radware

2021-2022年 全球威脅 分析報告 執行摘要

Radware 2021 年威脅報告檢視當年最重要的網路安全事件，並提供關於 2021 年攻擊活動的詳盡深入見解。報告中利用 Radware 威脅情報團隊提供的情報，以及蒐集自 Radware 雲端與管理服務、Radware 全球欺敵網路與 Radware 威脅研究團隊的網路與應用程式攻擊活動。

DDOS 攻擊

Radware 雲端 DDoS 服務每日平均可防禦 1,591 次攻擊。2021 年共防禦了 580,766 次攻擊。多數的分散式阻斷服務 (簡稱 DDoS) 活動集中在年中。在 2021 年 6 月的最初兩週單日的平均攻擊次數明顯更高，並在 2021 年 7 月10 日達到最多的 9,824 次攻擊。2021 年上半年呈逐漸增加的趨勢，到了下半年則有逐漸減少的趨勢。上半年防禦的攻擊次數幾乎等同於下半年防禦的攻擊次數。

從 2020 年到 2021 年，每位顧客封鎖的惡意事件成長了 37%。每位顧客的平均攻擊流量成長了 26%。平均來說，每位顧客的封鎖流量為 6.49TB。在 2021 年，一次 DDoS 攻擊的平均流量為 5.69 GB。最大攻擊紀錄出現在第 4 季，達到520Gbps 的規模。

儘管較不常見，但 2021 年曾有大型雲端供應商通報了數次百萬兆位元層級的攻擊。Microsoft Azure 在第 4 季通報有紀錄以來的最大 DDoS 攻擊，達到 3.47Tbps 的規模。在同一個季度，Microsoft 又再經歷了兩次超過 2.5Tbps 的攻擊。

隨著企業將重要資源與應用程式遷移至公用雲，攻擊者為了配合公用雲供應商的規模，勢必將會調整其策略與技術。儘管企業不必因為這些大規模攻擊報告而立刻感到驚慌，卻確實需要充分瞭解，不論企業的地理位置或產業為何，DDoS 攻擊就是其威脅情勢的一部分。因此，每當在使用或讓服務及應用程式接觸到網路時，企業都該實施包含 DDoS 防禦的保護措施。

在頻寬與資源為了正當企業而增加的同時，也在為威脅發動者增加了頻寬與資源；可以合理假設惡意發動者也能像其攻擊目標一樣迅速向上升級擴充。在公用雲中代管的服務將需要考量雲端規模攻擊。

多兆位元攻擊不一定會比多次的 100Gbps 攻擊更有效果或危險。2022 年初在安道爾舉行 Twitch Rivals 錦標賽 SquidCraft Games 活動期間，就有一個小於 100Gbps 的 DDoS 攻擊中斷其全國網路連線，並持續了數小時。那次攻擊是由針對該活動的個人或團體，透過付費訂閱的受僱型 DDoS 服務而發動。

微型洪水與應用層攻擊的趨勢更令人擔憂。我們注意到，在 2020-2021 年間，超過 10Gbps 的大規模攻擊次數稍微下降 (5%) (請參見在「大型攻擊媒介」中的「攻擊媒介及應用程式」部分)，而小於1Gbps 的攻擊則增加了近 80% (請參見在「微型洪水」中的「攻擊媒介及應用程式」部分)。微型洪水與較慢速攻擊 (如應用層攻擊) 可以不被偵測到而發動，並且會耗用資源。企業冒著必須時常增加基礎架構資源的風險，例如頻寬、網路與伺服器處理，直到服務使價格變得過高。要偵測到應用層攻擊，通常必須使用比偵測網路層洪水攻擊的更多資源。

地理位置與產業

在 2021 年，歐洲、中東與非洲 (EMEA) 及美洲共封鎖了40% 的攻擊，而亞太地區則封鎖了 20%。2021 年最常遭受攻擊的產業包括電玩、零售、政府、醫療保健、技術與金融。電子商務與電玩、零售與技術產業的顧客見證了數量增加最多的 DoS 事件與攻擊。政府、醫療保健、研究與教育產業的顧客則經歷了規模增加最大的攻擊。在 2020-2021 年間，針對研究與教育、政府及零售業的各 DoS 事件數量增加了數倍。這個增加情形可能表示策略有所變化：在過去都是隨機攻擊，現在則是將攻擊作為更有目標、更有系統的活動的一部分。

攻擊媒介

根據 Radware 紀錄，相較於 2020 年，在 2021 年大於 10Gbps 的攻擊媒介稍微減少 (5%)，中等攻擊媒介增加了 39%，而微型洪水攻擊則急劇增加了 79%。

在 2021 年第 1 季，平均每 1,000 個攻擊顧客的攻擊媒介中，有 10.8 個攻擊媒介大於 1Gbps；到了 2021 年第 4 季則降至4.93。在 2021 年第 2 季，顧客發現每 1,000 個攻擊媒介中，就有 3.31 個攻擊媒介大於 10Gbps。每 3,000 個攻擊顧客的攻擊媒介中，只有不到一個大於 100Gbps。

NTP、DNS 與 SSDP 是 2021 年最常利用的放大協定 。NTP 也是 Radware 全球欺敵網路中受掃描次數第二多的 UDP 連接埠。Memcached、LDAP、SSDP、SNMP 與 mDNS 都是受歡迎的 DDoS 反射與放大協定，也是欺敵網路紀錄中受掃描次數最多的前 10 個 UDP 連接埠。

受到利用的攻擊媒介，其多樣性會隨著攻擊媒介的規模增加而減少。平均的封包大小會隨著攻擊媒介的規模而增加。攻擊媒介數量變多，攻擊媒介的平均持續時間也會跟著增加，並且會從幾分鐘的微型洪水攻擊變成持續一小時且流量大於 100Gbps 的攻擊媒介。因此，攻擊媒介數量變多也是造成 2021 年有最多防禦量的原因。

根據 2021 年的紀錄，96% 的攻擊媒介都小於 10Mbps，而其產生的攻擊只占 2021 年總攻擊量的 0.3%。在 2021 年，60 % 的攻擊都來自 10Gbps-100Gbps 的攻擊媒介。大於 100Mbps 的攻擊媒介僅占 2021 年紀錄中所有攻擊媒介的 0.8%。

吞吐量少於 10Mbps 的 TCP 攻擊媒介會產生平均最大數量，且持續時間最長，而攻擊媒介大於 10Mbps 的 UDP 攻擊則有最大吞吐量與最長的持續時間。
TCP 攻擊媒介會造成最快的封包速率，僅次於攻擊媒介大於 100Gbps 的 UDP 攻擊封包速率。

隨著攻擊規模增加，攻擊的平均複雜度也會增加。 單次攻擊的最多攻擊媒介次數為 21 次，且流量介於 10Gbps 到 100Gbps 之間。10Gbps-100Gbps 的攻擊平均會持續 8.72 小時。低於 1Gbps 的攻擊其持續時間平均不到 1 小時。

入侵攻擊

網路入侵攻擊包括以已知漏洞為根據的易執行攻擊，以及從使用開放原始碼或商業工具的掃描、用於偵查的資訊揭露嘗試，到路徑遍歷與緩衝區溢位攻擊企圖，並可能造成系統無法作業或提供存取敏感資訊的權限。

DoS 事件占 2021 年全部封鎖事件的 1/3，而入侵攻擊則占 2/3。

2021 年的多數入侵活動都是由 SIP 掃描構成。2021 年封鎖第二多的漏洞攻擊是企圖透過 2004 年所發布的異常 BMP 漏洞，以攻擊 Microsoft Internet Explorer 中的檔案緩衝區溢位。封鎖第三多的入侵攻擊是經由 SSH 的暴力攻擊。

Log4Shell 可說是 2021 年最嚴重的漏洞，在 12 月讓整個安全性社群刮起風暴。我們的雲端服務在 12 月共偵測及封鎖了超過 80 萬次 Log4Shell 漏洞攻擊，並記錄的尖峰達到每天超過 9 萬次漏洞攻擊。

網路應用程式攻擊

從 2020 年到 2021 年，封鎖惡意網路應用程式的請求次數增加了 88%。

可預期的資源位置幾乎占了全部攻擊的一半。在 2017 OWASP Top 10 應用程式安全性風險方面， 權限控制失效與注入攻擊占了 2021 年紀錄中全部攻擊的 3/4。

多數攻擊都來自於美國與俄羅斯，緊接著是印度、英國與德國。產生攻擊的源頭國家通常不會和威脅發動者或團體的國籍相符。威脅發動者會根據受害者的位置選擇發動攻擊的源頭國家，或會選擇他們想在假旗行動期間栽贓的國家。

2021 年的攻擊活動分散在許多產業，沒有明顯較突出的類別。最常受到攻擊的產業是銀行金融業與 SaaS 供應商，其次為零售業與高科技產業。製造業、政府、運輸、交通、電子商務與電玩，以及研究與教育皆有顯著的活動量。

不請自來的網路掃描與攻擊活動

Radware 全球欺敵網路共登記了 29 億次不請自來的網路事件，且單日尖峰高達近 1000 萬次。

2021 年共記錄到 570 萬個唯一 IP，占了網路上可用公共 IPv4 位址的 0.15%。這個唯一 IP 的數量，很適合用來測量參與掃描及網路上惡意活動之惡意主機與裝置的數量。

在全部的不請自來 TCP 活動中，有半數是以 SSH 為目標，緊接著是 網路攝影機、RDP、VNC 與 SMB，最後才是最普遍的網路應用程式協定 HTTP 與 HTTPS。以 Redis 為目標的活動儘管只占全部活動的 2%，依然達到相當可觀的 2400 萬次，這個開放原始碼的記憶體資料結構儲存是作為資料庫、快取與訊息佇列使用，並在2021 年 7 月揭露了一個遠端執行程式碼漏洞 (CVE-2021-32761)，這會讓攻擊者能在目標系統上執行任意程式碼。

許多 VoIP 手機與供應商使用的 SIP 協定，是 2021 年最常成為攻擊目標的 UDP 型服務。VoIP 依然是確保企業生產力的關鍵，同時也是 2021 年最常受到 DDoS 攻擊的目標。VoIP 服務中的漏洞與弱點或預設密碼會讓它們遭到濫用，以進行初始存取、間諜監控及在企業網路中橫向移動。

NTP、Memcached、LDAP、SSDP/UPnP、SNMP 與 mDNS 都是 DDoS 放大攻擊最常利用的協定，占了全部不請自來網路活動的 60% 以上。黑帽威脅發動者會持續掃描與周密的登記這些服務，以濫用發動 DDoS 攻擊，白帽駭客則會評估在 DDoS 威脅情勢中的風險。

美國是 2021 年居首位的攻擊國家，共產生超過全部 1/3 的不請自來網路活動；緊接在後的是俄羅斯與中國，兩國約占全部活動量的 1/5。

1. OWASP Top 10 是針對開發人員與網路應用程式安全的標準安全性認知文件，由 OWASP 基金會所發布，代表著對網路應用程式最關鍵安全風險的廣泛共識。

Apache Hadoop YARN 是最熱烈遭受掃描與漏洞攻擊的線上服務，其次為 Java 企業版執行的平台、路由器與 Docker API。

網路服務中用在帳戶接管 (ATO) 攻擊的前 10 個濫用憑證中，有 8 個是由常見的脆弱密碼「admin」、「pass」、「password」、「123456」、「1234」、「1111」、「1234」與空白密碼所組成，並且全都加上使用者名稱「admin」或「root」。線上服務攻擊期間所使用的所有憑證中，有近 1/10 是由「root:icatch99」構成；「root:icatch99」是數位錄影機 (DVR) 中的寫死憑證，由廠商 LILIN 在 2020 年 3 月公開揭露 [1]。在物聯網的威脅情勢中DVR 依然無所不在，而負責提供的監控攝影機也是。

在線上服務攻擊過程中，「8hYTSUFk:8hYTSUFk」的憑證占了所有遭濫用憑證的 11%。這些憑證的確切源頭依然成謎。它們被用在範本裡，以將認證引數傳遞至寫在名為 Yiff Rewrite [2]節點中的通用網路 API 互動與探索模組；Yiff Rewrite 是以 furry API 包裝函式作為據點的延伸包裝函式。在多個惡意程式二元碼中也都發現了這個字串。

在 SSH 暴力 ATO 攻擊過程中，最常利用的使用者名稱毫無意外就是「admin」、「user」與「test」。前 10 名還包括「postgres」、「oracle」與「git」，暴露出 ATO 最受歡迎及最可能成為目標的服務。

企業必須要領先於威脅情勢，
才能為下一代的網路攻擊做準備。
下載完整報告以瞭解更多。