# 02_資安事件及異常紀錄 - 非法入侵 #677

## FINANCE-1

2024-02-15 08:58 - Joy Liao

| | | | |
|---|---|---|---|
| **狀態:** | Closed-關閉 | **開始日期:** | 2024-02-15 |
| **優先權:** | Normal | **完成日期:** | 2024-02-15 |
| **被分派者:** | 正達 駱 | **完成百分比:** | 100% |
| **分類:** | | **預估工時:** | 0:30 小時 |
| **版本:** | | | |

**概述**

Description
A suspicious process injected into another process in an unusual way. Investigate the process trees for the injector and injectee.

Command line
"C:\WINDOWS\system32\rundll32.exe"
D:\Users\ProgramData\Lenovo\Vantage\Addins\LenovoBatteryGaugeAddin\1.0.3.12\x64\LenovoBatteryGaugePackage.dll
UnloadBatteryGaugeFromExplorer

**歷史**

**#1 - 2024-02-15 11:20 - 正達 駱**

*- 完成日期 設定為 2024-02-15*

*- 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 0:30 小時*

**1.移除 Lenovo 提供的工具 Vantage,**
**D:\Users\ProgramData\Lenovo 底下已經沒有 Vantage資料夾**
**2.電腦名稱:修正為TPHQ6WKS324**

**#2 - 2024-03-01 10:40 - Joy Liao**

*- 狀態 從 Resolved-解決 變更為 Closed-關閉*