政府網際服務網通報	
發佈編號：GSN_SEC_150613	發佈日期：2016/6/13
統計期間：2016/05/01~ 2016/5/31	

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 96,511,815 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 TLS: OpenSSL Invalid Session Ticket Denial-of-Service Vulnerability (ONLY enable under DoS attack) ，事件攻擊數達 67,982,361 次，該漏洞是處理 TLS 建立 Session 時，產生出記憶體內容洩漏的風險。攻擊者可以通過發送惡意封包到有此漏洞的伺服器，造成服務阻斷攻擊。
2. 排名第 2 之攻擊事件為 DNS: DNS Reply Sinkhole Microsoft NO-IP Domain 事件攻擊數達 8,737,318 次，設備可能已感染惡意程式並企圖連回惡意中繼站進行報到，此中繼站採用 domain 方式管理，防止中繼站 IP 位址暴露被資安業者封鎖。
3. 排名第 3 之攻擊事件為 DNS: DNS Reply Sinkhole-Microsoft -199.2.137.0/24 事件攻擊數達 6,353,224 次，設備可能已感染惡意程式並企圖連回惡意中繼站(199.2.137.0/24)進行報到。
4. 排名第 4 之攻擊事件為 DNS: Wapack Labs Sinkhole DNS Reply 事件攻擊數達 4,539,729 次，設備可能已感染惡意程式並企圖連回惡意中繼站進行報到，此中繼站採用 domain 方式管理，防止中繼站 IP 位址暴露被資安業者封鎖。

5. 排名第 5 之攻擊事件為 DNS: Kaspersky Sinkhole DNS Reply 事件攻擊數達 2,615,675 次，設備可能已感染惡意程式並企圖連回惡意中繼站進行報到，資安設備監測出此中繼站可能採用 domain 方式管理，防止中繼站 IP 位址暴露被資安業者封鎖。
6. 排名第 6 之攻擊事件為 C1000059:HTMdropline #DNS-UDP
   攻擊者封包內容觸發技術服務中心提供之惡意連線特徵規則 (C1000059:HTMdropline #DNS-UDP)，後續相關檔案將提供給技術服務中心進一步分析。
7. 排名第 7 之攻擊事件為 DNS: DNS query for Morto RDP worm related domain jaifr.net
   設備可能已感染惡意程式並企圖連回惡意中繼站(jaifr.net)進行報到。
8. 排名第 8 之攻擊事件為 HTTP: SQL Injection Variable Declaration Evasion
   攻擊者透過宣告變數方式將 SQL 語法藏入變數中，藉此逃避系統檢測。
9. 排名第 9 之攻擊事件為 HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability
   攻擊者利用 PHP-CGI 的腳本命令注入漏洞，使得伺服器可能洩露原始程式碼，並獲得執行任意代碼。
10. 排名第 10 之攻擊事件為 HTTP: SQL Injection (WAITFOR)
    攻擊者藉由系統處理 WAITFOR 指令之反應時間推測 SQL 是否存在漏洞。
11. 本期閘口信譽名單監測攔阻機制，封鎖超過 20,000 萬筆可疑連線，其中包含可疑之 Botnet 連線、病毒蠕蟲檔案與間諜程式等各種惡意程式與行為；由攻擊來源事件數量統計發現，主要攻擊來源 IP 位址以美國為最大宗。

12.FTTB 多機型入侵防護 IPS，於本期同閘口 IPS 防護系統調整攻擊計次規則，降低事件時間之關聯性影響。本期共阻攔 949,814 起攻擊事件，排名第 1 之攻擊事件為 Anomaly-DNS- Z-Flag-UDP 攻擊事件，攻擊藉由變造 DNS 封包之旗標欄位，將目前保留使用之 Z 旗標值替換，使 DNS 伺服器丟棄該封包造成主機忙碌。排名第 2 之攻擊事件 Invalid TCP Flags，主要攻擊者透過更改 TCP 封包中的各項旗標設定，造成接收端組合封包時產生異常，造成主機忙碌阻斷整體服務。

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: http://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「嚴重」或「重大」Top 10 攻擊事件

No.	Filter Name	Severity	Hits
1	TLS: OpenSSL Invalid Session Ticket Denial-of-Service Vulnerability (ONLY enable under DoS attack)	Major	67,982,361
2	DNS: DNS Reply Sinkhole Microsoft NO-IP Domain	Major	8,737,318
3	DNS: DNS Reply Sinkhole - Microsoft - 199.2.137.0/24	Major	6,353,224
4	DNS: Wapack Labs Sinkhole DNS Reply	Major	4,539,729
5	DNS: Kaspersky Sinkhole DNS Reply	Major	2,615,675
6	C1000059: HTM#dpponline #DNS-UDP	Critical	1,349,978
7	DNS: DNS query for Morto RDP worm related domain jaifr.net	Major	1,243,458
8	HTTP: SQL Injection Variable Declaration Evasion	Major	378,707
9	HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Critical	323,206
10	HTTP: SQL Injection (WAITFOR)	Major	266,539

GSN 閘口 Top 10 攻擊事件

名稱	Sum(Sum(集合事件數))
Rep-NetworkWorm	94261654
Rep-Malware	86088303
TLS: OpenSSL Invalid Session Ticket Denial-of-Service Vulnerability (ONLY enable under DoS attack)	67982361
Rep-Miscellanous	22051991
DNS: DNS Reply Sinkhole Microsoft NO-IP Domain	8737318
DNS: Version Request (UDP)	8363963
Rep-Spyware	6740748
DNS: DNS Reply Sinkhole - Microsoft - 199.2.137.0/24	6353224
hpc-tw	5279417
DNS: Wapack Labs Sinkhole DNS Reply	4539729

GSN FTTB 多機型 Top 10 攻擊事件

Name	Count
Anomaly-DNS-Z-Flag-UDP	630136
Invalid TCP Flags	100719
ICMP-Frag-Needed-Storm	64000
MS-Report-Viewer-Con-XSS-GET	47721
Anomaly-IP-bad-frag-bits	24279
Apache-SSI-ERR-Host-XSS	14113
Anomaly-RealVNC-Auth-Bypass	13202
POP3-Auth-brute-force-attempt	10636
SSH-brute-force	10133
S_yandex.ru	5773