政府網際服務網通報	
發佈編號：GSN_SEC_200410	發佈日期：2020/05/11
統計期間：2020/4/1~ 2020/4/30	

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 530,618,310 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 156,644,881 次，此使用行為特徵為 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 Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass 事件攻擊數達 92,025,815 次，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。

3. 排名第 3 之攻擊事件為 Eyequila.curlmyip.com 事件攻擊數達 47,694,298 次，網域 curlmyip.com 為 Eyequilay 資料回溯分析服務列入黑名單之網址，通常為惡意中繼站或惡意連線位址。駭客在從事惡意活動時，為了掩藏自己的網路位址，會透過中繼站主機，對遠端的受害電腦進行操控、破壞，因此受害者會連結到有危害的網站，進而遭受到侵害，導致作業中斷、資料被竊取、中毒、網路斷線等危機。

4. 排名第 4 之攻擊事件為 AnyDesk 事件攻擊數達 36,057,602 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。

5. 排名第 5 之攻擊事件為 Eyequila.padrup.com

   事件攻擊數達 27,596,250 次，網域 padrup.com 為 Eyequilay 資料回溯分析服務列入黑名單之網址，通常為惡意中繼站或惡意連線位址。駭客在從事惡意活動時，為了掩藏自己的網路位址，會透過中繼站主機，對遠端的受害電腦進行操控、破壞，因此受害者會連結到有危害的網站，進而遭受到侵害，導致作業中斷、資料被竊取、中毒、網路斷線等危機。

6. 排名第 6 之攻擊事件為 SopCast

   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。

7. 排名第 7 之攻擊事件為 TeamViewer

   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。

8. 排名第 8 之攻擊事件為 DNS.TXT.Records.Tunneling

   TXT 紀錄是一種「網域名稱系統」(DNS) 紀錄，可將文字資訊提供給網域以外的來源。攻擊者嘗試透過 DNS TXT 來建立通道，存取遠端儲存的惡意 PowerShell 命令。可能造成資料被竊取、中毒、網路斷線等風險。

9. 排名第 9 之攻擊事件為 Eyequila.at.heheelibom.com

   網域 at.heheelibom.com 為 Eyequilay 資料回溯分析服務列入黑名單之網址，通常為惡意中繼站或惡意連線位址。駭客在從事惡意活動時，為了掩藏自己的網路位址，會透過中繼站主機，對遠端的受害電腦進行操控、破壞，因此受害者

會連結到有危害的網站，進而遭受到侵害，導致作業中斷、資料被竊取、中毒、網路斷線等危機。

10.排名第 10 之攻擊事件為 Eyequila.yeanqin.com

網域 yeanqin.com 為 Eyequilay 資料回溯分析服務列入黑名單之網址，通常為惡意中繼站或惡意連線位址。駭客在從事惡意活動時，為了掩藏自己的網路位址，會透過中繼站主機，對遠端的受害電腦進行操控、破壞，因此受害者會連結到有危害的網站，進而遭受到侵害，導致作業中斷、資料被竊取、中毒、網路斷線等危機。

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，避免掃瞄結果準確性降低。
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. 各單位可透過 GSN CSS 網站瞭解個別之防護情況。

   網址為: https://css.gsn.gov.tw/
9. 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 閘口 等級為「high」或「critical」Top 10 攻擊事件

No.	Filter Name	Severity	Hits
1	BitTorrent	high	156,644,881
2	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	critical	92,025,815
3	Eyequila.curlmyip.com	critical	47,694,298
4	AnyDesk	high	36,057,602
5	Eyequila.padrup.com	critical	27,596,250
6	SopCast	high	23,352,680
7	TeamViewer	high	23,284,799
8	DNS.TXT.Records.Tunneling	critical	22,607,967
9	Eyequila.at.heheelibom.com	critical	16,303,961
10	Eyequila.yeanqin.com	critical	13,933,336

GSN 閘口 Top 10 攻擊事件

攻擊事件類型	事件數
BitTorrent	156,644,881
UPnP.SSDP.M.Search.Anomaly	139,326,823
Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	92,025,815
Eyequila.curlmyip.com	47,694,298
AnyDesk	36,057,602
Eyequila.padrup.com	27,596,250
SopCast	23,352,680
TeamViewer	23,284,799
DNS.TXT.Records.Tunneling	22,607,967
Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner	17,441,754