政府網際服務網通報

發佈編號：GSN_SEC_240410	發佈日期：2024/04/10
統計期間：2024/3/1~ 2024/3/31	

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 287,969,598 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 100,416,047 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 Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass 事件攻擊數達 56,893,423 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。
3. 排名第 3 之攻擊事件為 BitTorrent
   事件攻擊數達 44,635,760 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。
4. 排名第 4 之攻擊事件 DNS.TXT.Records.Tunneling
   事件攻擊數達 41,001,122 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 TeamViewer

   事件攻擊數達 25,967,359 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 Realtek.SDK.UDPServer.Command.Execution

   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。

7. 排名第 7 之攻擊事件為 Back.Orifice.Traffic

   Back.Orifice 為木馬程式名稱，該木馬允許入侵者透過監視和篡改主機。在一般攻擊中，入侵者將 Back Orifice 特洛伊木馬作為電子郵件附加程式發送給受害者。當電子郵件收件者執行程式附件時，木馬會開啟從受害端到 Internet 的連線。Back Orifice 允許駭客檢視和修改被駭主機上的任何檔案、建立日誌檔案、截取螢幕回傳給攻擊者等。

8. 排名第 8 之攻擊事件為 Trin00

   Trin00 是一種分散式阻斷服務 (DDoS) 攻擊工具，攻擊者透過使用此工具發起 DDoS 攻擊，使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。

9. 排名第 9 之攻擊事件為

   Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection

   遠端攻擊者利用指令注入漏洞攻擊 Hikvision 產品的網頁伺服器，並利用此漏洞在受影響之產品上執行任意指令。

政府網際服務網通報

10.排名第 10 之攻擊事件為 Telnet.Default.Credentials

此行為表示攻擊者嘗試使用系統預設的 telnet 帳號與密碼登入，Mirai 等惡意軟體有時會透過掃描未關閉之 telnet 連接埠，並使用這些預設之憑證登入，進而造成遠端攻擊者登入系統並加以控制。

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. 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 閘口 等級為「high」或「critical」Top 10 攻擊事件

NO	Filter Name	Severity	Hits
1	AnyDesk	high	100,416,047
2	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	critical	56,893,423
3	BitTorrent	high	44,635,760
4	DNS.TXT.Records.Tunneling	critical	41,001,122
5	TeamViewer	high	25,967,359
6	Realtek.SDK.UDPServer.Command.Execution	critical	4,925,315
7	Back.Orifice.Traffic	high	3,489,189
8	Trin00	high	1,887,516
9	Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection	critical	958,271
10	Telnet.Default.Credentials	high	873,029

GSN 閘口 Top 10 攻擊事件

攻擊事件類型	事件數
QUIC	871,441,185
NTP.Monlist.Command.DoS	288,984,054
AnyDesk	100,416,047
Nmap.Script.Scanner	74,477,451
Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	56,893,423
BitTorrent	44,635,760
DNS.TXT.Records.Tunneling	41,001,122
TeamViewer	25,967,359
TikTok	23,171,648
Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner	20,097,547