eASPNet

網頁應用程式防火牆
方案簡介

數位通國際

Version 2020

網站安全事件頻傳

網站安全攸關企業的營運、資料、交易及形象

進行網站安全防護的困難

原廠本身漏洞
無法自行修改

運行中的架構
調整不易

系統老舊無法
修正漏洞

資安威脅手法
日益複雜

WAF對網站安全防護的效益

原廠本身漏洞
無法自行修改

運行中的架構
調整不易

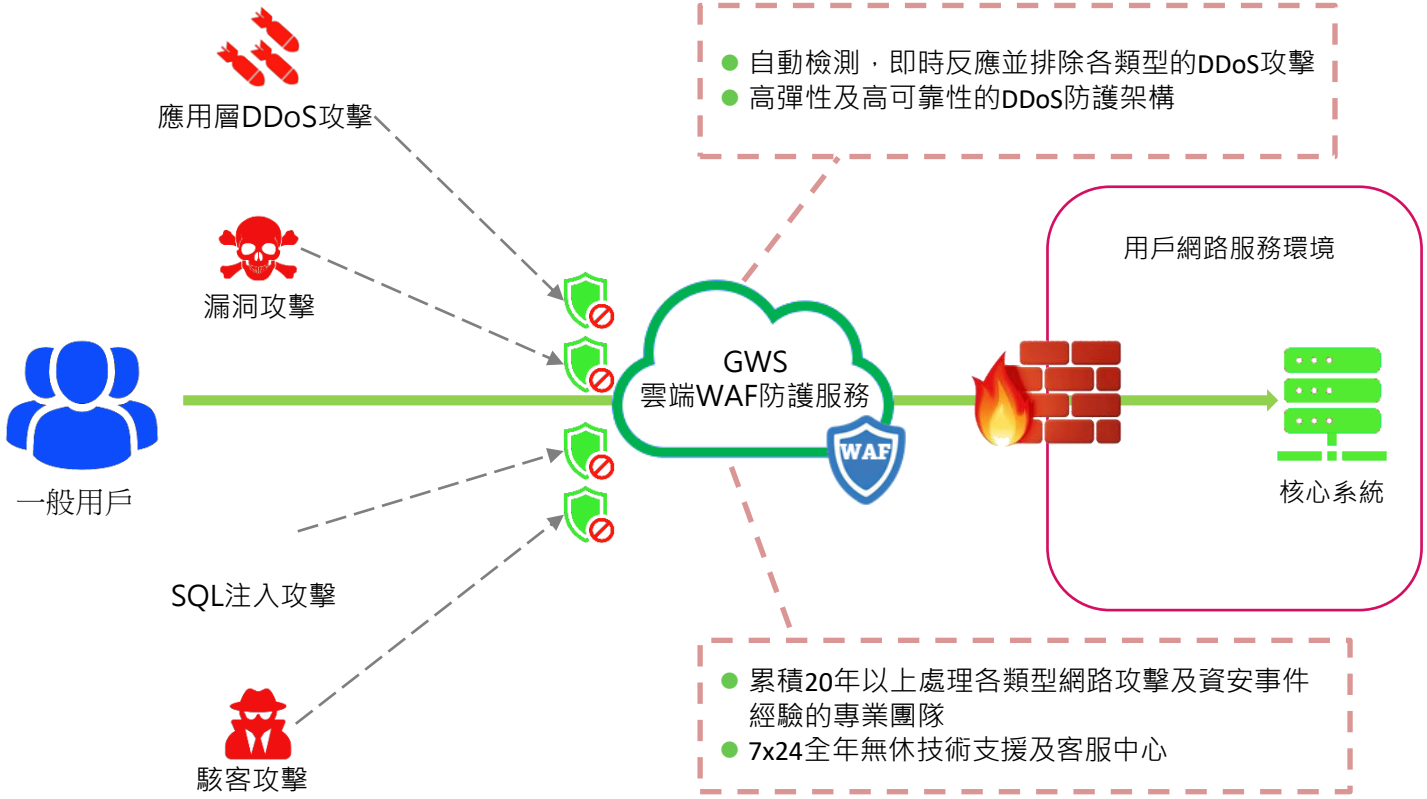
系統老舊無法
修正漏洞

資安威脅手法
日益複雜

WAF 功能	可針對原廠漏洞問題 提供暫時性的防護措施	可針對現有漏洞問題 設定專屬的防護規則	透過機器學習與行為分析，防護未知攻擊

達到保護企業資產
避免損失的目標

GWS 雲端WAF防護服務



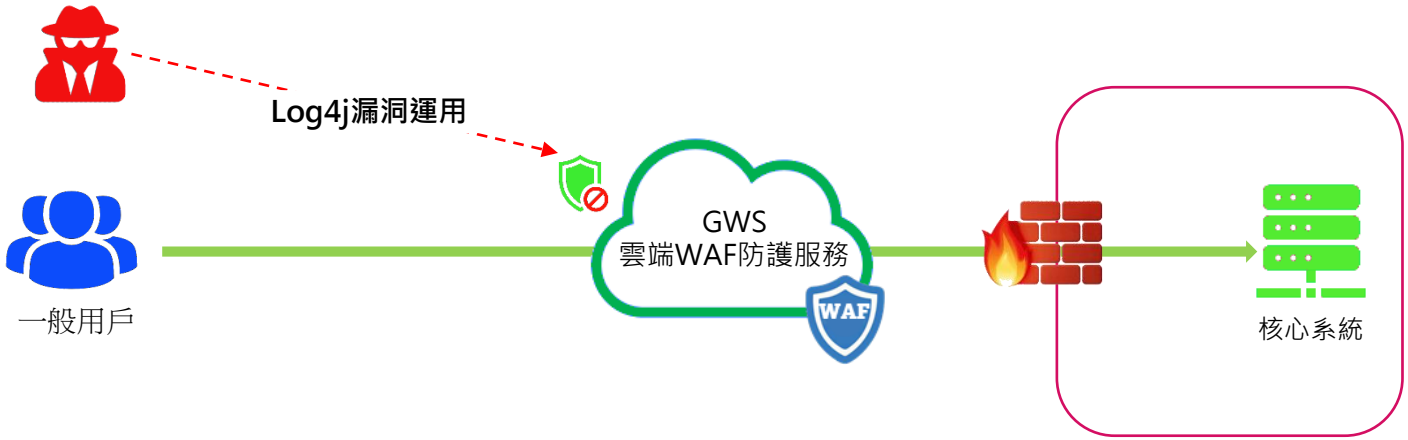
實際案例介紹_Log4j

2021年12月網路上揭漏十年最危險的資安漏洞之一。這個名為「Log4j」(或Log4Shell) 的開放原始碼軟體漏洞，因為 Log4j被使用於Java語言、網站伺服器及網路應用的紀錄方案, 因此它的影響遍及各種企業廣泛採用的應用程式和服務，包括：蘋果iCloud、微軟Azure、Amazon、Google等，以及Oracle、IBM、Red Hat、Vmware、Cisco、Splunk 等等.....

實際運用介紹_ Log4j防護

針對特徵碼進行防護，將以下幾項特徵加入WAF防護規則中，可緩解Log4j造成的影響

- Log4j 標頭
- Log4j 主體
- Log4j 網址



實際運用介紹_撞庫攻擊

駭客使用撞庫攻擊行為模式如下:

1.透過不法方式取得外洩之帳密個資

2.使用自動化程式針對特定網站進行帳密驗站(撞庫攻擊)

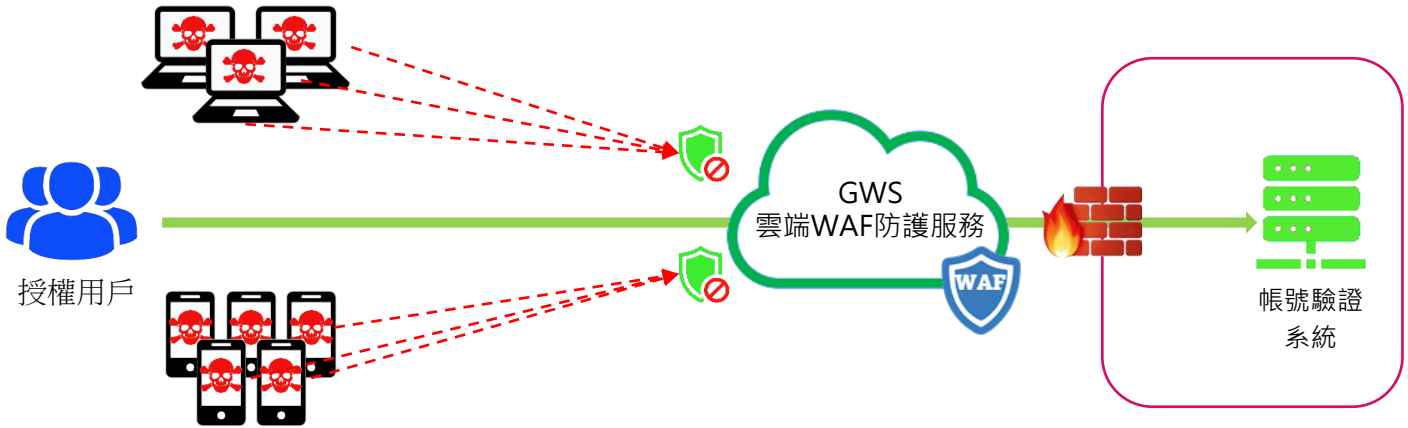
3.透過撞庫取得可驗證成功之帳號及個資

4.使用成功驗證之帳號個資，登入應用系統，進行不法利益行為及破壞

實際運用介紹_撞庫攻擊

針對行為進行防護

- 對單一帳號透過多個不同IP嘗試登入
- 對單一IP使用多個帳號進行嘗試登入
- 利用機器學習方式精準辨識自動化及爬蟲行為，防止駭客進行帳號驗證動作




Thank You
0800-880-668
cs@easpnet.com
www.easpnet.com
eASPNet