

02_資安事件及異常紀錄 - 非法入侵 #684

ULPU-WG-PC-0019

2024-02-19 10:17 - Joy Liao

狀態:	Closed-關閉	開始日期:	2024-02-19
優先權:	Normal	完成日期:	2024-02-29
被分派者:	宗沛 陳	完成百分比:	100%
分類:		預估工時:	0:00 小時
版本:			
概述			
Description			
A suspicious process read lsass memory. Adversaries often use this to steal credentials. If credentials were dumped, change your passwords and review the process tree.			
Command line			
"C:\Program Files\Cybereason ActiveProbe\minionhost.exe" -p 4916 -rc a568ecb5-1d1f-44df-93c4-f6a5ffbc99b1 -t 384			

歷史

- #1 - 2024-04-30 10:46 - 宗沛 陳
- 狀態 從 New-新增 變更為 Resolved-解決
- #2 - 2024-04-30 10:48 - 宗沛 陳
- 完成百分比 從 0 變更為 100
- #3 - 2024-05-03 14:13 - Joy Liao
- 狀態 從 Resolved-解決 變更為 Closed-關閉