

政府網際服務網通報

發佈編號：GSN\_SEC\_210927

發佈日期：2021/9/27

統計期間：2021/8/1~2021/8/31

**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 186,952,437 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 BitTorrent 事件攻擊數達 123,384,013 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。
2. 排名第 2 之攻擊事件為 SopCast  
事件攻擊數達 23,357,563 次，SopCast 是免費的線上 p2p 視訊軟體，提供免費的即時 p2p 頻道和廣播。SopCast 可以穿越防火牆和 NAT，並可透過各種傳輸媒體格式，且僅需低記憶體和 CPU 負載，提供端到端安全性，因此讓惡意行為難以被偵測。
3. 排名第 3 之攻擊事件為 AnyDesk  
事件攻擊數達 15,797,394 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。
4. 排名第 4 之攻擊事件為 DNS.TXT.Records.Tunneling  
事件攻擊數達 9,038,546 次，DNS Tunneling 是隱蔽通道的一種，經由將其他

通信協定封裝在 DNS 通信協定中傳輸，以突破企業安全機制的限制而完成非法通訊的過程。因為在網際網路的 DNS 是一個必不可少的基礎服務，防火牆和入侵檢測系統很少會過濾 DNS 流量，這就給 DNS 作為一種隱蔽通道提供了條件，從而可以利用它實現例如遠端控制，資料傳輸作業。DNS Tunneling 也經常在殭屍網路和 APT 攻擊中扮演著重要的角色。

#### 5. 排名第 5 之攻擊事件為 TeamViewer

事件攻擊數達 4,926,437 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。

#### 6. 排名第 6 之攻擊事件為

Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass

廠牌型號為 Netcore/Netis 網路路由設備，其韌體存在後門程式，允許攻擊者遠端執行命令、讀檔以及變更設定組態。

#### 7. 排名第 7 之攻擊事件為 Torpig.Mebroot.Botnet

此行為代表被攻擊者感染 Tropic 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。

#### 8. 排名第 8 之攻擊事件為 Resilio

Resilio（以前稱為 BitTorrent Sync）是一種可用於 Windows，Mac 和 Linux 的點對點檔案同步工具。它透過 P2P 技術在本地設備之間或透過 Internet 在遠端設備之間同步檔案。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，進而促成各種網路攻擊。

#### 9. 排名第 9 之攻擊事件為 QVOD

此行為特徵為 QVOD 應用服務，QVOD 是一款免費的中文媒體播放器，使用 P2P 檔案分享協定(BitTorrent)來提供視頻點播服務。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。

#### 10.排名第 10 之攻擊事件為 TinyProxy

Tinyproxy 是一個用於 POSIX OS 的輕量級 HTTP Proxy，其佔用很少的系統資源，可以在非常老的機器上運行。它支援 HTTPS 連接的轉發，並且可以設置成透通式或反向式 proxy。然而其容易受到遠端攻擊者藉著傳送特製的要求標頭而造成的拒絕服務影響。

#### 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. 各機關系統管理人員，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。

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

No.	Filter Name	Severity	Hits
1	BitTorrent	high	123,384,013
2	SopCast	high	23,357,563
3	AnyDesk	high	15,797,394
4	DNS.TXT.Records.Tunneling	critical	9,038,546
5	TeamViewer	high	4,926,437
6	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	critical	4,503,963
7	Torpig.Mebroot.Botnet	critical	1,420,357
8	Resilio	high	1,027,916
9	QVOD	high	890,346
10	TinyProxy	critical	528,615

### GSN 開口 Top 10 攻擊事件

攻擊事件類型	事件數
BitTorrent	123,384,013
Nmap.Script.Scanner	62,936,049
SopCast	23,357,563
AnyDesk	15,797,394
NTP.Monlist.Command.DoS	12,187,049
DNS.TXT.Records.Tunneling	9,038,546
Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner	5,522,341
TeamViewer	4,926,437
Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	4,503,963
TCP.Split.Handshake	2,117,832