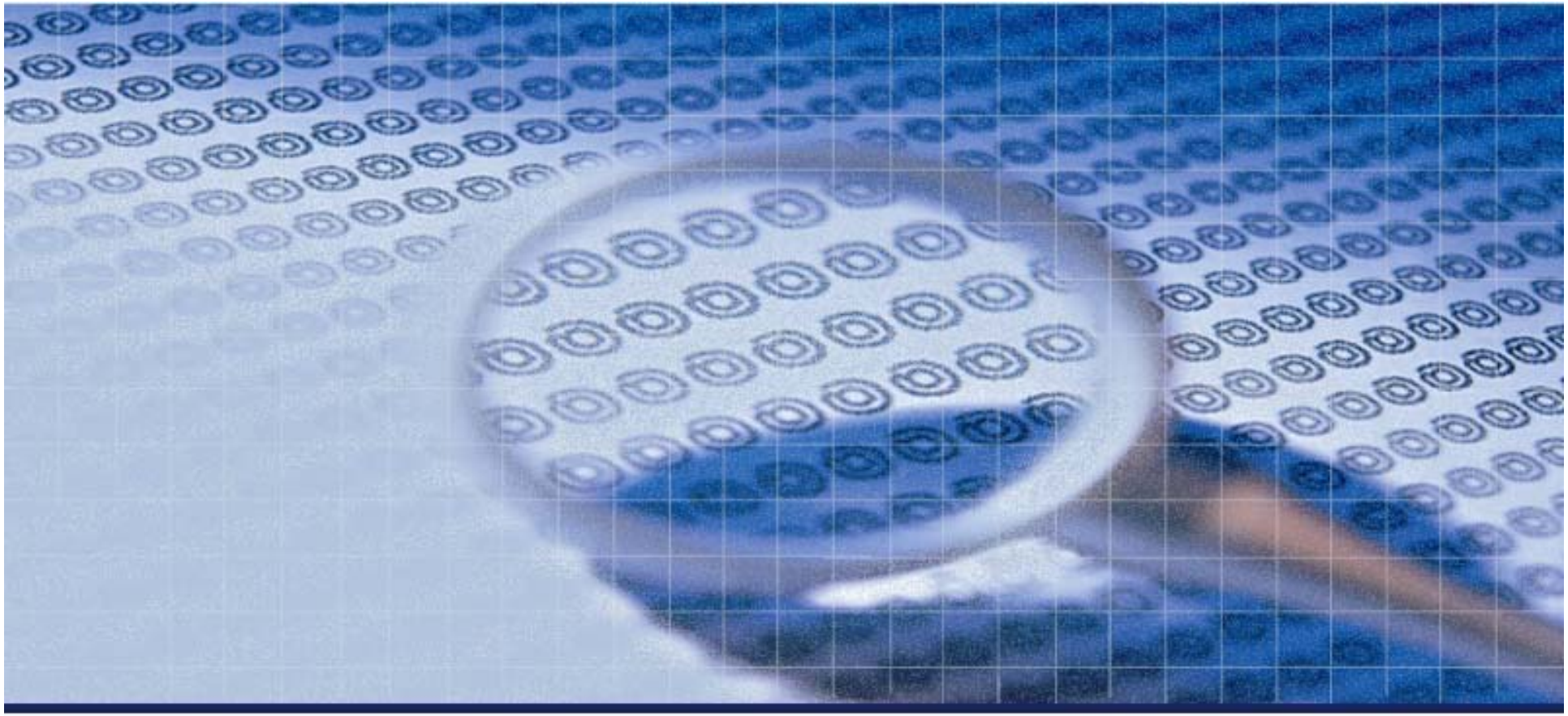


Security Online, Hacker Offline!

大綱

駭客戀上線上遊戲

母體駭人？人駭母體？

玩？還是被玩？

地下城主指南

工商服務時間

駭客戀上線上遊戲

駭客想要什麼？

- 傳統的駭客：
  - 政治意圖
  - 爽
  - 練技術
  - 出名
- 動機導致結果

換網頁！

- But...

遊戲官網被換網頁的請舉手？？？？

Stark Technology Inc.
敦陽科技股份有限公司

所以，駭客真正想要什麼？

- 最終目的：

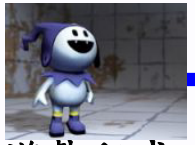
  $$$

- 動機導致結果
  - 攻擊遊戲商
    - 取得資料庫機密資料
    - 取得網站主機權限對內攻擊
    - 破解付費機制
    - 流量勒索？
    - 內賊？
  - 攻擊玩家
    - 置換頁面埋藏木馬
    - 跨站腳本欺騙使用者
    - Web 2.0 趨勢

為什麼選擇遊戲公司？

- 玩家對財產的警覺性低
  - 消費金額小
  - 年齡層分布廣，伸手牌、尼特族、閒錢上班族
  - 主動尋找被騙的機會
- 虛擬世界真實匯率
  - 虛擬寶物、貨幣可以轉成真錢
- 安全層級比金融單位
  - 虛擬財產對遊戲業者來說沒有直接損失
- 跨企業金流物流？
  - 與其他業界結合，例如小額付款、便利超商活動？

存取途徑-玩家



遊戲程式

遊戲主機

遊戲資料庫

玩家

唉噎

討論/購物

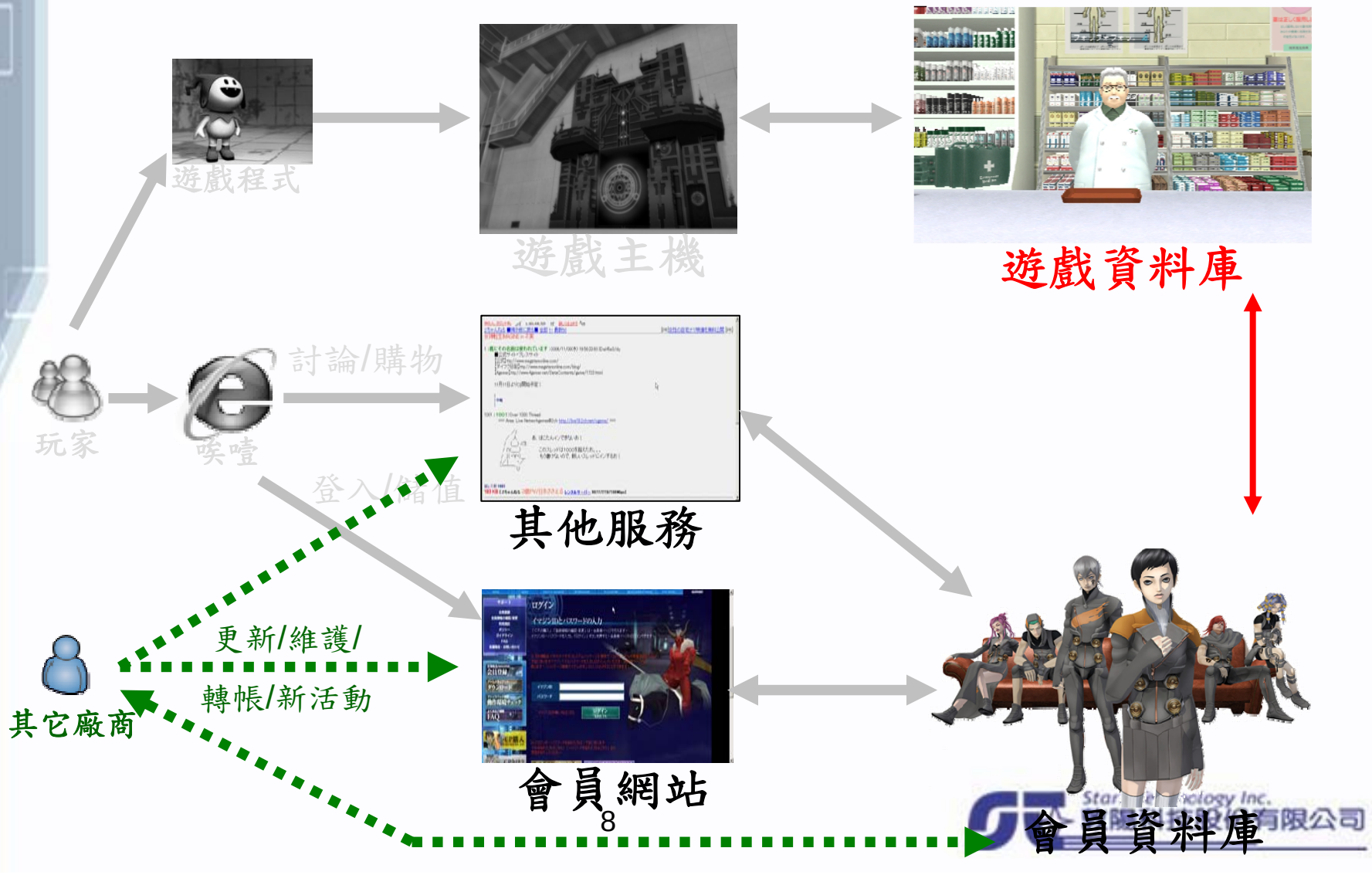
其他服務

登入/儲值

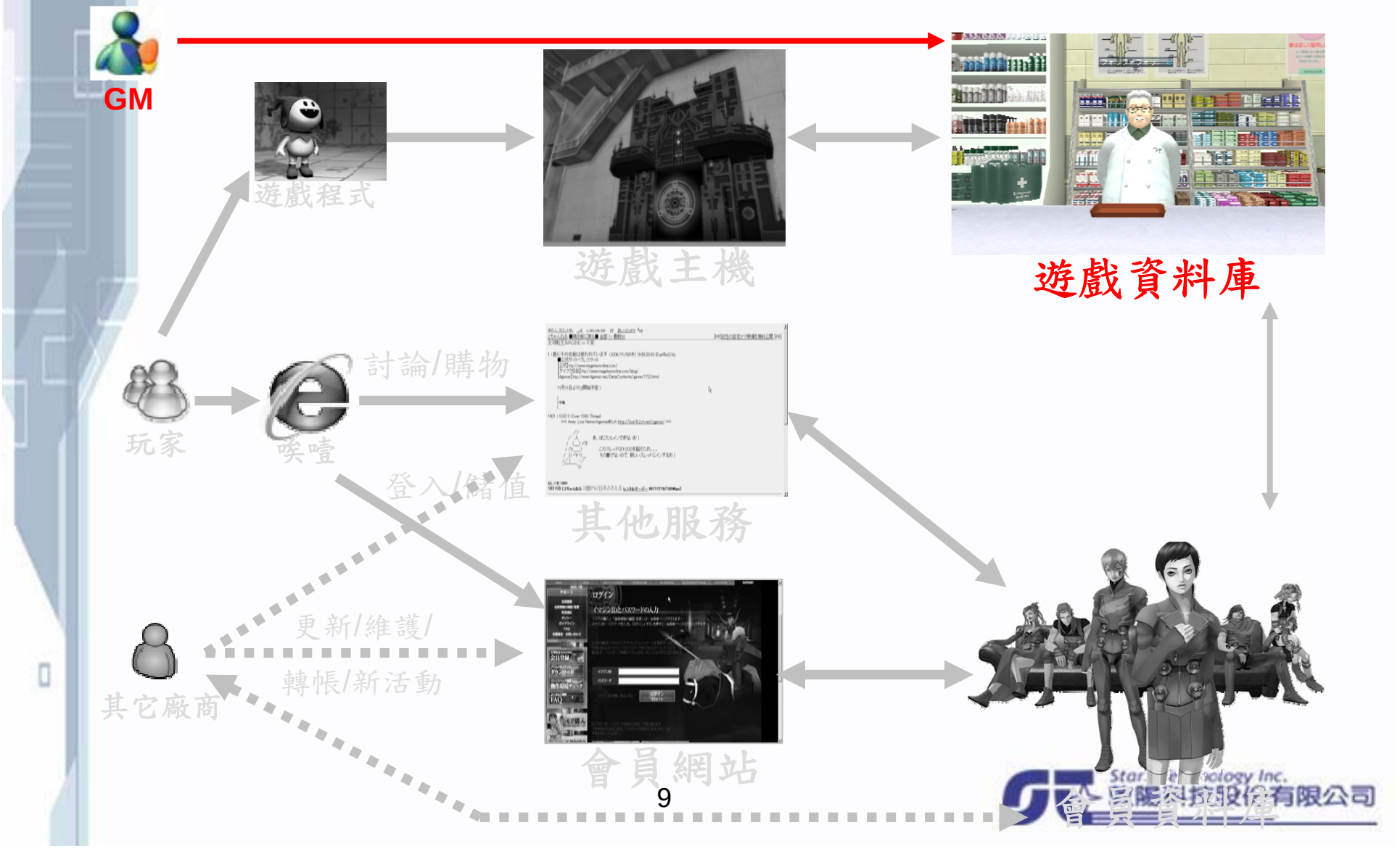
會員網站

會員資料庫

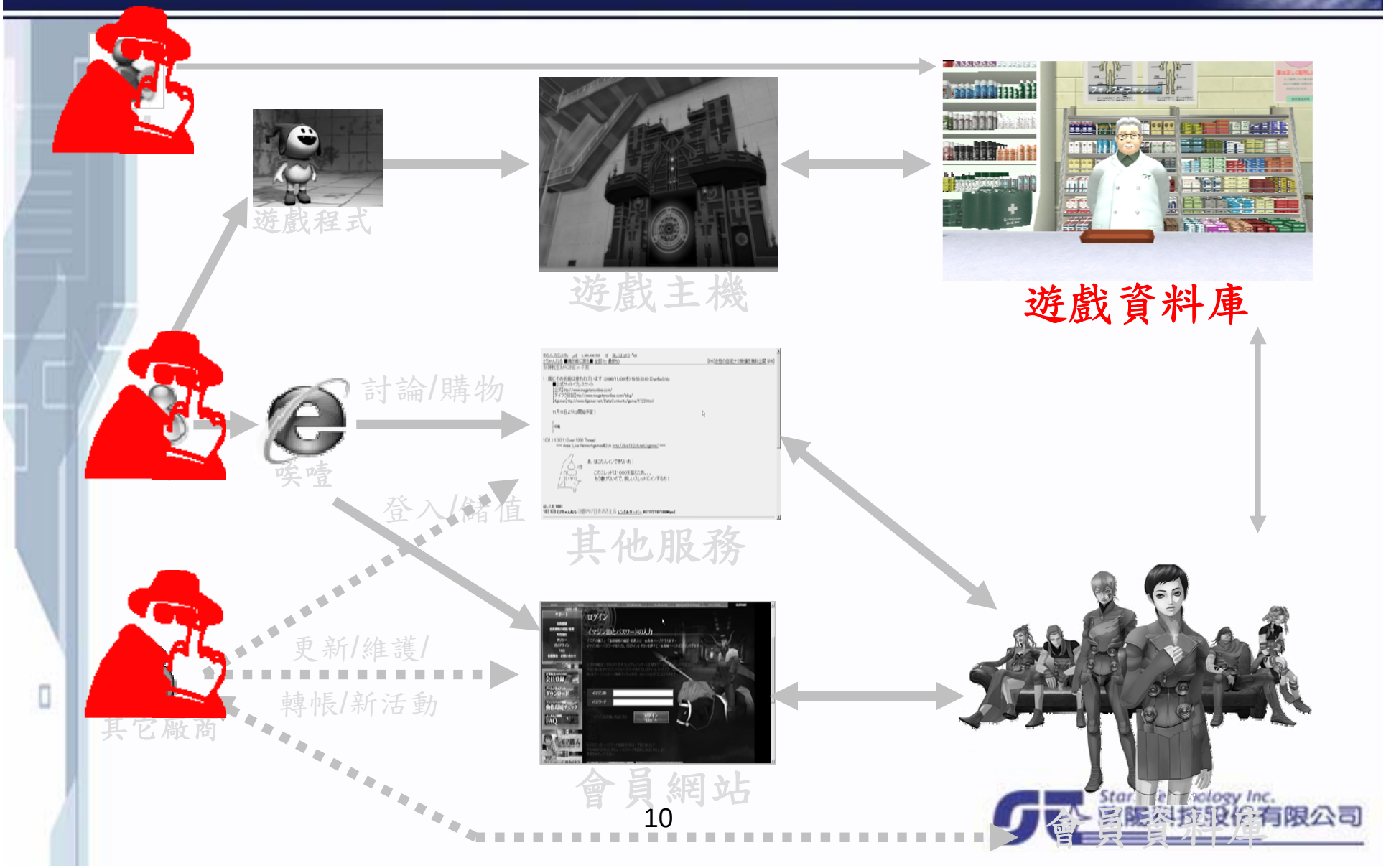
存取途徑-第三方廠商


遊戲程式
遊戲主機
遊戲資料庫
玩家
瀛噎
討論/購物
登入/儲值
其他服務
更新/維護/
轉帳/新活動
其它廠商
會員網站
會員資料庫

存取途徑-GM

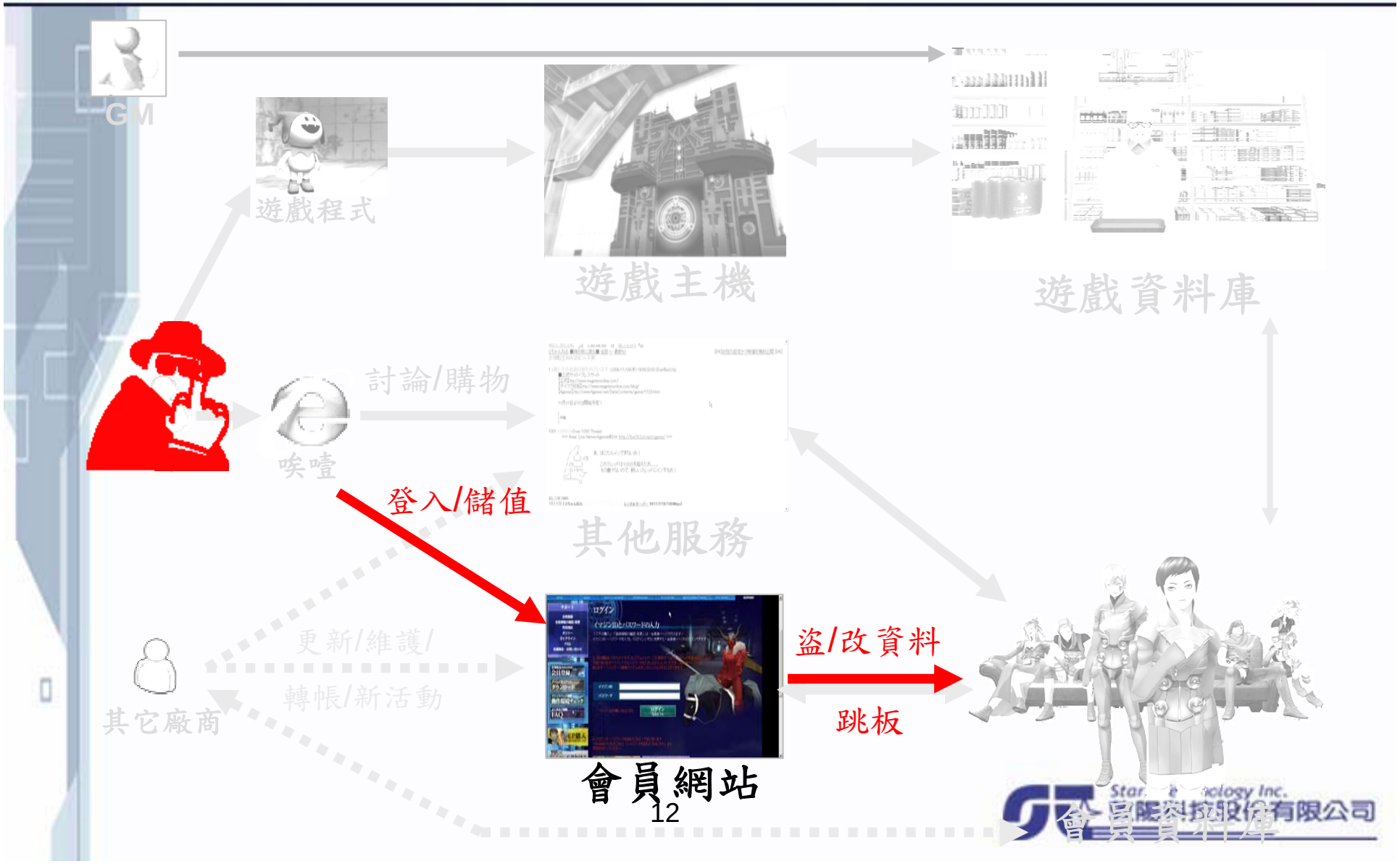

GM
遊戲程式
遊戲主機
遊戲資料庫
玩家
瀛嘻
討論/購物
登入/儲值
其他服務
更新/維護/
轉帳/新活動
其它廠商
會員網站
會員資料庫

存取途徑-駭客



母體駭人？人駭母體？

攻擊官網/儲值網


GM
遊戲程式
遊戲主機
遊戲資料庫
討論/購物
唉噎
登入/儲值
其他服務
更新/維護/
轉帳/新活動
其它廠商
盜/改資料
跳板
會員網站
會員資料庫

迷思: 使用SSL = 網站很安全?

- 對於 SSL 的期待:
  - “我們網站用 SSL，不怕資料被竊聽，所以是安全的！”
  - “我們 SSL 用了 強加密，所以很安全！”
  - “我們使用 VeriSign 的 SSL 憑證，所以非常安全！”
- 事實上，使用SSL ≠ 作好Application Security
  - 多數 SSL 僅提供 Client 辨識 Server 的身分, 以及**連線過程的私密性**
  - Web AP安全和資料傳輸的安全，是屬不同層次的問題
  - 資料加密的連線內容，防火牆/IDS/IPS是看不懂的！
  - 當**駭客**化身/偽裝成**使用者**時...?!

Stark Technology Inc.
敦陽科技股份有限公司

SQL中出(SQL Injection)

- 下面是一段登入檢查程式碼 (ASP+MSSQL):

```
set oConn = Server.CreateObject("ADODB.Connection")

oConn.Open "driver={SQL
   Server};server=(local);uid=sa;pwd=;database=db1"

sqlstr = "select * from Accounts where Username='" &
   Request("username") & "' and Password='" &
   Request("password") & "'"

set rs = oConn.Execute(sqlstr)

......
```

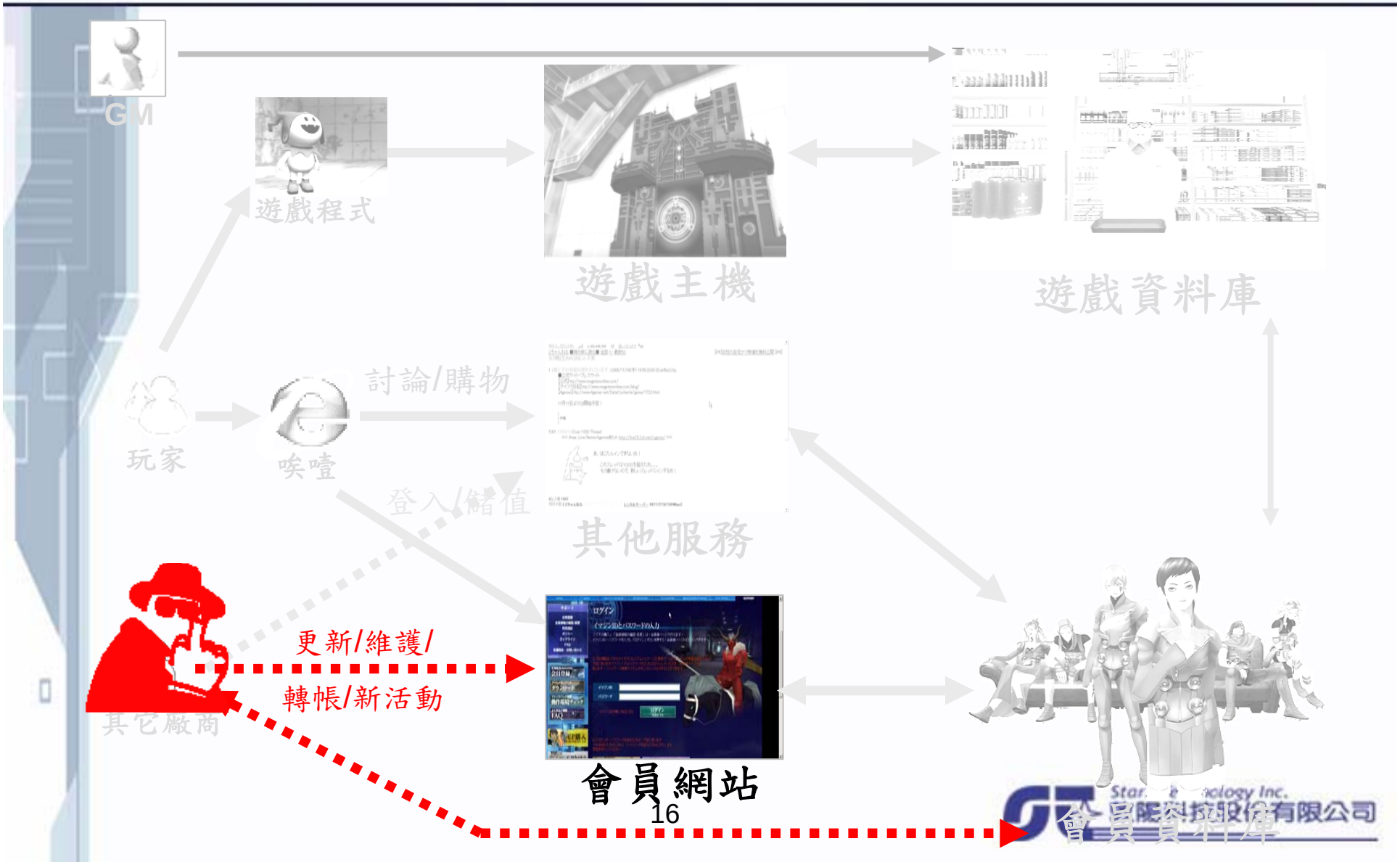
- 某個晚上，網站掛了，客戶資料也外流了，可是，防火牆、IDS/IPS、防毒都查不到...

Stark Techno 敦陽科技 限公司

什麼是SQL中出？

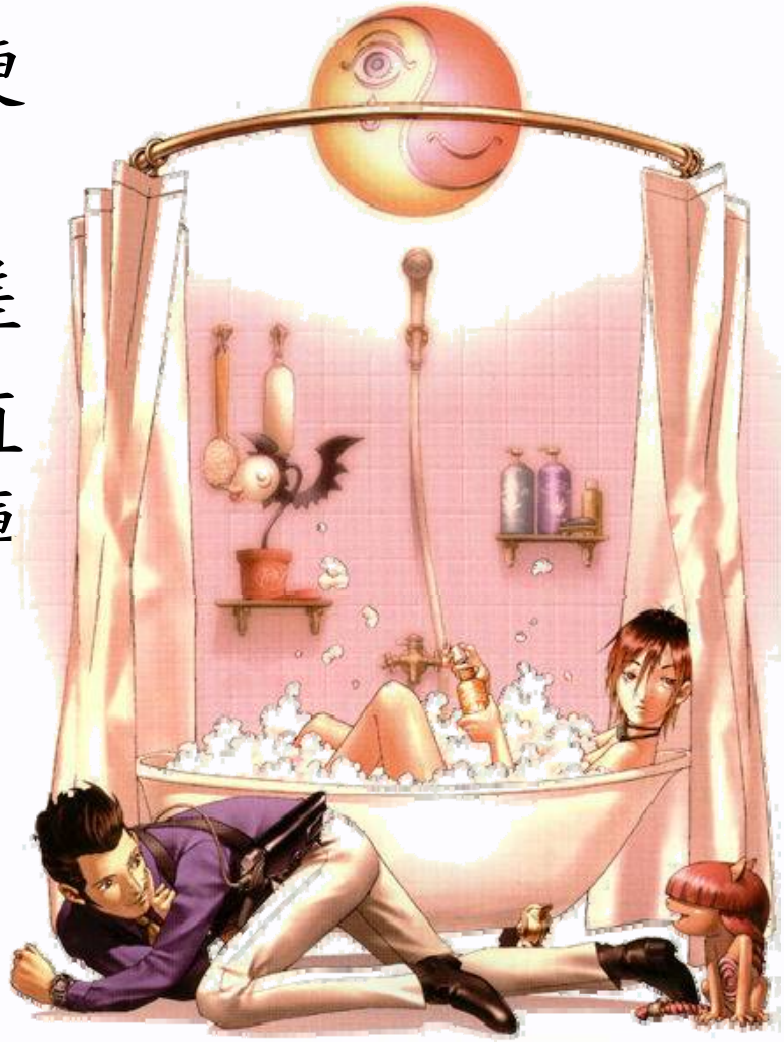
Stark Technology Inc.
敦陽科技股份有限公司

攻擊後台


GM
遊戲程式
遊戲主機
遊戲資料庫
玩家
唉噎
討論/購物
登入/儲值
其他服務
其它廠商
更新/維護/
轉帳/新活動
會員網站
會員資料庫

後台「被」管理

- 供管理者或維護商方便
- 以為只有少數人知道，安全考量比正式網頁差
- 管理功能強大，還可直接上下傳檔案與資料庫
- 缺乏登入記錄機制
- 沒有限制來源是誰



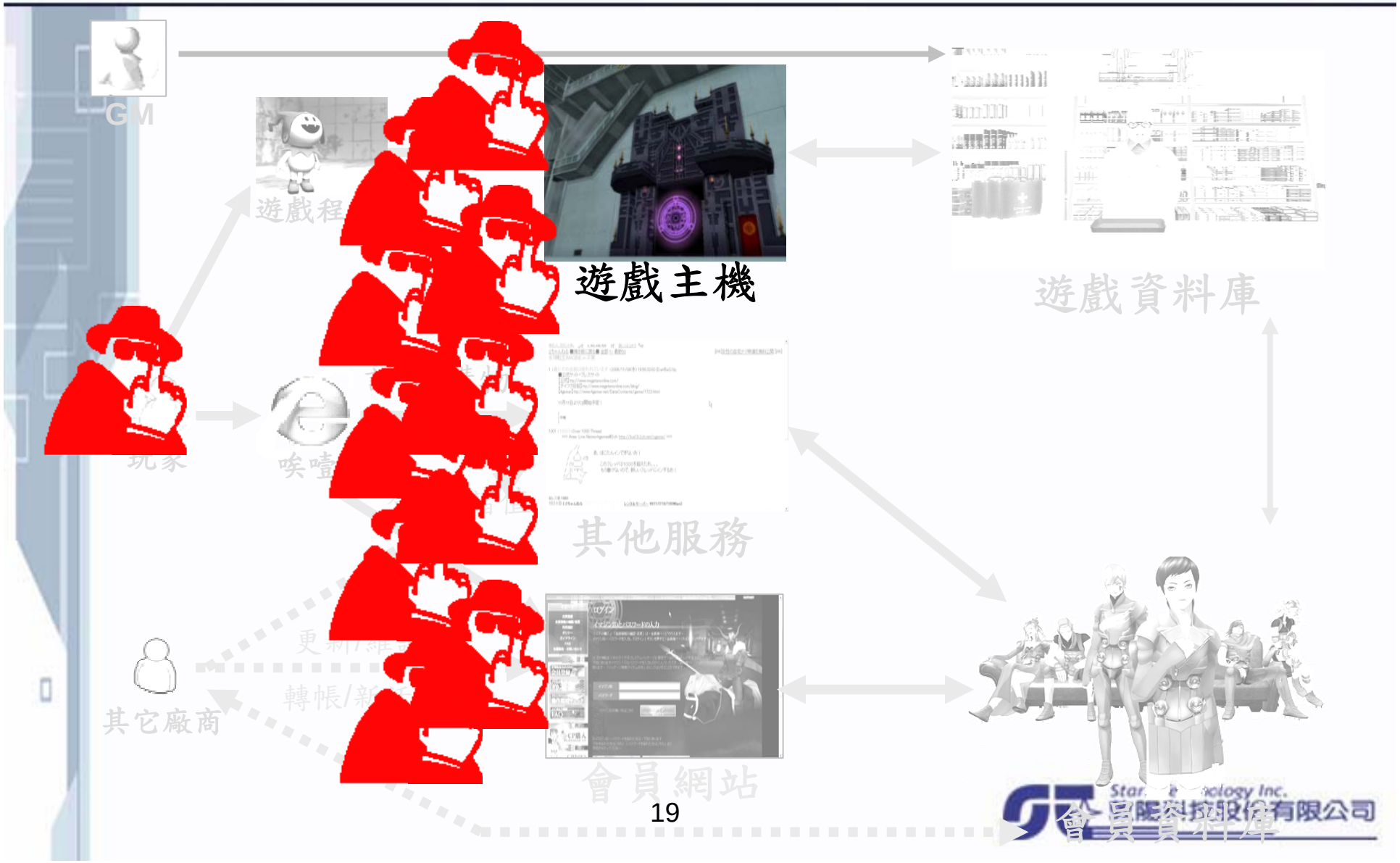
Stark Technology Inc.
敦陽科技股份有限公司

管得動第三方嗎？

- 開放直接連接資料庫？
- 開放讓合作廠商自由上傳網頁？
- 臨時的行銷活動網頁？登記抽公仔
- 有監控廠商作過什麼事嗎？
- 舊網頁下線了嗎？
- 合作的金流物流邏輯？

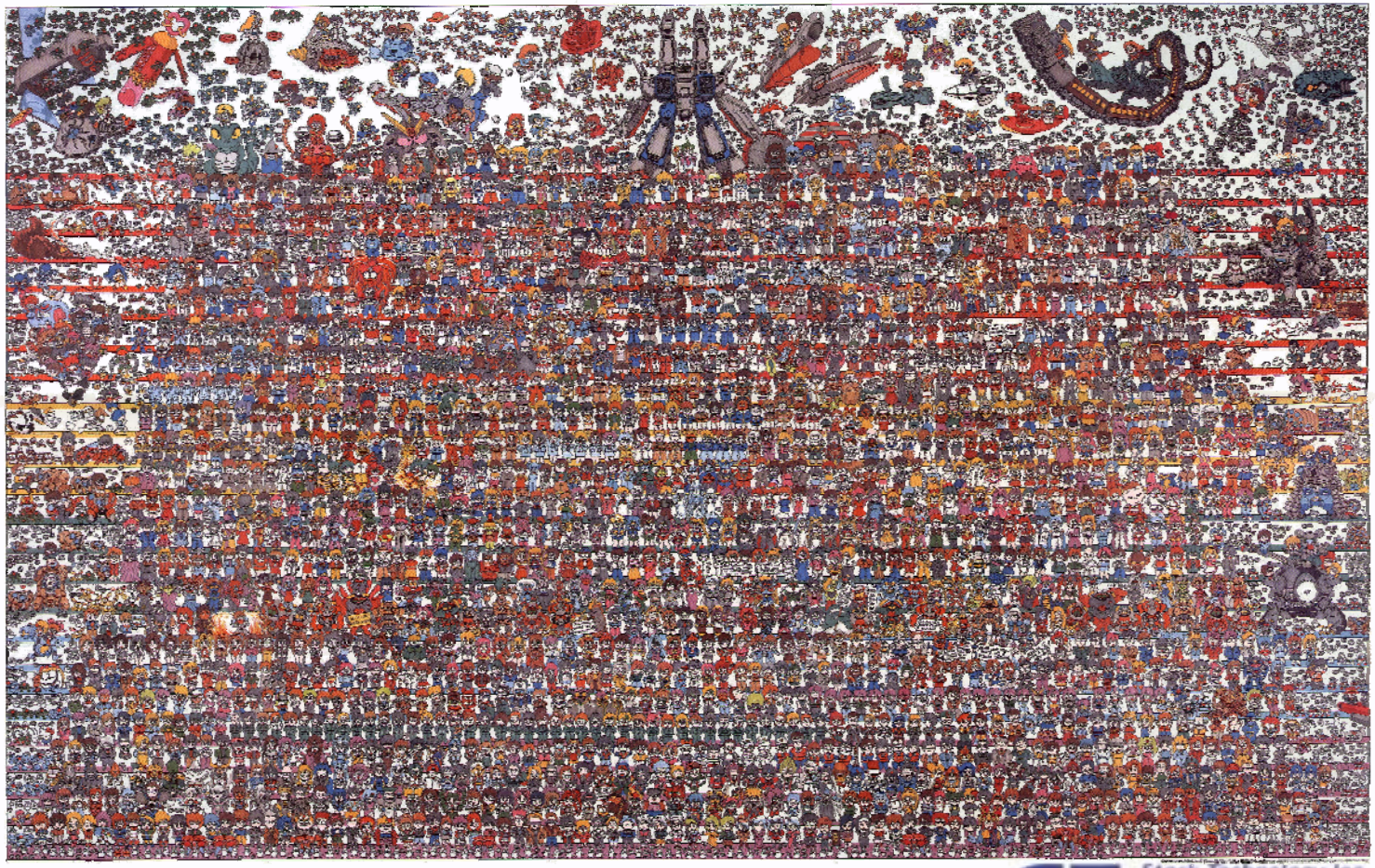
Stark Technology Inc.
敦陽科技股份有限公司

攻擊遊戲主機



DoS的用意

- 勒索！



Stark Technology Inc.
敦陽科技股份有限公司

內賊

遊戲程式

遊戲主機

遊戲資料庫

玩家

唉噎

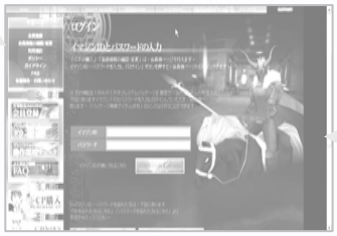
討論/購物

其他服務

登入/儲值

其它廠商

更新/維護/轉帳/新活動



會員網站

會員資料庫

真實案例

抱歉是機密不能說...orz...

聽說 遊戲業界案例比銀行多超多...

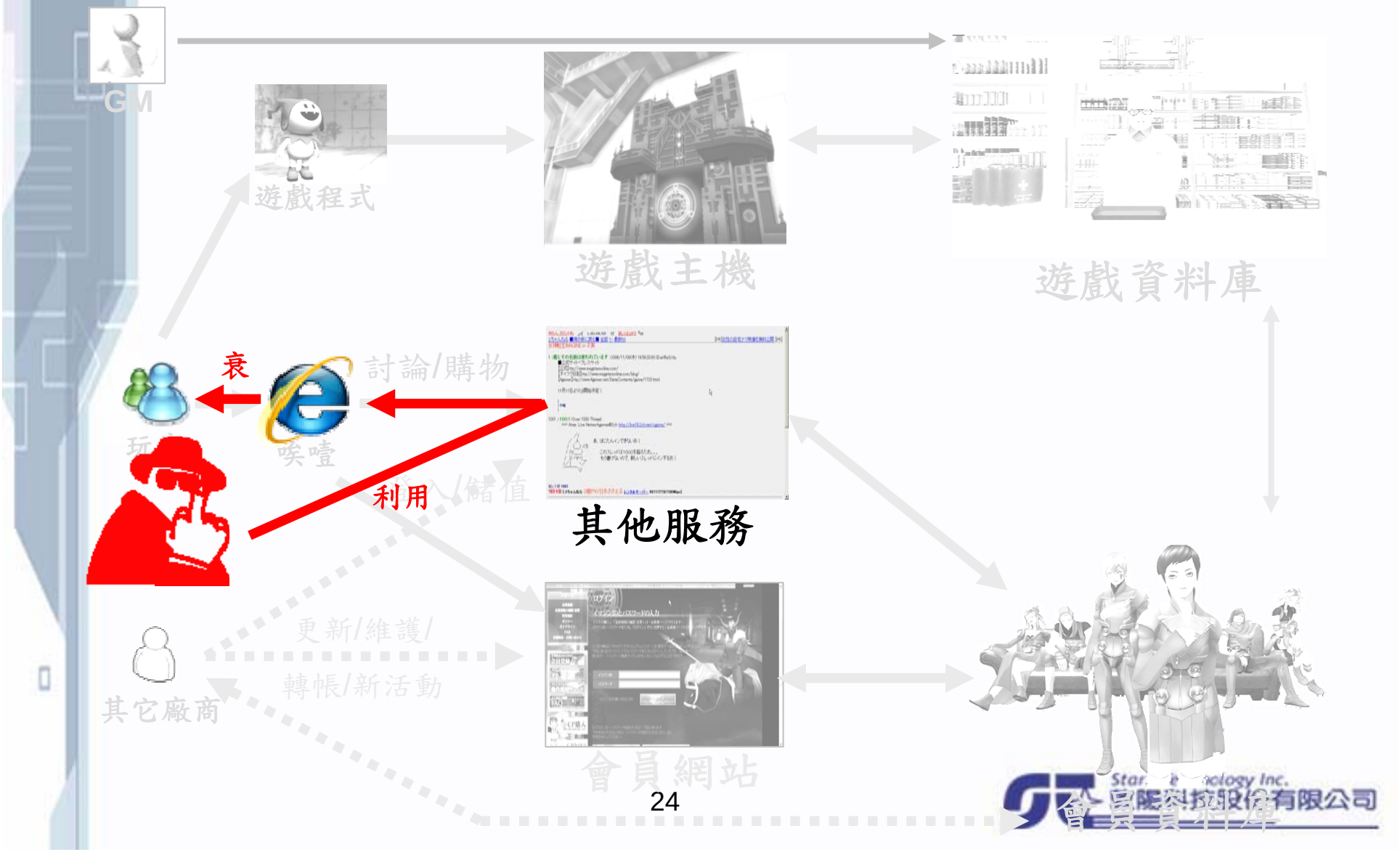
敦陽科技股份有限公司

好康滴加啦！

玩？還是被玩？

...It's a Question...

攻擊官網/儲值網


GM
遊戲程式
遊戲主機
遊戲資料庫
衰
討論/購物
玩
喚噎
利用
儲值
其他服務
更新/維護/
轉帳/新活動
其它廠商
會員網站
會員資料庫

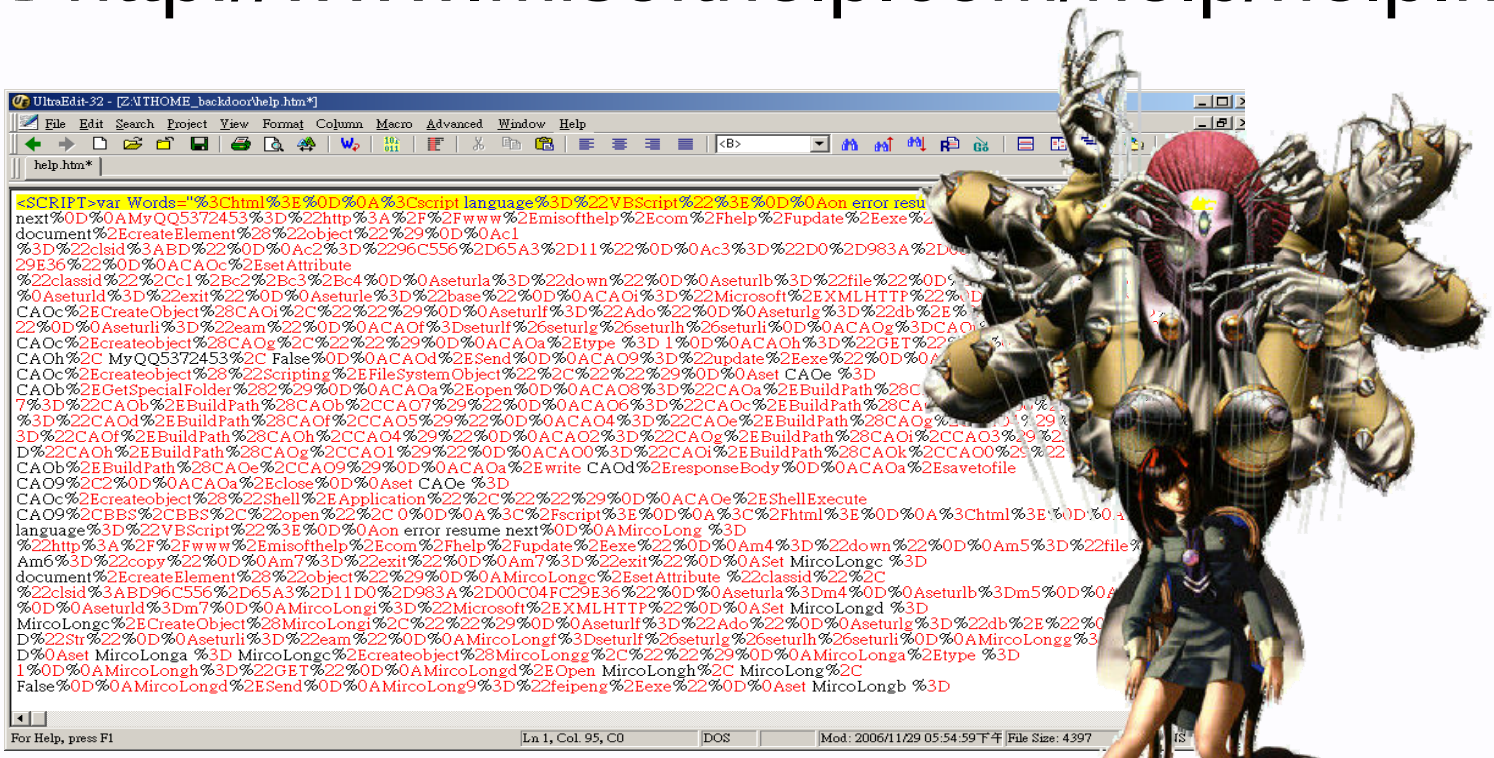
一、加料型

- 資料庫被改
- 網頁被改
- 未限制上傳新檔案
- 討論區留言裏允許特殊語法
- …

敦陽科技股份有限公司

難以分辨的木馬

- http://www.misofthelp.com/help/help.htm



埋木馬...盜帳號

Stark Technology Inc.
敦陽科技股份有限公司

二、反射型

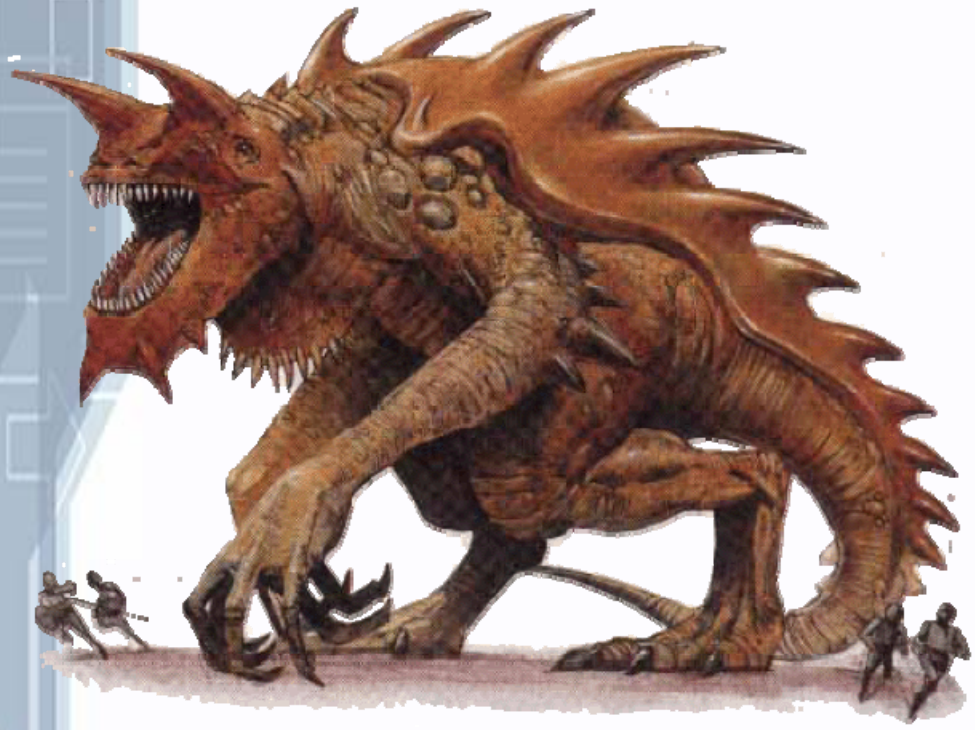
- 駭客發文：「管理者是白癡！」，內文含偷取cookie的語法
- 管理者用管理權限登入看文，殺文
- 管理者cookie被偷走
- 駭客利用管理者權限登入後台
- 利用資料庫備份拿下主機，建立跳板

地下城主指南

遊戲裏最有錢的角色？

Stark Technology Inc.
敦陽科技股份有限公司

誰是大肥羊？



宰了會掉很多錢！

宰了會掉高等寶！

宰了他可以出名！

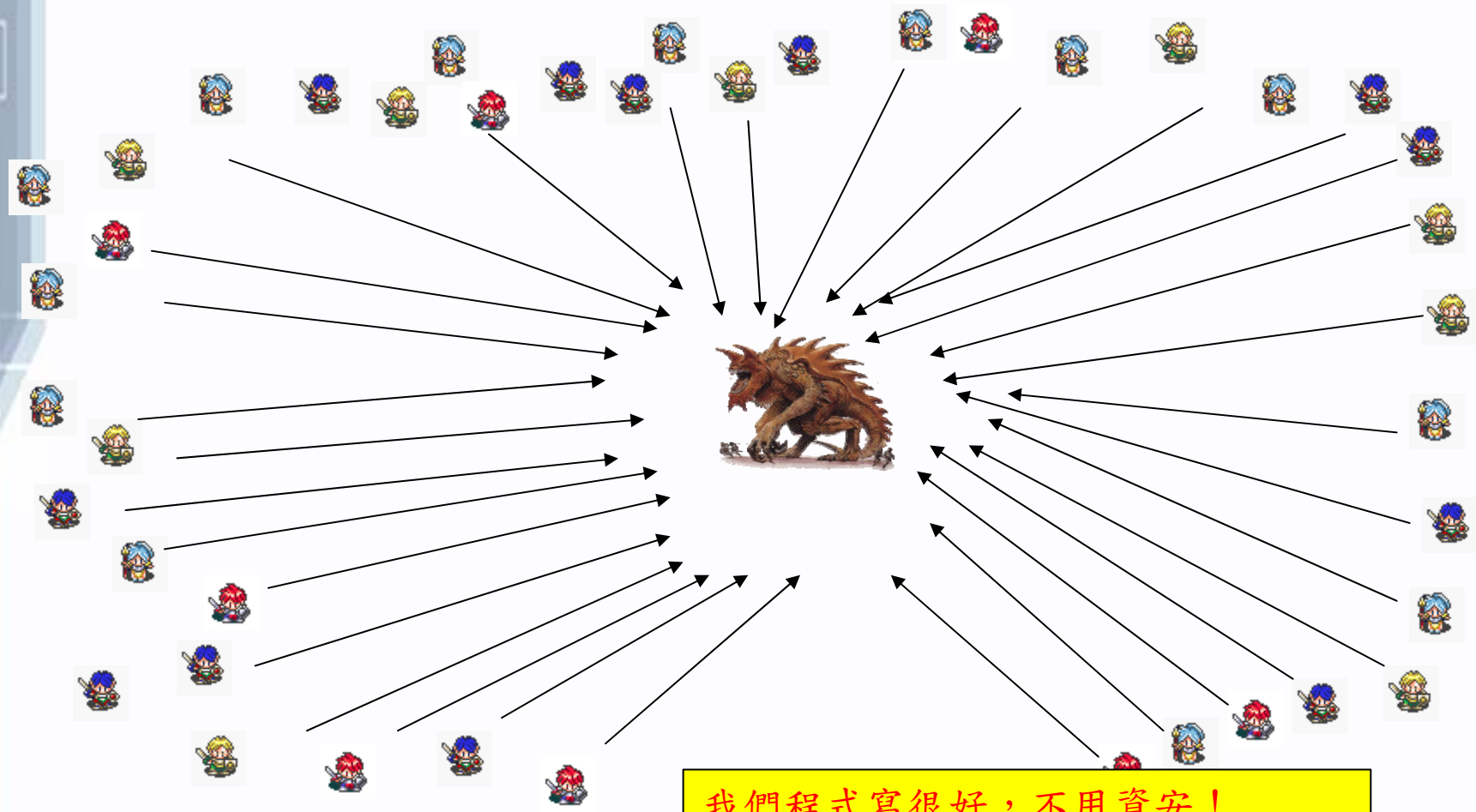
沒人真的怕……

……大家都想宰他!

這工作有沒有很熟悉？

Stark Technology Inc.
敦陽科技股份有限公司

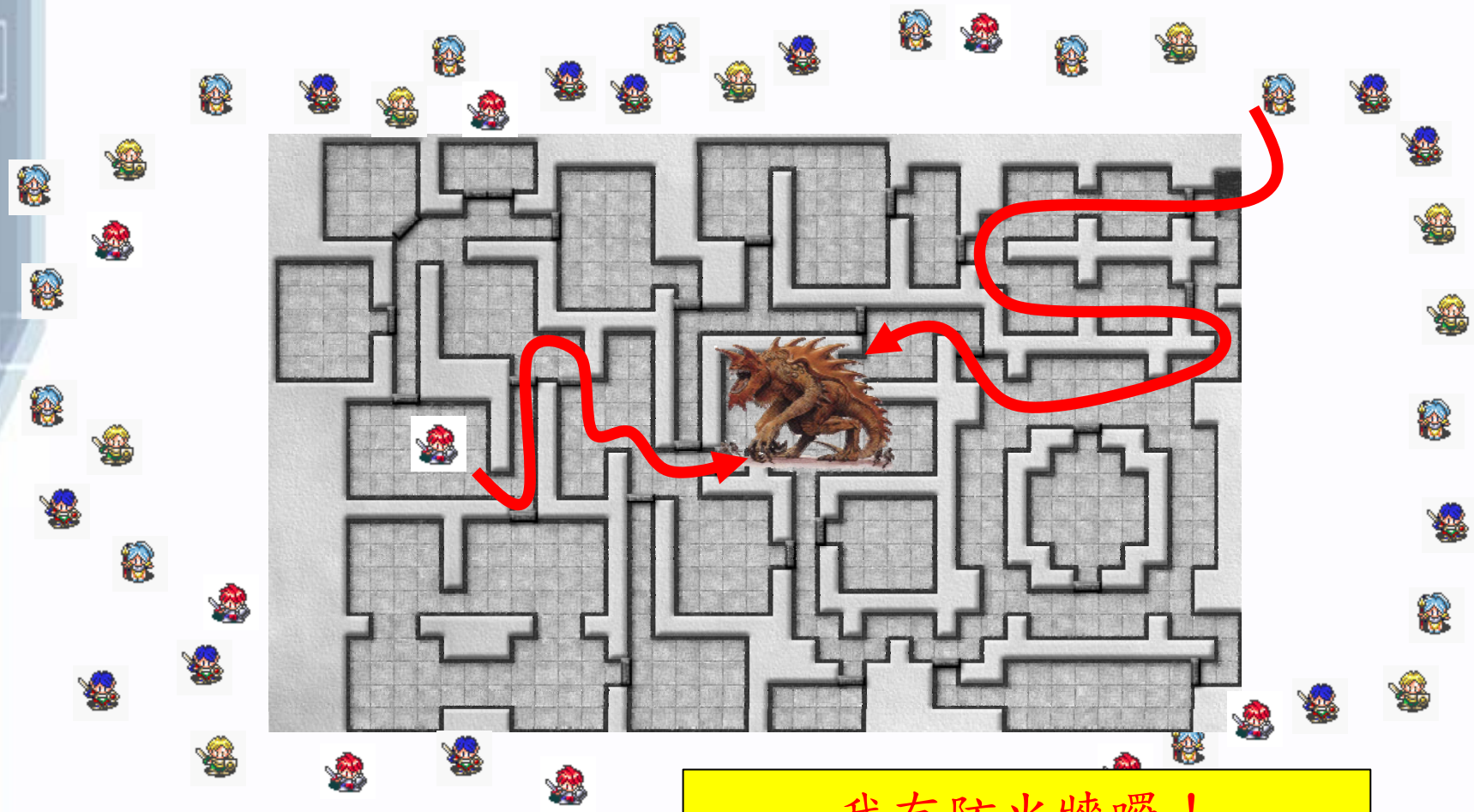
不蓋城的王



我們程式寫很好，不用資安！
我們流量太大，不能裝防火牆！

Stark Technology Inc.
敦陽科技股份有限公司

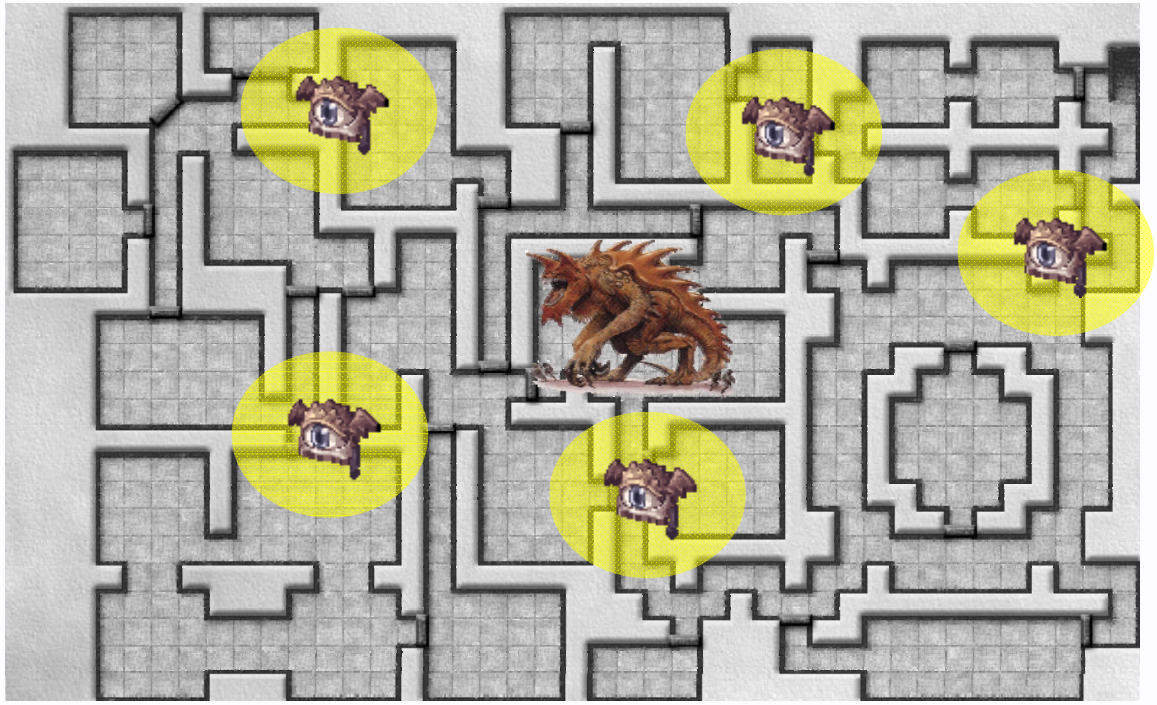
防火牆



我有防火牆囉！

Stark Technology Inc.
敦陽科技股份有限公司

IDS/IPS



來裝入侵偵測系統

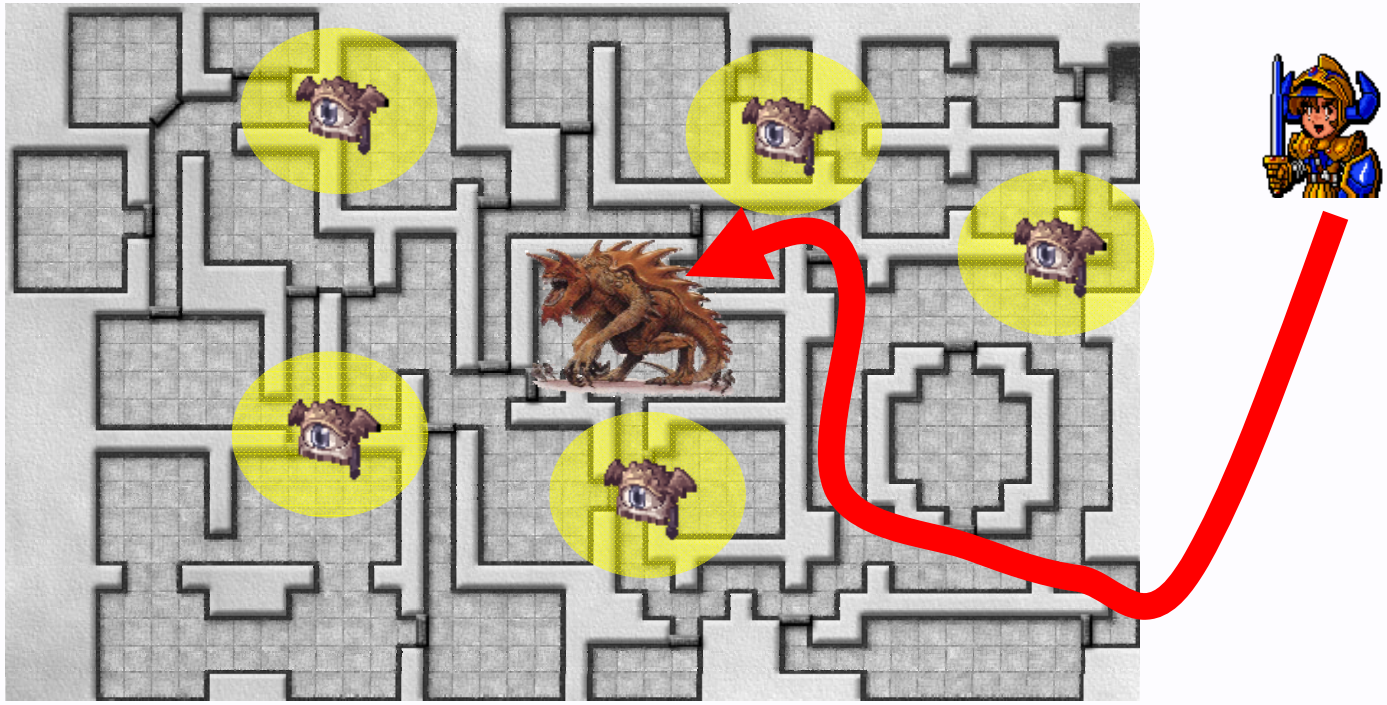
Stark Technology Inc.
敦陽科技股份有限公司

IDS/IPS的不足

- 無法辨識SSL流量
- 只能看得懂認識的攻擊行為
- 只針對已知的程式或系統
- 需搭配人力24小時監看
- 無法辨識後台猜測
- 只辨識簡易的SQL中出攻擊
- 無法了解金流邏輯問題

Stark Technology Inc.
敦陽科技股份有限公司

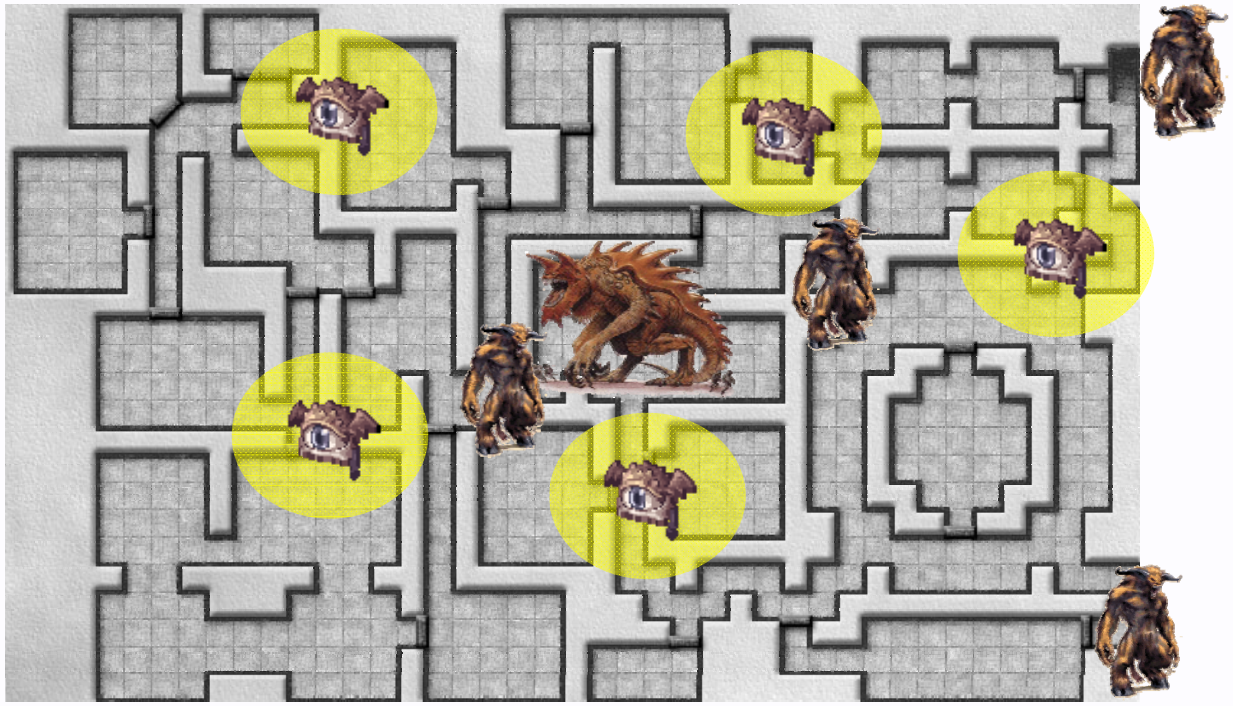
評估與稽核



先來了解一下自己！

Stark Technology Inc.
敦陽科技股份有限公司

應用層防護



守門員檢查應用程式內容

Stark Technology Inc.
敦陽科技股份有限公司

工商服務時間

敦陽科技提供服務

安全規劃
弱點稽核
滲透測試
木馬移除
緊急應變
資安諮詢
教育訓練

Stark Technology Inc.
敦陽科技股份有限公司

問題與討論

Stark Technology Inc.
敦陽科技股份有限公司