪問性和彈性。通過利用行為分析和機器學習等尖端技術，Radware 解決方案可以準確識別和緩解 DDoS 威脅。
- **可擴展和彈性基礎設施：**Radware DDoS 防護服務可以處理大容量 DDoS 攻擊而不會使服務中斷。Radware 通過全球分佈的清洗中心和智慧引流機制，確保合法流量通過，同時有效過濾惡意流量。
- **低誤報率：**Radware 基於行為的檢測，使用先進的專利機器學習演算法來防範已知和未知的威脅。自動區分合法流量和攻擊流量。這使得檢測更加準確，誤報率更低。
- **靈活部署：**Radware 可提供多種部署選項，包括本地部署、雲服務，以及混合解決方案。
- **高級 Web DDoS 防護**：Radware 的 Web DDoS 防護採用先進的 L7 行為基礎檢測和緩解技術，以阻止威脅到 Web 和移動應用可用性的複雜 Web DDoS 海嘯級攻擊。
- **集成的網路和應用防護：**Radware 的 DDoS 防護集成在一個雲解決方案中，因此客戶可以通過一個集成的解決方案，來滿足所有基礎設施和應用防護需求。
- **即時威脅情報：**Radware DDoS 防護通過多個威脅情報源進行增強，資料來源自 Radware 雲清洗中心及誘捕網路，主動檢測到攻擊者並在其對客戶造成影響之前發現他們。
- **全面的報告和分析：**Radware 解決方案提供詳細的報告和分析功能，為政府部門提供有關攻擊趨勢、攻擊風險緩解效果和網路性能的詳細分析。

Radware DDoS 防護解決方案提供全面管理服務，並由 Radware 應急回應團隊(ERT)提供支援。

Radware Cloud DDoS 防護服務覆蓋全球 19 個清洗中心，具有 12 Tbps 的風險緩解能力(並且還在不斷增長)。Radware 清洗中心進行全球連接路由，確保 DDoS 攻擊在最接近其起源點的地方得到緩解，並提供真正的全球 DDoS 風險緩解，甚至能夠吸收更大容量的攻擊。

Radware 台灣

電話：+886 2 2697-6318 | 傳真：+886 2 2697-6319 | 電郵：TW_Marketing@radware.com

如欲了解更多，請造訪：www.radware.com