優勢總結

近來的網路釣魚、詐騙等安全事件造成損失頻傳，若能善用域名過濾和防禦方案，將能有效減少威脅來源。iSafer DNS Booster是業界首先在終端用戶域名連線的活動管理過程中，整合全球威脅情報的防護機制，保障終端用戶在安全條件下存取資訊及服務，進而大幅降低企業遭受網路惡意威脅的風險，提高工作生產效率與安全；同時，也突破傳統域名系統在運作管理上衆多的盲點與效率性，以面對未來應用即服務對於連線品質和用戶使用體驗的嚴峻挑戰。

iSafer爲您的企業網路安全扮演不可或缺的得力幫手!

域名系統安全威脅影響

DNS (Domain Name System,域名系統)是網際網路的主要索引，作用如同是一本世界級的電話簿但儲存的是域名或IP。對所有組織和企業來說DNS是必要的，但卻只有少數組織有針對DNS執行防護與監控的政策機制。

全球雲端活動愈加活躍，網路資安威脅事件中DNS就經常被駭客所利用，藉由滲透進入受害組織網站內以進行不法的行爲，此現象亦是暴增。近幾年來DNS已成爲惡意程式攻擊和資料洩漏的新途徑，當DNS的安全失守不僅是影響使用者上網的行爲造成困擾，而是會整體影響公司的商業信用。當組織官網無法瀏覽，企業內部營運郵件無法收發，此刻除了對外進行溝通受阻外，外部對於企業組織的形象觀感指數也隨之下降。

而駭客對企業和政府組織的DNS(Domain Name System)發動攻擊無外乎有以下種動機和利益：

敲詐勒索：駭客利用DNS攻擊將受害組織的網站或服務暫時關閉，然後向該組織提出贖金要求，以恢復正常運營。這種攻擊通常稱爲「勒索攻擊」，並且可以對組織造成極大的經濟損失。

惡意破壞：某些駭客可能出於惡意、報復或政治目的，對企業或政府組織的DNS進行攻擊，以破壞其網路運營或服務。這可能會導致網站無法訪問，對外部用戶造成困擾，或破壞組織的聲譽。

盜取敏感信息：通過DNS攻擊，駭客可以截取網路流量或修改DNS解析結果，將用戶重新定向到惡意網站。這樣的攻擊可能用於竊取敏感信息，如登錄憑據、金融帳號、個人身份資訊。

進行釣魚攻擊：駭客可能通過DNS攻擊來進行釣魚攻擊。他們可能使用僞造的網站或DNS解析結果來欺騙用戶，引導他們提供敏感資訊，如密碼或信用卡詳細內容。

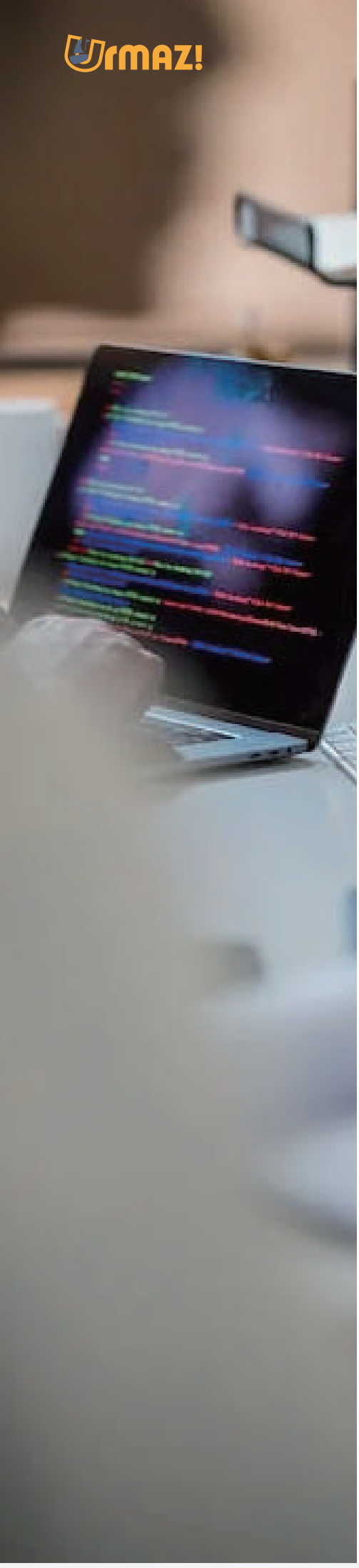
除此之外仍有一些未被重視，但逐漸浮現的威脅如：

新域名威脅

作爲域名系統 (DNS) 的一部分，每天都會創建和發佈新的網域，但並非所有域名都是出於合法目的而創建的。域名管理機構無法得知創建動機且也無從預知危險，因而惡意行爲者會在創建新域名的最初幾分鐘內使用新域名進行垃圾郵件、惡意軟體發散、殭屍網路等犯罪活動。

短網址威脅

短網址可以用於隱藏惡意鏈接，駭客可能發送包含短網址的釣魚郵件或訊息，這些網址將指向旨在竊取敏感資訊或散發惡意軟體的僞造網站。而攻擊者可以利用短網址或域名冒充特定品牌或知名網站/服務。他們可能創建與合法網站極爲相似的虛假網址或網站，欺騙用戶提供敏感信息或安裝惡意軟體。攻擊者可以利用縮短的網址或新註冊的域名與感染惡意軟件的系統建立通信通道。這些網址或域名可能充當命令和控制伺服器，使攻擊者能夠遠端控制受影響的設備、外洩數據或進行更多的攻擊。



目前全球制定了一些相關的安全防禦規範和最佳實踐，以應對DNS攻擊。以下是其中一些重要的規範：

- **DNSSEC（Domain Name System Security Extensions）：**DNSSEC是一項安全擴展，通過使用公鑰加密和數字簽名來保護DNS解析的完整性和眞實性。它能夠防止DNS緩存中毒、資料竄改和僞造的DNS回答。

- **DANE（DNS-Based Authentication of Named Entities）：**DANE利用DNSSEC來確保安全通信的憑證眞實性。它將憑證信息嵌入到DNS記錄中，用於驗證TLS/SSL憑證的有效性，以增強網絡安全。

- **RPZ（Response Policy Zones）：**RPZ是一種DNS防火牆技術，可以對特定的域名或IP地址進行黑名單或白名單設置，從而阻止或限制對這些資源的訪問。

以上是一些DNS安全威脅的例子與參考規範，突顯了DNS安全對組織可能產生的影響。爲了緩解這些威脅，組織應該實施DNS安全措施，例如使用安全的DNS解析器、實施DNSSEC（DNS安全擴展）、監控DNS流量以檢測異常情況，並保持強大的DNS安全實踐和配置。

iSafer是URMAZI專門設計用於域名系統進階管理及安全威脅防禦的解決方案，這是一套可支援在虛擬化環境中安裝的軟體平台。有鑑於衆多的企業IT資源有限而採用一般開源的軟體架構其域名系統，無論是管理功能陽春以及欠缺安全防禦機制，不僅難以匹配現代寬頻網路的靈活應用度以及保有相關的活動軌跡紀錄，更是無法應付多變的網路惡意攻擊行爲，極容易因用戶終端缺乏安全辨識能力而主動引入攻擊威脅，造成企業資產和信譽的巨大損失。iSafer就是從終端DNS管理著手，爲您企業解決上述困難最佳的標靶工具。

此外，iSafer結合了URMAZI專屬的安全研究學院(USRA)的情資內容，這是基於域名內容以深度學習及人工智慧的技術探探出連線行爲的數據資訊加以分析、歸類與預測的加值服務。主動將強烈威脅性如Botnet、Phishing、Scam的連線進行阻斷保護，以及其他55種類別行爲域名的解析數據庫，有效強化組織終端用戶上網連線安全和更準確的行爲資訊，協助IT管理者和經營決策者爲其企業組織打造更先進更安全也更有競爭性的網路服務，保護資產以及創造更高生產營收。

iSafer DNS Booster 應用優勢不僅是以提升企業DNS服務效率爲限，還包含其他更多高階管理機制及安全防護功能：

活動日誌

iSafer自動封存保留七日內以及最近五分鍾內的域名詢答日誌，並區分新列入觀察或回應的活動列表，提供網管人員在需要時能回溯查找，快速地定位並縮小問題範圍。

服務多重定址

面對全球化競爭，服務的穩定性及不中斷性是企業服務最重要的一環；iSafer具備健康檢查機制，全時偵測服務主機的連線狀態，並搭配演算技術適當分配處理進入服務主機流量，不僅大幅降低因線路故障導致無法連線到服務的風險，同時藉由負載均衡的功能也能增強web services 的運作效率，保護服務伺服器的資源不被消耗殆盡。

黑名單政策

可使用檔案匯入，限制境內外惡意網域名稱或IP位址，作爲資安防護的第一線防衛措施。越來越多惡意程式及殭屍裝置利用DNS查詢C&C伺服器，黑名單政策讓管理者自訂阻擋的網域名稱和查詢回應位址，避免使用者接取惡意或不當的網域名稱或IP位址。

支援DNSSEC

單鍵啟用或自行匯入密鑰，確保網域名稱記錄的內容正確性。當查詢者使用DNSSEC協定時，將會取得查詢記錄的對應內容以及該內容的簽章，確保取得的內容未被惡意變更，避免使用者連線到有問題的目的，導致資料外洩或被植入惡意程式。

