02_資安事件及異常紀錄 - 一般 #1212

INCGC-15090 -Low-Windows Authentication Replay Attack Detected

2025-12-12 13:52 - 益利 周

狀態:	Closed-關閉	**開始日期:**	2025-12-12
優先權:	Normal	**完成日期:**	
被分派者:	弘政 黃	**完成百分比:**	100%
分類:		**預估工時:**	4:00 小時

概述

Analysis:

The case involves a detected Kerberos replay attack on host WCB20101 , originating from TAHOAD.TAHOHO.COM.TW , indicating a potential Adversary-in-the-Middle (AiTM) attack. The process C:\Windows\System32\dns.exe (PID 848) on TAHOAD.TAHOHO.COM.TW was running under the user TAHOAD$, targeting the Kerberos process on WCB20101 with the user WCB20101$.

歷史

#1 - 2025-12-12 14:44 - 益利 周

- 狀態 從 New-新增 變更為 In process-進行中

- 被分派者 設定為 弘政 黃

Analysis:

The case involves a detected Kerberos replay attack on host WCB20101 , originating from TAHOAD.TAHOHO.COM.TW , indicating a potential Adversary-in-the-Middle (AiTM) attack. The process C:\Windows\System32\dns.exe (PID 848) on TAHOAD.TAHOHO.COM.TW was running under the user TAHOAD$, targeting the Kerberos process on WCB20101 with the user WCB20101$.

Recommendations:

1. Immediately isolate TAHOAD.tahoho.com.tw and conduct a thorough forensic investigation focusing on the dns.exe process (PID 900) and the TAHOAD$ machine account for signs of compromise, such as malware or unauthorized code execution.
2. Perform a forensic analysis on the target host WCB20101 and the WCB20101$ machine account to assess for any successful Kerberos exploitation or compromise resulting from the replay attack.
3. Scrutinize the privileges and network access granted to both TAHOAD$ and WCB20101$ machine accounts, ensuring they strictly adhere to the principle of least privilege and are not over-privileged for their intended roles.

#2 - 2025-12-12 14:46 - 益利 周

- 狀態 從 In process-進行中 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

- 預估工時 設定為 4:00 小時

分析：

本案例涉及對主機 WCB20101 偵測到的 Kerberos 重播攻擊，攻擊源自 TAHOAD.TAHOHO.COM.TW，顯示可能存在中間人攻擊 (AiTM)。TAHOAD.TAHOHO.COM.TW 上的進程 C:\Windows\System32\dns.exe（進程 ID 848）以用戶 TAHOAD$ 的身份運行，目標是 WCB20101 上以用戶 WCB20101$ 身份運行的 Kerberos 進程。

經查
1.WCB20101 自 12/4 起有頻繁的 DNS DYNAMIC_UPDATE 事件.
2.查 WCB20101 有線 及 無線網路 同時運作 易形成 Multi-homed Hosts 的行為

處理
拔除 停用拔除無線網卡 觀察 已無大量 DNS DYNAMIC_UPDATE 記錄產生.

#3 - 2026-01-12 13:07 - Joy Liao

- 狀態 從 Resolved-解決 變更為 Closed-關閉