URMAZI

White Paper

iSafer DNS
活動紀錄的十大跡象

▶ 關於DNS

企業爲保護其數位資產和網路通訊，普遍性都會建置防火牆作爲內外的安全隔離，同時也會自主保留連線和安全事件紀錄以掌握屬於組織的資安情報。

但身爲維繫所有Internet服務運作的域名系統 (Domain Name System)，無論您是採用Microsoft或是開源的BIND作爲架構企業組織的域名系統，雖然系統足戡穩定，但對於IT管理均存在相同的資安合規性問題，就是缺乏詳盡且容易判讀的DNS活動紀錄。以致於每當資安事件發生時將難以溯源調查，甚至擬定安全預防策略使得企業暴露在攻擊風險之中；倘若能完整保留DNS查詢和回應記錄，將是提供有關潛在安全威脅的有利資訊，包括正常和高風險威脅的訪問內容和方式。

 | www.urmazi.com | 台北市中正區忠孝西路一段80號16樓 | SF-WP-31106

URMAZI!

White Paper

基於DNS記錄對於識別高風險威脅訪問的一些具體跡象

- **異常查詢模式**
  查找DNS流量中的異常查詢模式，例如對特定域名的異常高查詢次數或頻繁請求不存在的網域（查詢結果爲NXDOMAIN）。這些模式可能代表惡意活動，如惡意軟體利用域名生成演算法（DGA）。

- **黑名單域名**
  維護已知的惡意或高風險域名列表，並即時將DNS查詢記錄與該列表進行比對。如果觀察到DNS查詢涉及黑名單中的域名，那麼這即是潛在高風險威脅的明顯跡象。

- **異常頂級域名(TDL)**
  注意DNS查詢中不常見或可疑的頂級域名（TLD）。惡意域名通常使用較不常見的TLD，例如.xyz或.info，以逃避常規安全檢測。頻繁查詢此類TLD可能是警告信號。

- **快速變換或域名翻轉**
  監控與快速變換或域名翻轉技術相關的域名的DNS記錄。惡意行爲者常常使用這些策略迅速更改與域名關聯的IP地址，以隱藏其惡意活動。

- **異常的查詢流量**
  DNS查詢流量突然增加或對特定域名的過度DNS流量可能會是分佈式拒絕服務（DDoS）攻擊或參與僵屍網路的受感染系統。

- **查詢失敗**
  頻繁的DNS查詢失敗，表明該來源可能正在進行DNS查詢探測，確認是否有設定錯誤或防護機制，以便進一步滲透和入侵。

- **過長或可疑的子域名**
  分析DNS查詢中的子域名。查找過長或可疑的子域名字符串，因爲它們可能用於混淆惡意活動。例如，子域名如"login.paypal.com.malicious.com"可能表明釣魚行爲。

- **反向DNS查找**
  對來自您網路的DNS查詢的IP地址執行反向DNS查找。檢查IP地址是否對應於已知的惡意服務器或與可疑活動相關。

- **DNS隧道**
  DNS隧道是惡意軟體用於秘密洩露數據的一種技術。監視具有異常長負載或不尋常字符的DNS查詢，因爲它們可能與數據洩露的相關。

- **時間和地理位置**
  分析DNS查詢的時間和地理位置。突然出現在意外位置或不尋常時間發起的DNS查詢可能表明惡意活動或受感染設備。

要有效地使用DNS記錄識別正常和高風險威脅，可導入 iSafer DNS安全解決方案以幫助企業組織自動化檢測異常連線情況、提供即時告警並就DNS流量內容進行統計分析，不僅能即時識別潛在威脅加以阻擋保護，多元的圖表數據還提供IT部門精確的活動可視度，作爲後續管控策略訂定的技術依據以及符合資安法規的相關佐證標準。此外，保持DNS威脅情報源的最新性可以進一步增強您即時檢測和應對高風險威脅的能力。

關於URMAZI Networks Inc.

我們是專精於以網域系統(DNS)爲基礎的資通安全防禦方案的開發團隊，豐富的外商網路安全整合應用經驗。有鑑於網域與線上服務緊密的連鎖關係和威脅影響，開啟我們著手打造符合且眞實解決企業資通安全需要的產品-iSafer。同時，爲能更快速地反應對於未知威脅的前期偵測，我們利用深度學習與人工智慧技術設立專屬的USRA研究小組，提早建立預警情資數據並與全球相關組織進行交換，URMAZI將是您最值得信賴的合作夥伴。

Further Together

 | www.urmazi.com | 台北市中正區忠孝西路一段80號16樓 | SF-WP-31106