

政府網際服務網通報

發佈編號：GSN_SEC_240607

發佈日期：2024/06/07

統計期間：2024/5/1~2024/5/31

政府網際服務網通報摘要：

1. 本期由閘口 IPS 阻擋「重大」及「嚴重」紀錄事件統計中，共攔截 248,207,010 次次攻擊。其中依前十大惡意攻擊次數排名顯示，排名第 1 之攻擊事件為 AnyDesk 事件攻擊數達 98,201,829 次，此行為特徵為 AnyDesk 應用服務，AnyDesk 為一跨平台圖形介面之遠端桌面軟體。因其可跨越防火牆之特性，攻擊者可藉由 AnyDesk 上檔案之傳輸、軟體漏洞等竊取使用者敏感資訊或取得終端主控權，以利攻擊者進一步攻擊。
2. 排名第 2 之攻擊事件為 BitTorrent
事件攻擊數達 66,232,410 次，此行為特徵為 BitTorrent 應用服務，BitTorrent 是一種廣用的 P2P 檔案分享協定，P2P 網路可能藉由用戶間點對點檔案之傳送，造成惡意檔案或病毒由此路徑傳送，盡而促成各種網路攻擊。
3. 排名第 3 之攻擊事件 TeamViewer
事件攻擊數達 27,565,932 次，此行為特徵為 TeamViewer 應用服務，TeamViewer 是兩終端電腦用於遠端控制、分享桌面操作與檔案傳輸之服務。因其可跨越防火牆之特性，攻擊者可藉由 TeamViewer 上檔案之傳輸、軟體漏洞等竊取使用者敏感資訊或取得終端主控權，以利攻擊者進一步攻擊。
4. 排名第 4 之攻擊事件 Realtek.SDK.UDPServer.Command.Execution
事件攻擊數達 23,997,186 次，此行為表示攻擊者嘗試利用 Realtek 設備中的命令執行漏洞，該漏洞是由易受攻擊的軟體處理惡意請求時發生的錯誤引起的，攻擊者可能能夠利用此漏洞在易受攻擊的系統上執行任意代碼。
5. 排名第 5 之攻擊事件 Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass
事件攻擊數達 13,650,421 次，Netcore/Netis 網路路由設備，韌體內藏後門程式，允許攻擊者遠端執行命令、讀檔以及變更設定組態。

政府網際服務網通報

6. 排名第 6 之攻擊事件 Wireshark.ENTTEC.DMX.Data.RLE.Buffer.Overflow
攻擊試圖利用 Wireshark 中的緩衝區溢位漏洞進行攻擊，此漏洞是由於應用程式在解析採用遊程編碼 (RLE) 壓縮的 ENTTEC DMX 封包時出現錯誤所致，遠端攻擊者可能利用此漏洞在應用程式上下文中執行任意程式碼，或造成服務中斷之情形。
7. 排名第 7 之攻擊事件為 Memcached.UDP.Amplification.Detection
攻擊者利用 Memcached 的 UDP 埠展開反射性的放大攻擊，透過偽造的請求到啟用 Memcached UDP 的伺服器上，伺服器回應遠大於請求之封包至被攻擊目標，造成目標網域的資源用罄，對目標造成阻斷式服務攻擊。
8. 排名第 8 之攻擊事件為 Back.Orifice.Traffic
BackOrifice 是一種允許入侵者控制目標系統的木馬，任何未受保護的系統都可能受到攻擊，攻擊者甚至可以遠端控制被入侵之系統，並竊取使用者的個人資料與敏感資訊等。
9. 排名第 9 之攻擊事件為 Linux.Kernel.TCP.SACK.Panic.DoS
攻擊者透過利用 linux kernel 處理比較小 MSS (maximum segment size) 的 TCP 封包時產生的錯誤，利用此漏洞造成網路或服務中斷的攻擊行為。
10. 排名第 10 之攻擊事件為 Sora.Botnet
Sora 是一種針對嵌入式系統的物聯網惡意軟體。此行為代表被攻擊者感染 Sora Botnet 惡意程式，感染之終端設備可能嘗試連網惡意中繼站、被攻擊者命令發動其他攻擊行為或資料竊取等情形。

政府網際服務網通報

防護建議：

1. 機關委外進行弱點掃描及漏洞修補服務時，建議進行此類服務前，能先向 GSN 維運小組提出申請進行開放，避免掃描結果準確性降低。
2. 機關應定期注意各作業系統或軟體是否有發佈漏洞弱點之公告，並即時修補相關弱點，或採取相對應變措施，以避免造成資安風險。
3. 資訊系統人員應監測網站或系統連線之封包數，流量或 Sessions，如有發生異常，應保持警覺監控來源 IP，並應情況適時封鎖，以避免服務遭受阻絕式服務攻擊。
4. 網頁程式撰寫時應對輸入資料欄位進行格式及特殊字元檢查及過濾，另對於檔案上傳應檢測檔案型態，大小與內容等，以避免遭受駭客竊取資訊或植入後門程式遙控主機。
5. 各機關係統管理人員，應定期檢視防火牆連線紀錄，並過濾特殊協定封包，確認無異常連線之紀錄；若須對外網路開放服務之埠號，建議採取正面表列準則且盡量以點對點原則訂定，縮小網路開放範圍。
6. 各機關應提醒使用者，盡量勿用公務電子信箱註冊網站，以降低遭受垃圾郵件攻擊之情形。
7. 各機關網路管理人員應定期審視相關網路設備是否有異常連線，並定期稽核相關登入日誌，以降低資安風險發生之機率。
8. 如用戶發現有因入侵防禦系統誤判而導致連線異常之情況，請來電告知 GSN 維運小組設定例外排除。GSN 維運小組電話：(02) 2344-2836#1204。

政府網際服務網通報

GSN 開口 等級為「high」或「critical」Top 10 攻擊事件

| NO | Filter Name | Severity | Hits |
|----|--|----------|------------|
| 1 | AnyDesk | high | 98,201,829 |
| 2 | BitTorrent | high | 66,232,410 |
| 3 | TeamViewer | high | 27,565,932 |
| 4 | Realtek.SDK.UDPServer.Command.Execution | critical | 23,997,186 |
| 5 | Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass | critical | 13,650,421 |
| 6 | Wireshark.ENTTEC.DMX.Data.RLE.Buffer.Overflow | critical | 4,973,016 |
| 7 | Memcached.UDP.Amplification.Detection | high | 2,080,526 |
| 8 | Back.Orifice.Traffic | high | 2,040,341 |
| 9 | Linux.Kernel.TCP.SACK.Panic.DoS | high | 1,528,093 |
| 10 | Sora.Botnet | high | 1,206,527 |

GSN 開口 Top 10 攻擊事件

| 攻擊事件類型 | 事件數 |
|---|-------------|
| QUIC | 910,150,087 |
| AnyDesk | 98,201,829 |
| NTP.Monlist.Command.DoS | 81,662,894 |
| Nmap.Script.Scanner | 74,036,642 |
| BitTorrent | 66,232,410 |
| TikTok | 30,925,685 |
| TeamViewer | 27,565,932 |
| Realtek.SDK.UDPServer.Command.Execution | 23,997,186 |
| Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner | 19,388,679 |
| Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass | 13,650,421 |