



進行一個

POLICE LINE DO NOT CROSS

POLICE LINE DO NOT CROSS

POLICE LINE DO NOT CROSS

微鑑識

的動作

高譚市爆炸了





# 蝙蝠洞警報

監控通報

使用者感覺

第三方回報

# 事故嚴重性



檢調介入  
犯罪或損害調查  
C&C

大範圍事故  
頻繁事故

重要系統無法運作

重要系統受損  
服務品質降低

不重要系統中斷

# 選擇偵查目標



事故回復



事故排除



事故存證



# 是誰搞的鬼？



Root4

A cinematic image of Batman in his tactical suit, sitting in a high-tech control room. He is looking intently at a computer monitor. The room is dimly lit with blue and green light from the screens. The text is overlaid on the right side of the image.

從哪裡下手？

人員

網路/通訊

系統

# 高譚 交通網







**防毒系統(Anti-Virus)**  
**防護垃圾信件(Anti-Spam)**  
**防護針對式攻擊(Anti-APT)**

入侵偵測系統(IDS/IPS)

網頁防火牆(WAF)



SNORT

Malicious Attacks Prevention

ShellCode

Encoding Attack



Keyword Filter

Directory Traversal

HTTP Attack



SQL Injection

Buffer Overflow

Anti-tampering

Directory protection

# 高譚CSI

# 犯罪現場



Local Surveillance

Glide   
Hang 

程式佔用埠號  
當前連線狀態  
網路分享

機碼值

系統環境

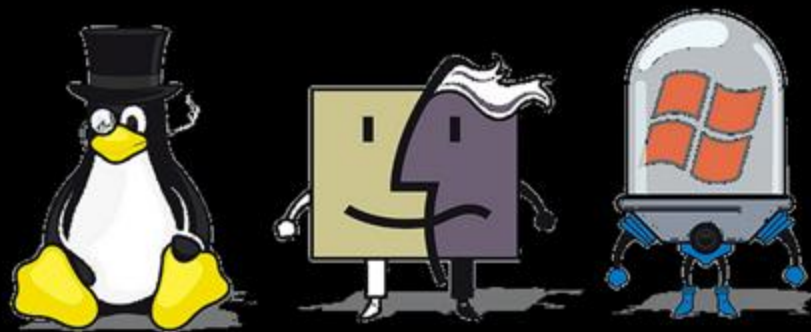
開機時程式與排定的工作

使用者與群組列表

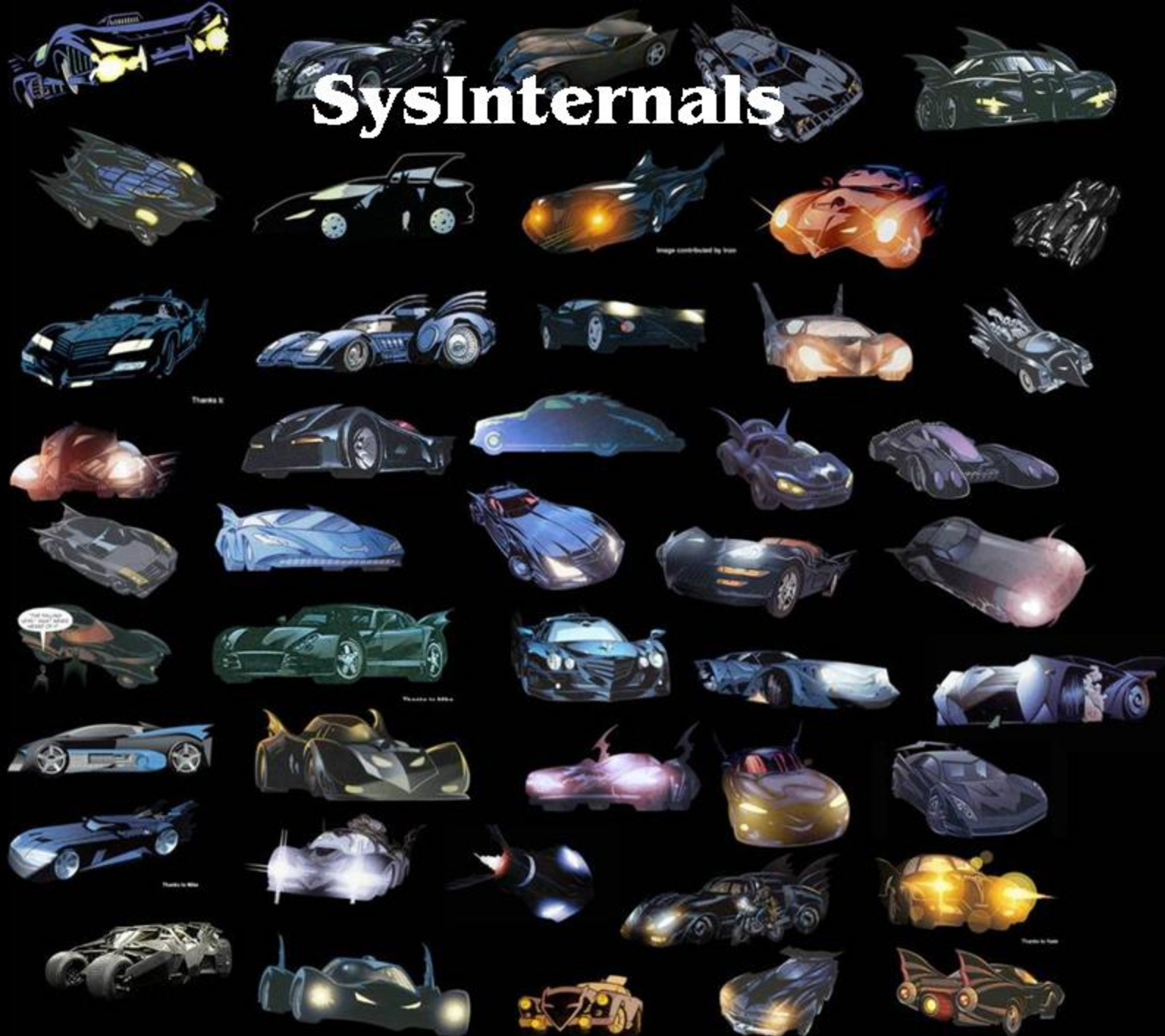
執行中程式清單

執行中DLL清單

開啓服務



# SysInternals



使用者躲藏





主機端

個人電腦端

# Event Log





# 惡意程式躲藏 - 基本型



# 程式分析 – AntiVirus (VirusTotal)



Encase



# 不道德追查



# 工商服務



我們的老闆

我們的資安顧問

我們的業務


我們的工程師





# 問題與討論

lucifer 點 yang 小老鼠 sti 點 com 點 tw

A comic book illustration showing Batman in his black suit and cowl, looking down at the Joker. The Joker is wearing a purple shirt and has a wide, menacing grin with visible teeth and blood on his face. A speech bubble above the Joker contains the Chinese characters '投降' (surrender). The background is a solid green color.

投降