02_資安事件及異常紀錄 - 一般 #1357

[INCGC-15706]-Low-Outbound Communication Detected To Malicious Domain Detected On Firewall

2026-01-12 17:43 - 益利 周

狀態:	Resolved-解決	**開始日期:**	2026-01-12
優先權:	Normal	**完成日期:**	
被分派者:	益利 周	**完成百分比:**	100%
分類:		**預估工時:**	1:00 小時

概述

clipboard-202601121743-lep0j.png

歷史

#1 - 2026-01-12 17:49 - 益利 周

- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

- 預估工時 設定為 1:00 小時

防火牆警報「偵測到與惡意網域的出站通訊」表明，主機 ULPU-TL-PC-0002（IP 位址 10.15.88.101，MAC 位址 A0:AD:9F:97:10:F4）透過 HTTPS 與網域 OBJECTSTORAGE.AP-TOKYO-1. 134.70.80.3）進行了通訊。儘管根據開源情報，目標網域被認為是潛在的惡意網域，但此流量仍被 Web 過濾策略允許，導致網路 HTTP 流量透傳。

已將網站 "objectstorage[.]ap-tokyo-1[.]oraclecloud[.]com" IP 位址 10.15.88.101 列入封鎖名單.

#2 - 2026-01-15 09:58 - 益利 周

- 檔案 clipboard-202601150955-xh368.png 已新增

- 檔案 clipboard-202601150957-nysxt.png 已新增

1/12 將 "objectstorage[.]ap-tokyo-1[.]oraclecloud[.]com" 加入 DNS 黑名單.
未獲預期成效
clipboard-202601150955-xh368.png
1/14 新增網站防護 將"objectstorage[.]ap-tokyo-1[.]oraclecloud[.]com" 加入攔阻網站名單
clipboard-202601150957-nysxt.png

檔案

clipboard-202601121743-lep0j.png	45.3 KB	2026-01-12	益利 周
clipboard-202601150955-xh368.png	15.8 KB	2026-01-15	益利 周
clipboard-202601150957-nysxt.png	17.5 KB	2026-01-15	益利 周