不久不久之前，

在一個很近很近的雲端...

行跡大戰

雲 力 覺 醒

雲端與大數據時代的駭客入侵

時間進入雲端時代，資訊共和聯盟的絕地工程師獲得雲力建造出全新的伺服環境。他們應用大數據運算來提供雲端伺服、雲端防毒、雲端備援以將資安風險分散，維繫快速穩定的資訊環境...

但在不為人知的黑暗一隅，匿名勢力在強力誘因驅動下、也快速進化適應了雲端環境。黑暗雲力經過大數據運算的加持，悄悄形成了新的地下產業帝國...

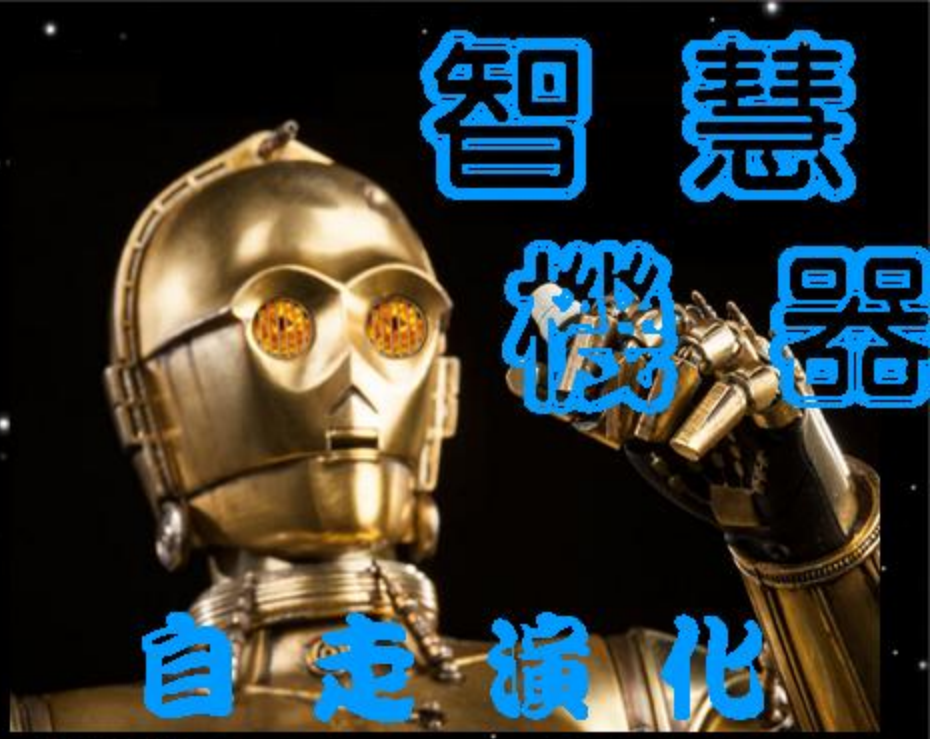
首部曲

威脅潛伏

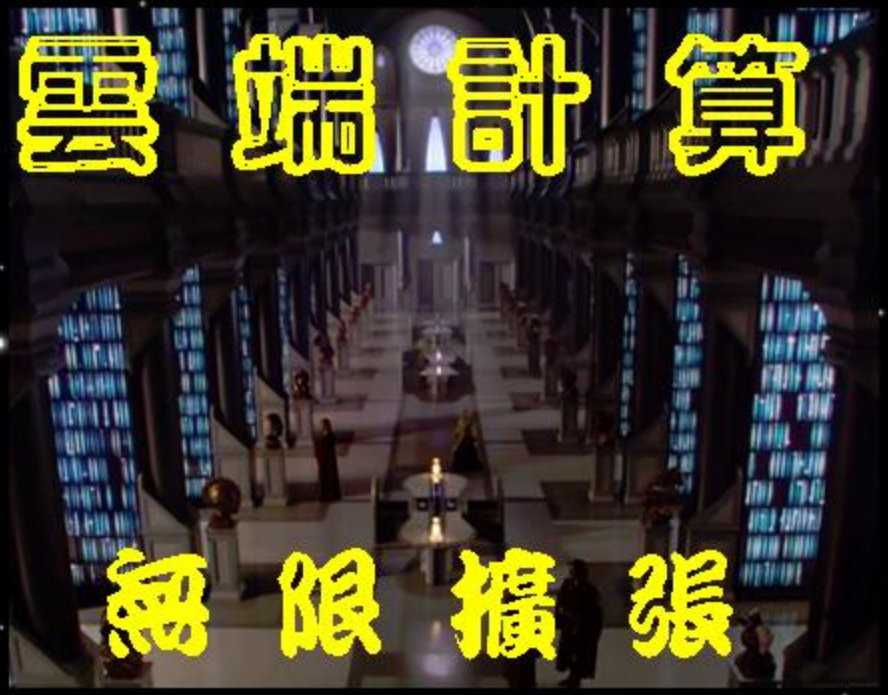
鄔賀銓，2013年8月中國互聯網大會

大智格雲時代

大
數據
海量情報


智慧
機器
自走演化

移動裝置
機動作業


雲端計算
無限擴張

大數據

大 (Volume)

處理TB級資料量

快 (Velocity)

即時輸入資料

瞬間輸出資訊

雜 (Variety)

不同資料交叉分析

疑 (Veracity)

辨別來源資料可信度

大智移雲

大數據

大 (Volume)

處理TB級資料量

快 (Velocity)

即時輸入資料

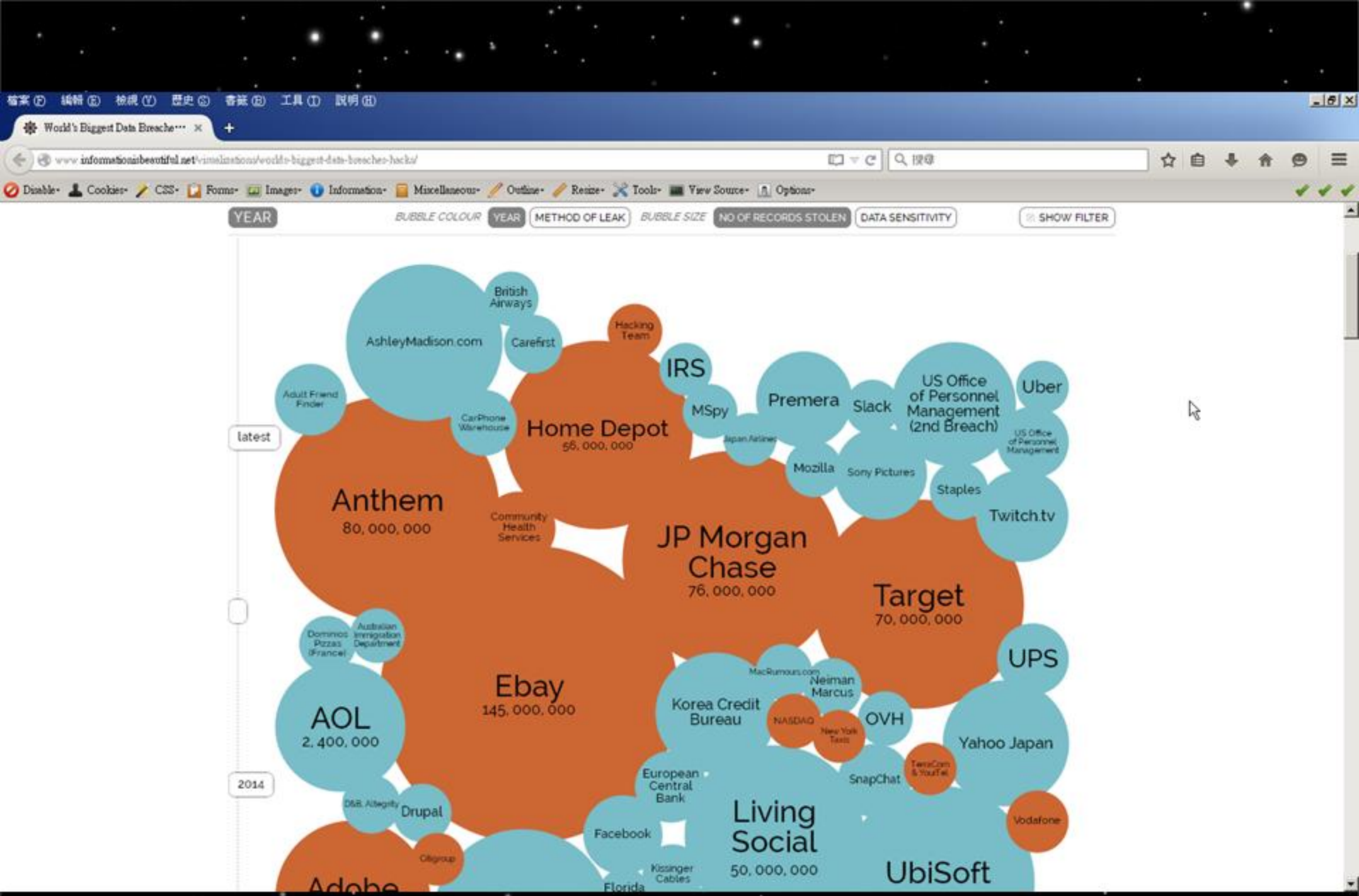
瞬間輸出資訊

雜 (Variety)

不同資料交叉分析

疑 (Veracity)

辨別來源資料可信度

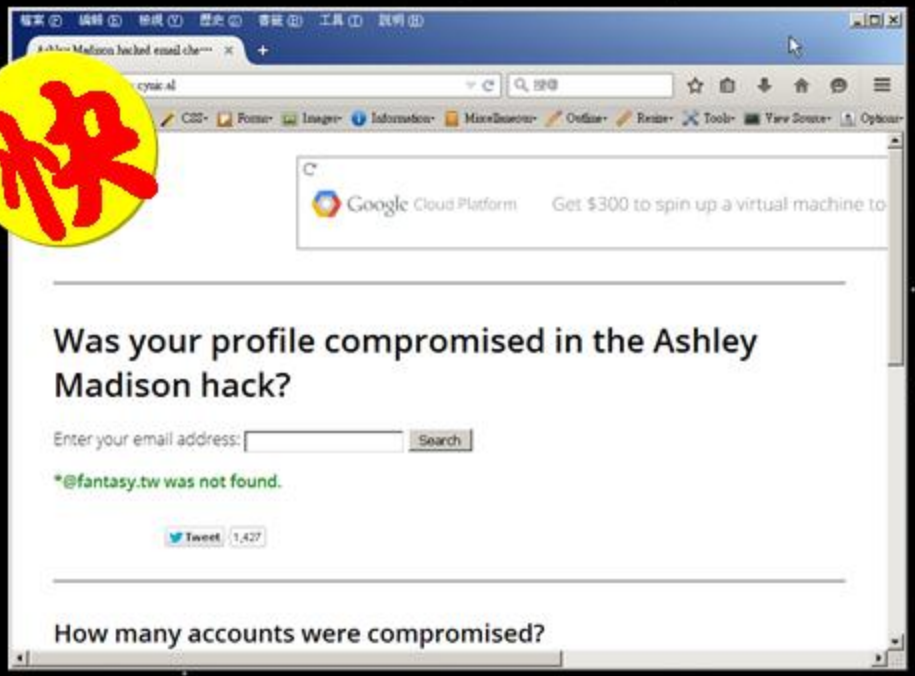


資料來源：http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

大

AshleyMadison.com
美國最大偷情網
37,000,000筆

快



偷情網站遇駭 美數百官員入會遭抓包

發稿時間：2015/08/21 05:48　最新更新：2015/08/21 08:41　字級：A- A+

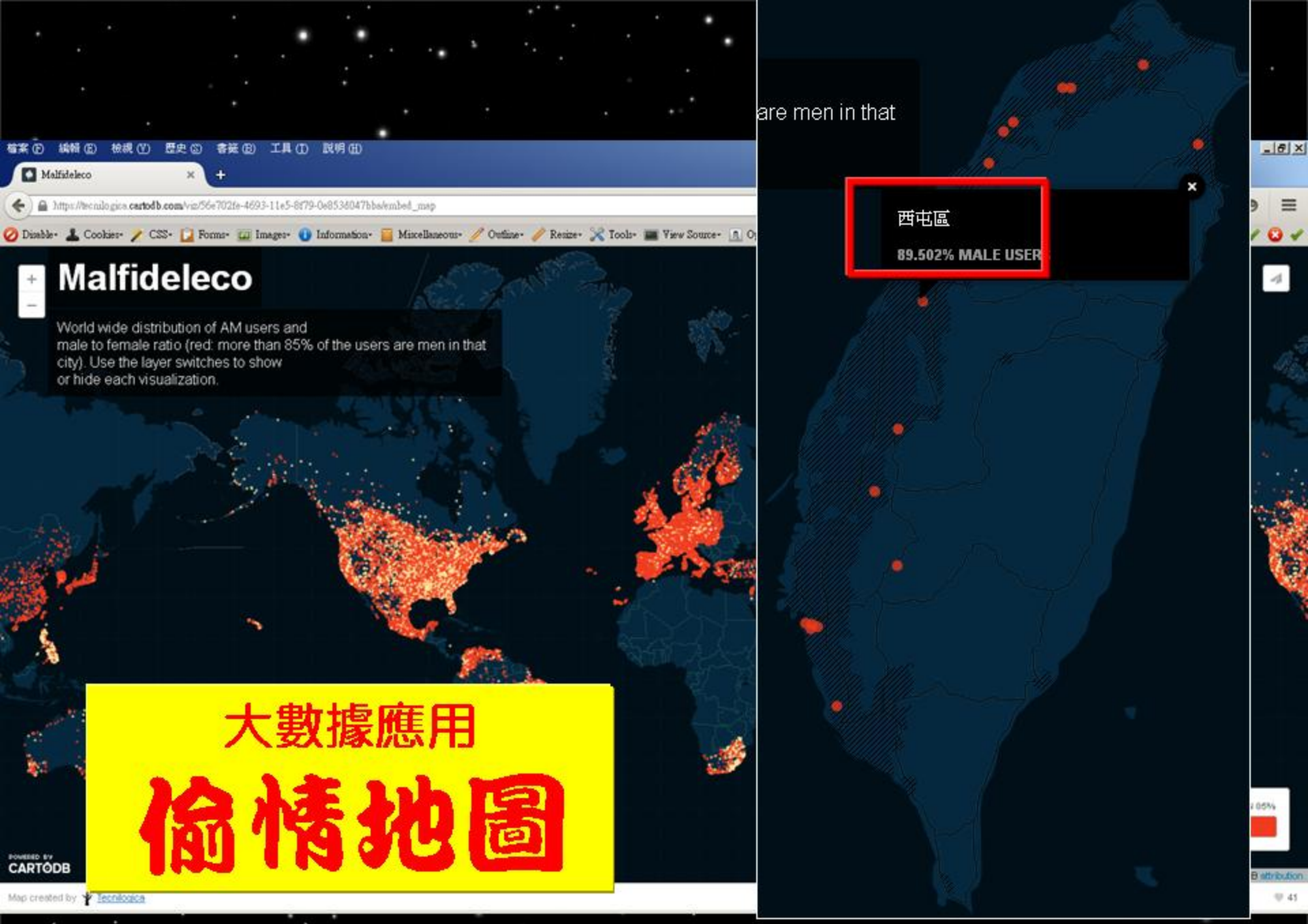
偷情網站Ashley Madison遭駭客入侵，大批用戶資料外洩，美聯社追查發現，部分用戶甚至是聯邦政府機構員工。（圖取自Ashley Madison網頁 www.ashleymadison.com）

雖

疑

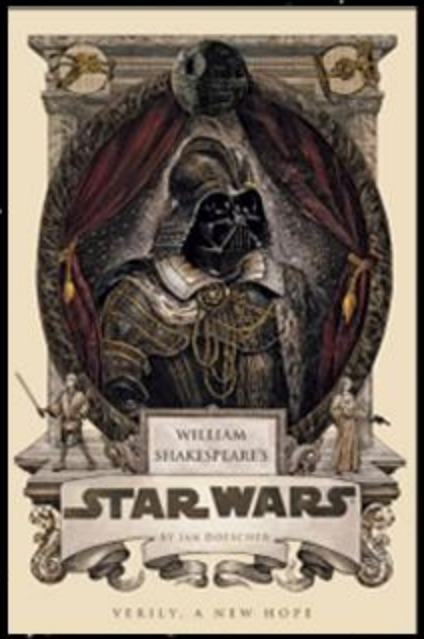
控偷情網站未刪資料 受害者集體提告

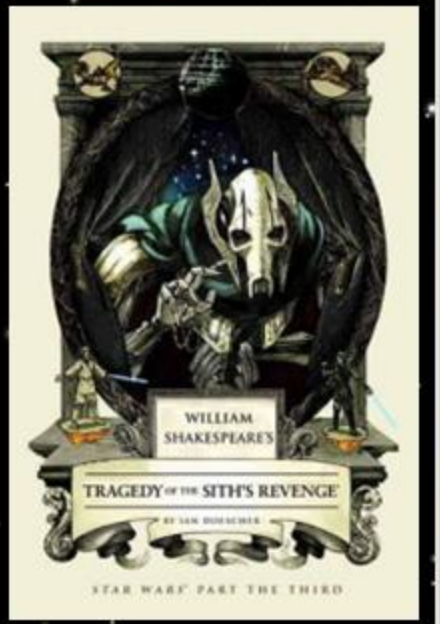
1 / 26　法新社



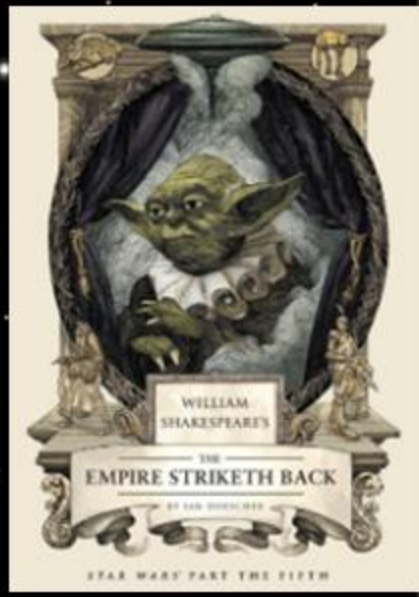
資料來源：https://tecnilogica.cartodb.com/viz/56e702fe-4693-11e5-8f79-0e853d047bba/embed_map

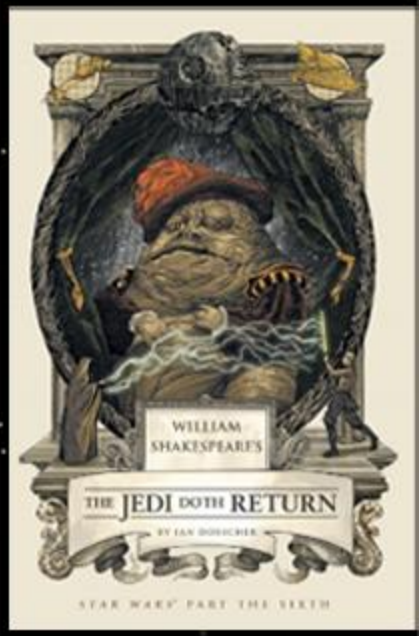
資料科學


WILLIAM SHAKESPEARE'S
STAR WARS
BY IAN DOESCHER
VERILY, A NEW HOPE


WILLIAM SHAKESPEARE'S
TRAGEDY OF THE SITH'S REVENGE
BY IAN DOESCHER
STAR WARS PART THE THIRD

檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
駭客也變文青：利用世界…
www.ithome.com.tw/news/97780
R2D2
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools
iThome
駭客也變文青：利用世界名著《理性與感性》躲避防毒程式偵測
思科指出，駭客使用19世紀的文學作品來遮掩21世紀的安全威脅，這只是用來躲避偵測的手法之一，事實上，有許多惡意程式的作者利用資料科學來建立由電腦產生的首頁，以這些看似平常的首頁來欺騙使用者，當中有些流量來自惡意廣告。
讚 1.6萬 按讚加入iThome粉絲團
讚 分享 270
g+1 12
文/ 陳曉莉 | 2015-07-29 發表


WILLIAM SHAKESPEARE'S
THE EMPIRE STRIKETH BACK
BY IAN DOESCHER
STAR WARS PART THE FIFTH


WILLIAM SHAKESPEARE'S
THE JEDI DOTH RETURN
BY IAN DOESCHER
STAR WARS PART THE SIXTH

智慧機器

機器學習

自我分析進化

懶人生活

- 無人車
- 智慧病床
- 智慧手

工業2.0

智慧工廠 + 物聯網

人工大腦

大智移雲

智慧機器

智慧機器的重心是

道德！

Level 4: 機器自我道德
Level 3: 機器演化道德
Level 2: 道德程式化
Level 1: 道德意識
Level 0: 沒什麼道德

資料來源：http://www.gartner.com/newsroom/id/3007417

记录每天的运动数据
12:32 PM 26
走路上班
500步
慢跑
2000步
下班健身
5000步
和朋友逛街
3000步
深度睡眠
4小时
自动切换
睡眠模式

洗衣机漏洞简述
2.越权控制：洗衣机之间权限控制不严，bypass指令过滤
导致相互可发控制指令
攻击者
含有"C
不能发出
Bypass：大小写绕过

CCTV 13
新闻
电视被"黑"

九阳豆浆机
@黄源小童鞋
360
安全播报平台

移動裝置

上班族更忙

行動特助

搭捷運必備

行動生活

當老公超恨

行動購物

慣老闆最愛

行動辦公室

大智移雲

移動裝置

偷 企業資料

行動特助

搶 下載病毒通常不收錢

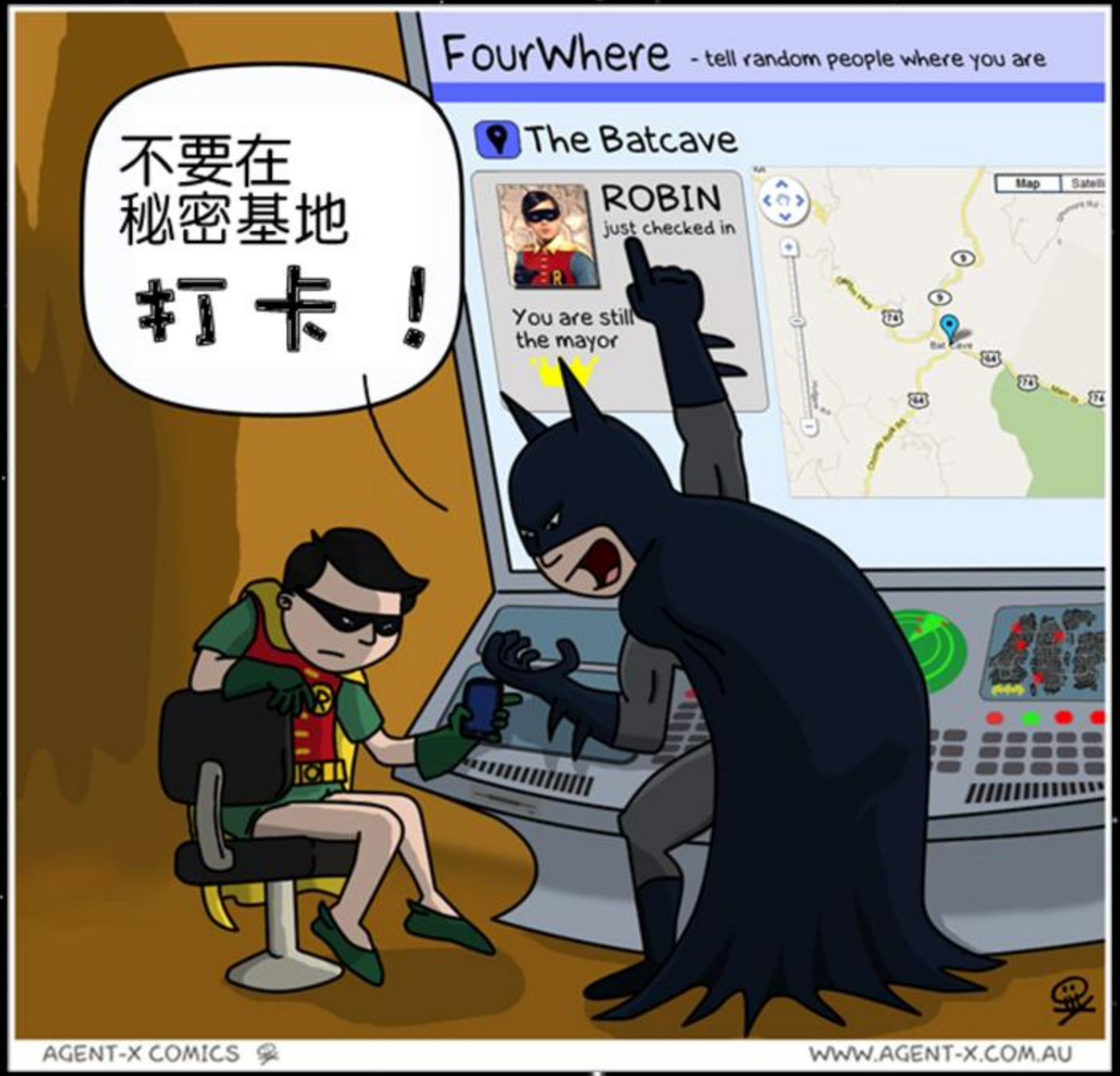
行動生活

搶 身份驗證、信用卡

行動購物

騙 隨時可進門

行動辦公室


不要在
秘密基地
打卡！
FourWhere - tell random people where you are
The Batcave
ROBIN
just checked in
You are still
the mayor
Map
AGENT-X COMICS
WWW.AGENT-X.COM.AU

想越獄？

雲端運算

上雲端架站

IaaS

上雲端開發

PaaS

上雲端服務

SaaS

大智移雲

雲端運算

專注、癲瘋

IaaS

毒瘤

PaaS

程式漏洞

SaaS

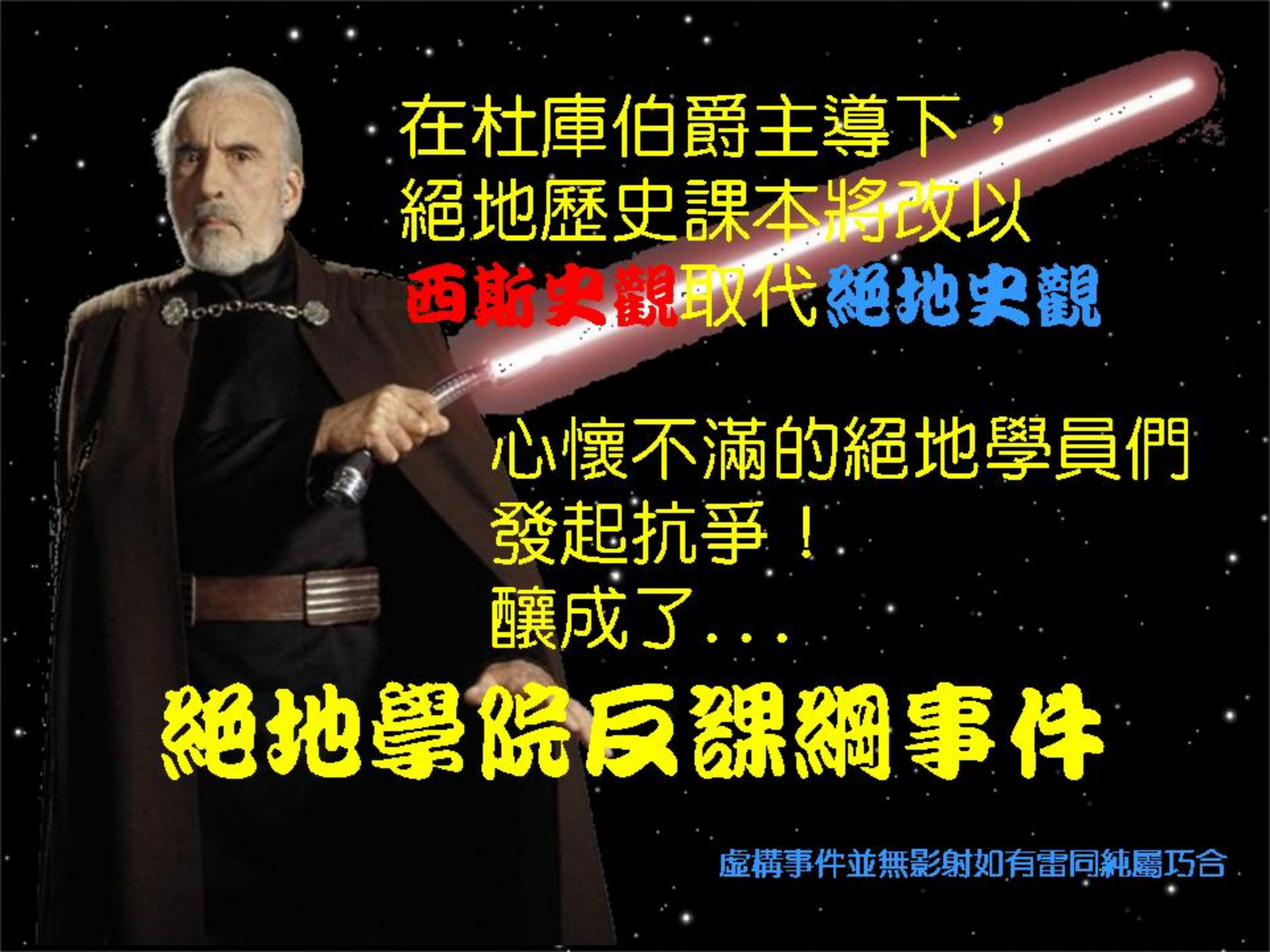
上雲端駭人

HaaS

二部曲

複製人

全面進攻


在杜庫伯爵主導下，
絕地歷史課本將改以
西斯史觀取代絕地史觀
心懷不滿的絕地學員們
發起抗爭！
釀成了...
絕地學院反課綱事件
虛構事件並無影射如有雷同純屬巧合

古典手法
單挑

絕地匿名者

一刀斃命

零時差
漏洞

受害者

提到網絡攻擊，最容易上手…又或者可以這樣說，只要有錢便可隨時發動到大型的攻擊的模式，DDoS 必定上榜，提到 DDoS 近年來即使本身並未從事IT，相信都總有聽過這名字，原來就在 2015 年的第一季，就有多達 8 個大型的 DDoS 發生，似乎 DDoS 已成爲一種最熱門的攻擊模式。

根據 Akamai 的報告，我們可以看到 2015 年第一季就 PLXrouted 網絡所觀察到的 DDoS 攻擊次數創新高，比起 2014 年第一季增加超過一倍，較上季則上升了超過 35%。然而，攻擊機制經已改變。去年最常見的攻擊均爲高頻寬但持續時間短的攻擊；但於 2015 年第一季，典型的 DDoS 攻擊每秒低於 10 Gbps（千兆位），並持續超過 24 小時。第一季有八個大型攻擊，每個均超過 100 Gbps。雖然比起 2014 年第四季少了一個巨型攻擊，但此等大型攻擊在一年前比較罕見。2015 年第一季觀察到最大型的 DDoS 攻擊是 170 Gbps。

鄉民起義

絕地匿名者

在討論區發文宣戰

鄉民

鄉民

鄉民

鄉民

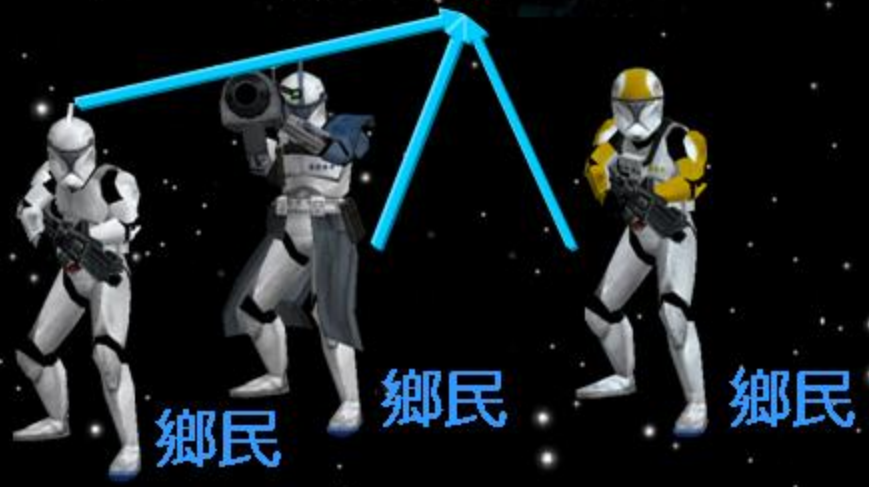
鄉民

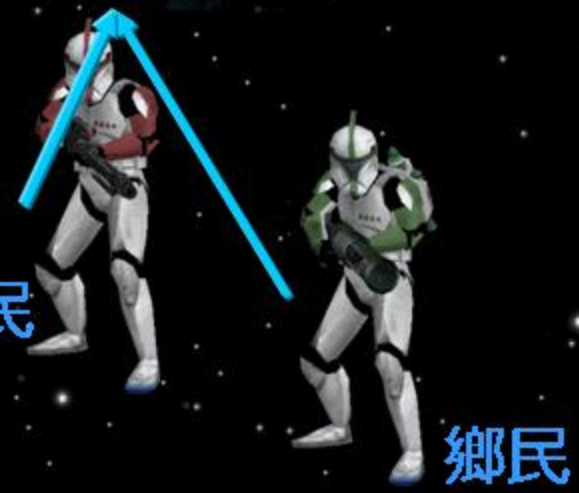
一起按F5
重整網頁

受害者

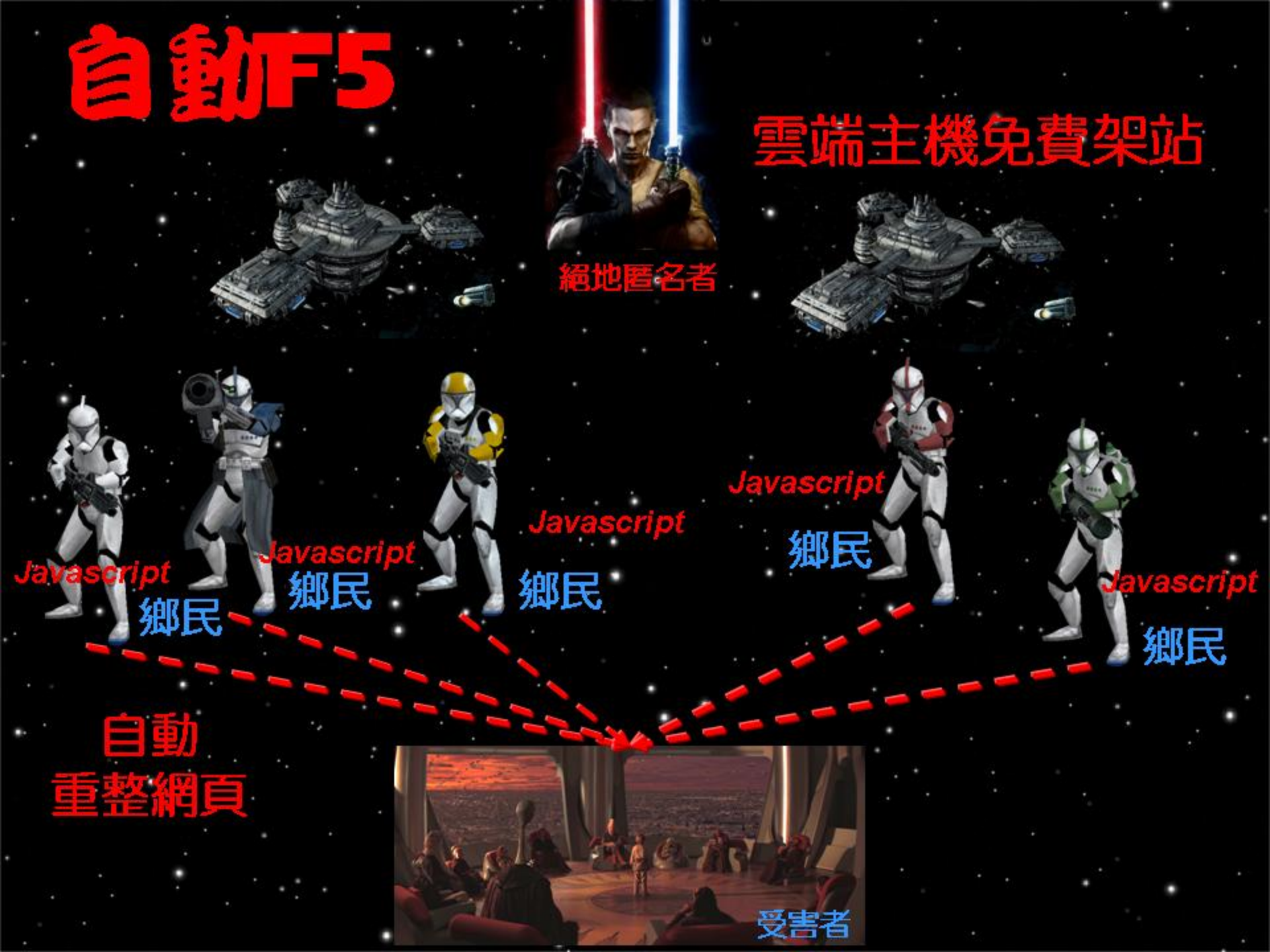
自動F5

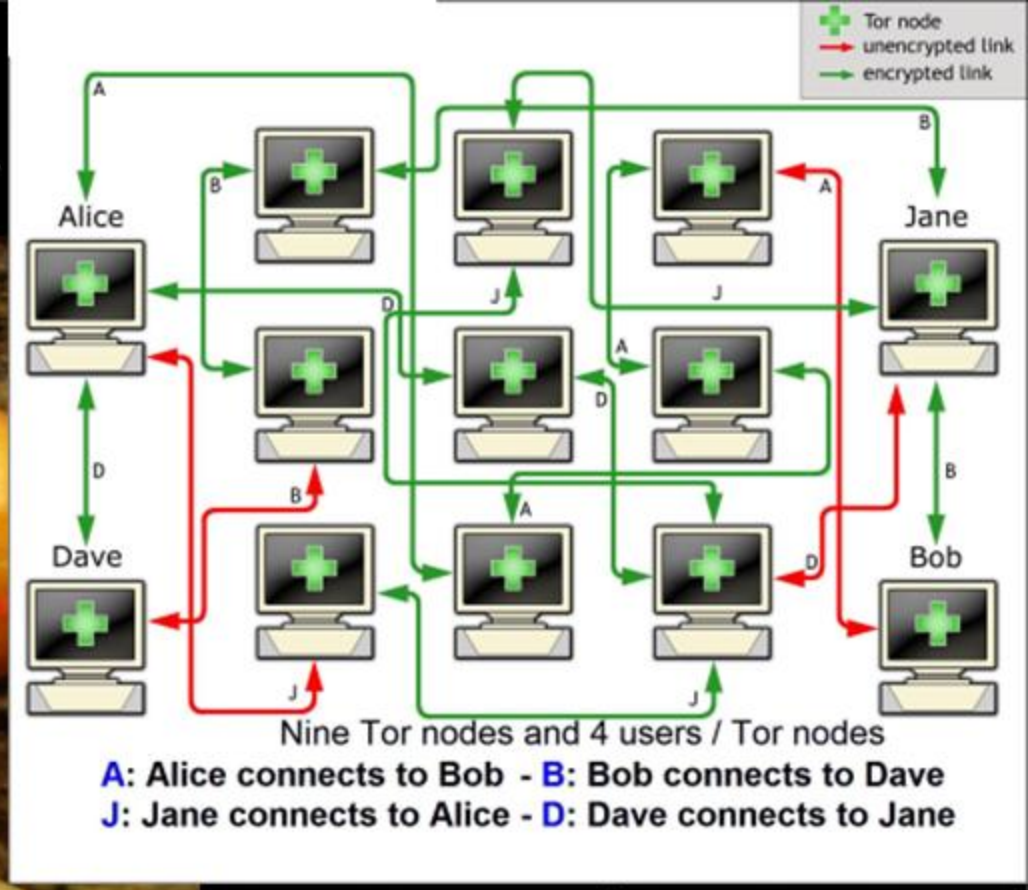
雲端主機免費架站





自動F5


雲端主機免費架站
絕地匿名者
Javascript
鄉民
Javascript
鄉民
Javascript
鄉民
Javascript
鄉民
Javascript
鄉民
自動
重整網頁
受害者



TOR 洋蔥網路

為躲避中共長城防火牆，
利用加密和多節點出口
以到達目的網站。

洋蔥匿蹤

絕地匿名者

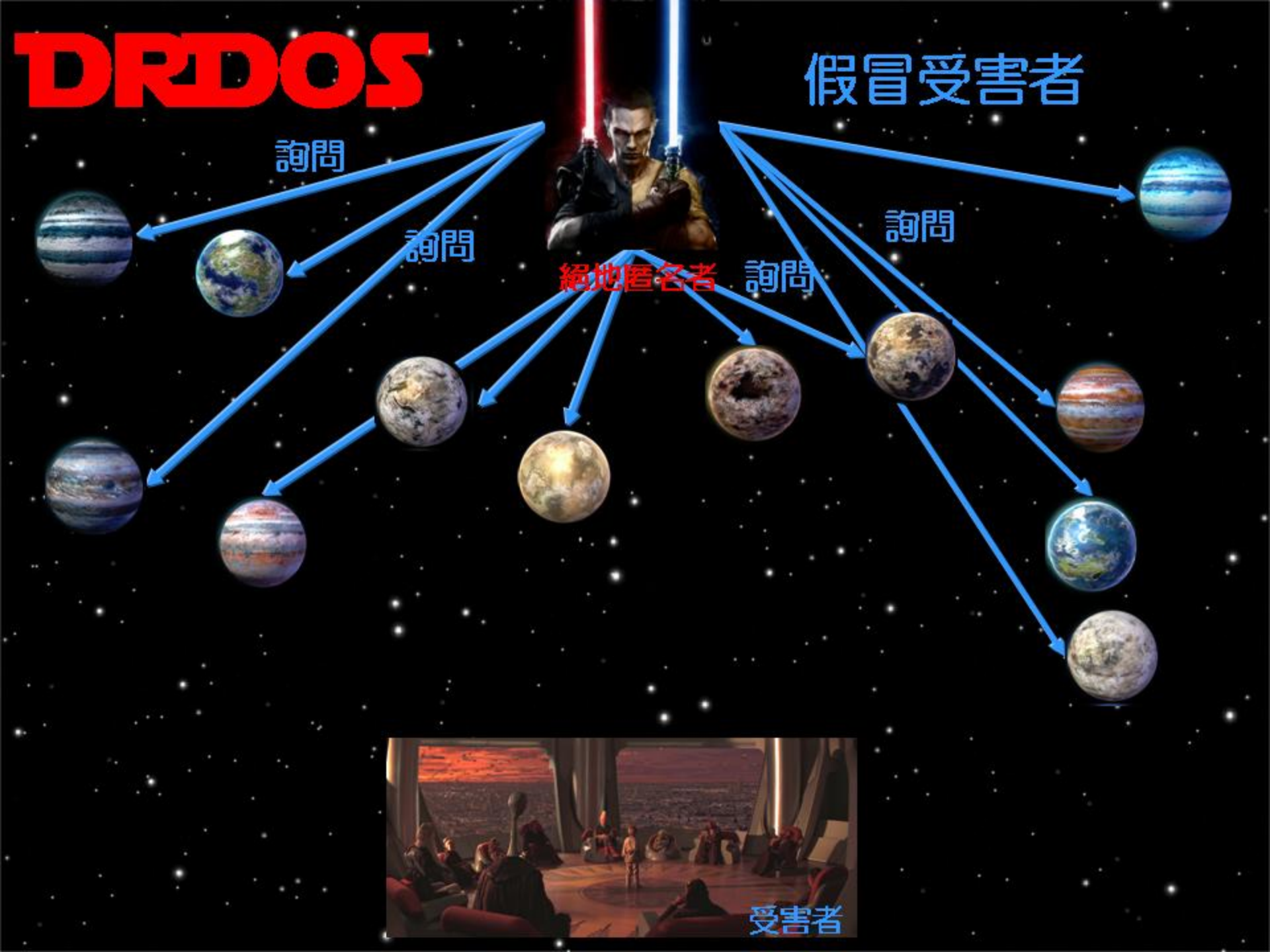
洋蔥網路

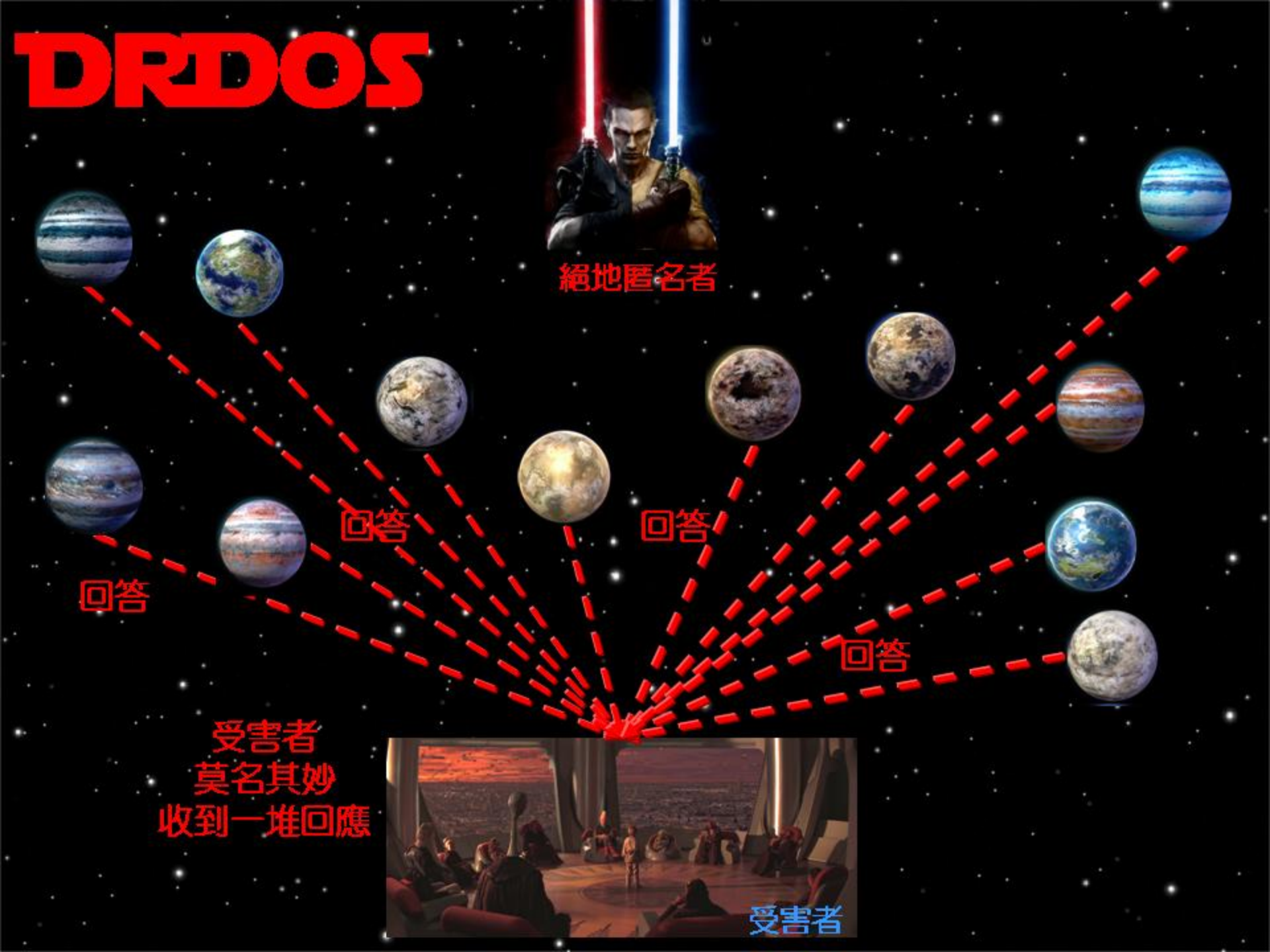
各種DoS手法

受害者

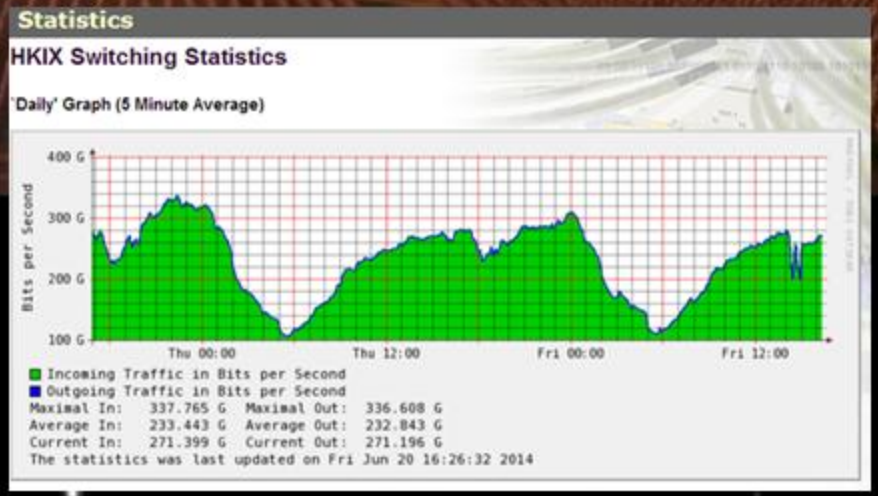
反彈式攻擊
(DISTRIBUTED REFLECTION DOS)

最早被利用是駭客發現網際網路上的路由器幾乎都開放 BGP 179埠。
駭客偽造受害者IP送出SYN封包，讓路由器回應SYN/ACK給受害者


DRDOS
假冒受害者
詢問
詢問
詢問
詢問
絕地匿名者
受害者


DRDOS
絕地匿名者
回答
回答
回答
回答
受害者
莫名其妙
收到一堆回應
受害者

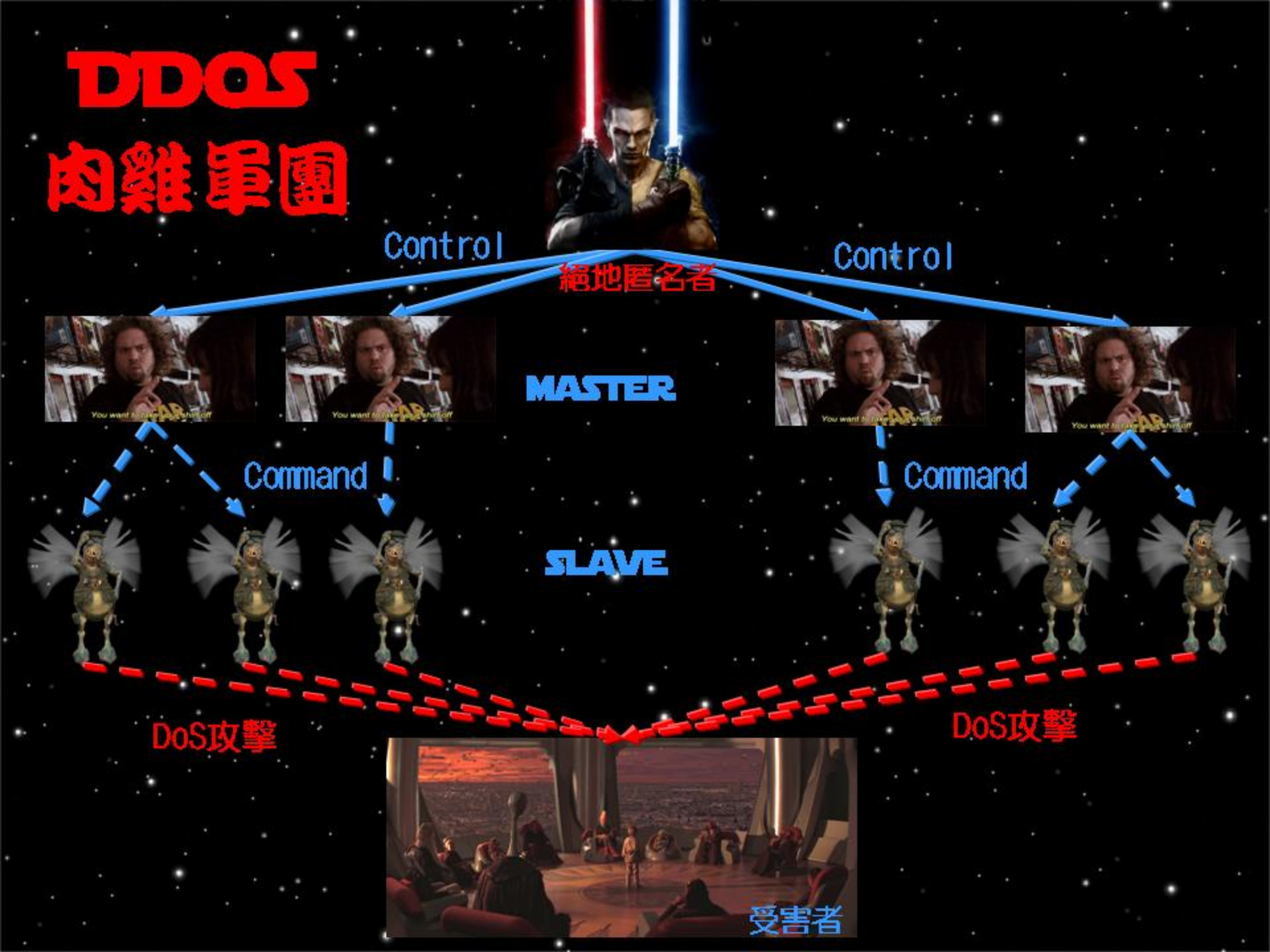
主機已無法承受
只能靠雲端清洗

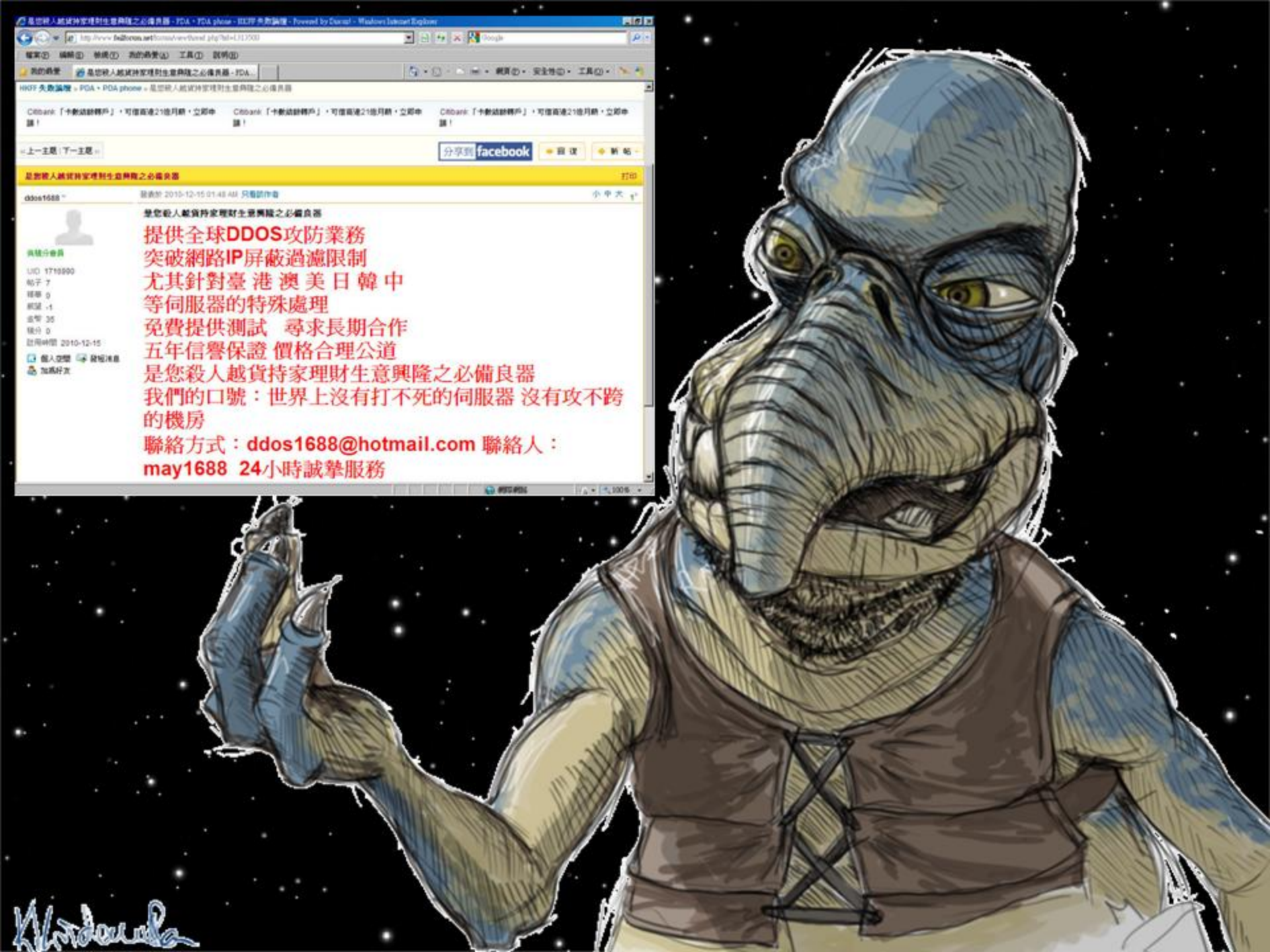


用別人架的網站
也可以彈

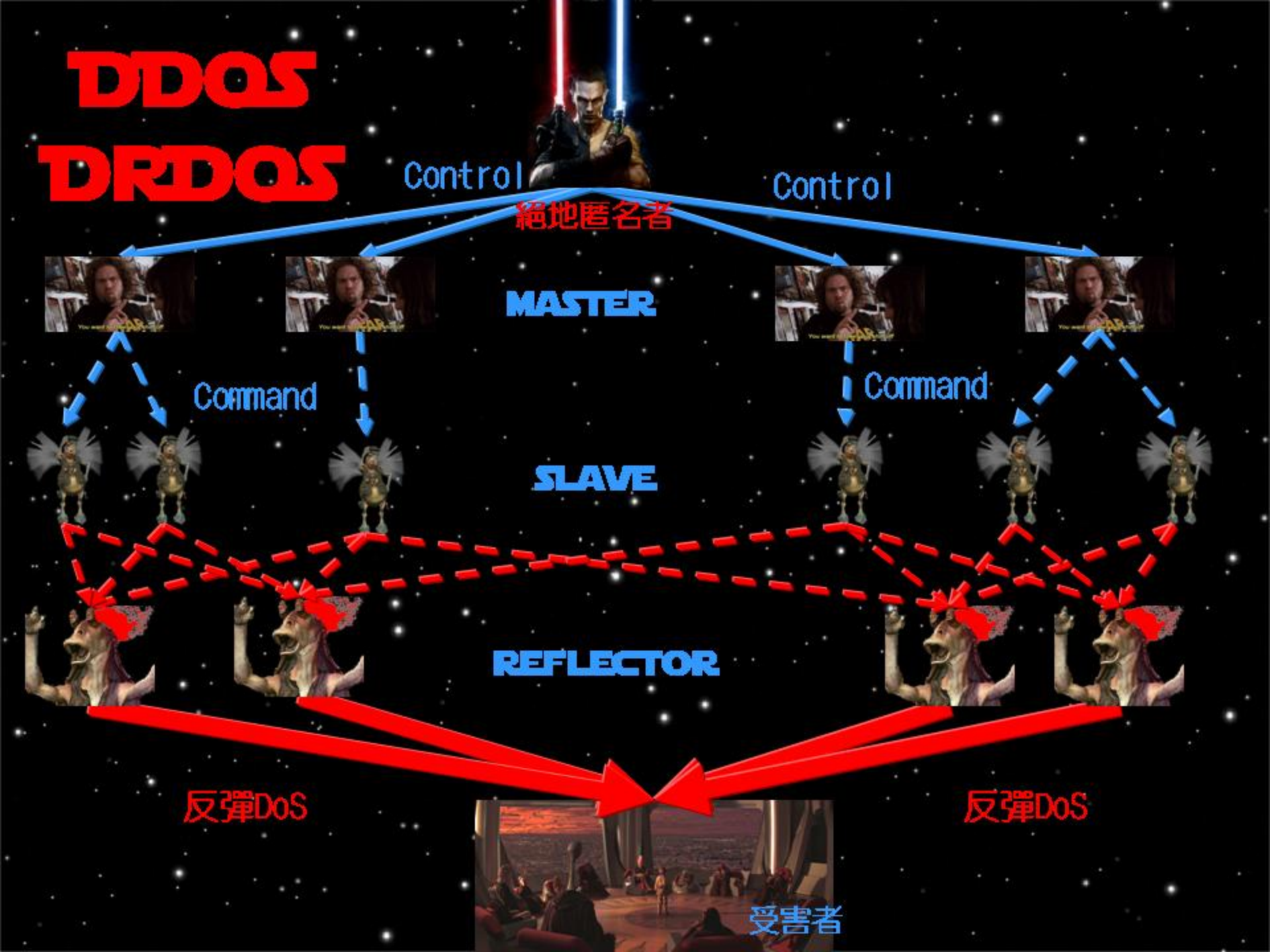
用 BT也可以彈
(50~120倍)

DDOS
肉雞軍團


Control
絕地匿名者
Control
MASTER
Command
Command
SLAVE
DoS攻擊
DoS攻擊
受害者


提供全球DDOS攻防業務
突破網路IP屏蔽過濾限制
尤其針對臺 港 澳 美 日 韓 中
等伺服器的特殊處理
免費提供測試　尋求長期合作
五年信譽保證 價格合理公道
是您殺人越貨持家理財生意興隆之必備良器
我們的口號：世界上沒有打不死的伺服器 沒有攻不跨的機房
聯絡方式：ddos1688@hotmail.com 聯絡人：
may1688　24小時誠摯服務

DDOS
DRDOS


Control
Control
絶地匿名者
MASTER
Command
Command
SLAVE
REFLECTOR
反弾DoS
反弾DoS
受害者

DDOS IRC

絕地匿名者

我愛「受害者」

加入

加入

SLAVE

REFLECTOR

反彈DoS

反彈DoS

受害者

DDOS
雲端化

絕地匿名者

加入

加入

SLAVE

REFLECTOR

反彈DoS

反彈DoS

受害者

General Veers my boss's breathing is so annoying, its all like "HOOO PAAAA HOOOO PAAA" whats up with that?

10 minutes ago · Comment · Unlike

Admiral Motti likes this.

Admiral Motti ROFL. i saw under his mask once. it looked like humpty dumpty had an abortion.

9 minutes ago · Delete

Darth Vader Perhaps you should consider setting your profile to private.

8 minutes ago · Delete

General Veers my...my LORD! It was just a stupid joke.

6 minutes ago · Delete

Admiral Motti we meant no disrespect.

5 minutes ago · Delete

Darth Vader I am going to force choke the piss out of you at work tomorrow.

5 minutes ago · Delete

Darth Vader Nevermind. I think I can just do it from here.

4 minutes ago · Delete

Darth Vader Yep! Now if only I could use the force to change your statuses to "Dead as Hell."

2 minutes ago · Delete

Grand Moff Tarkin L-O-L

2 minutes ago · Delete

Write a comment...

StewPig.com

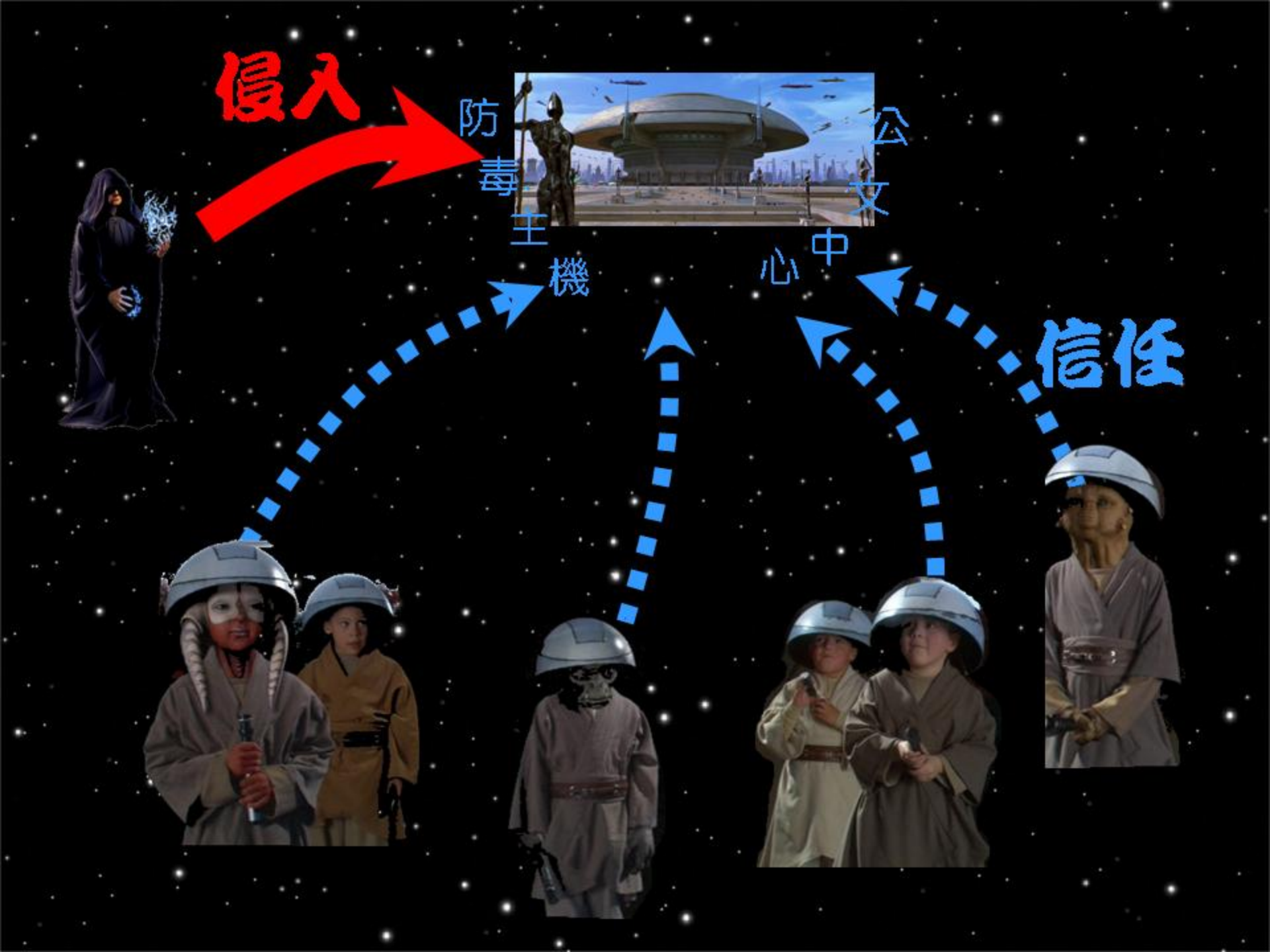
三部曲

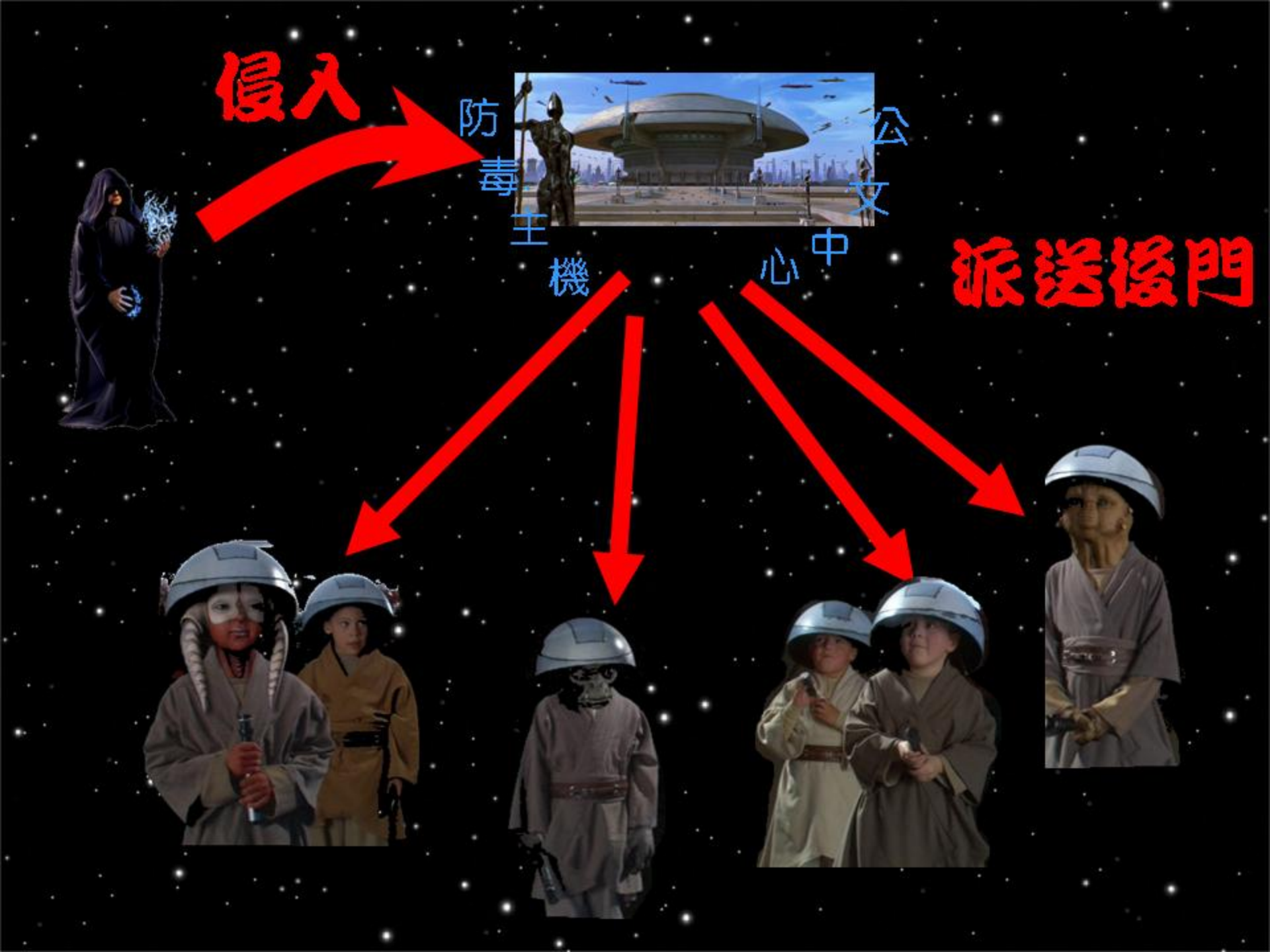
西斯大帝的復仇

絕地工程師們終於發現，
雲端聯盟的議長白卜庭…
就是濫用雲力的
西斯大帝

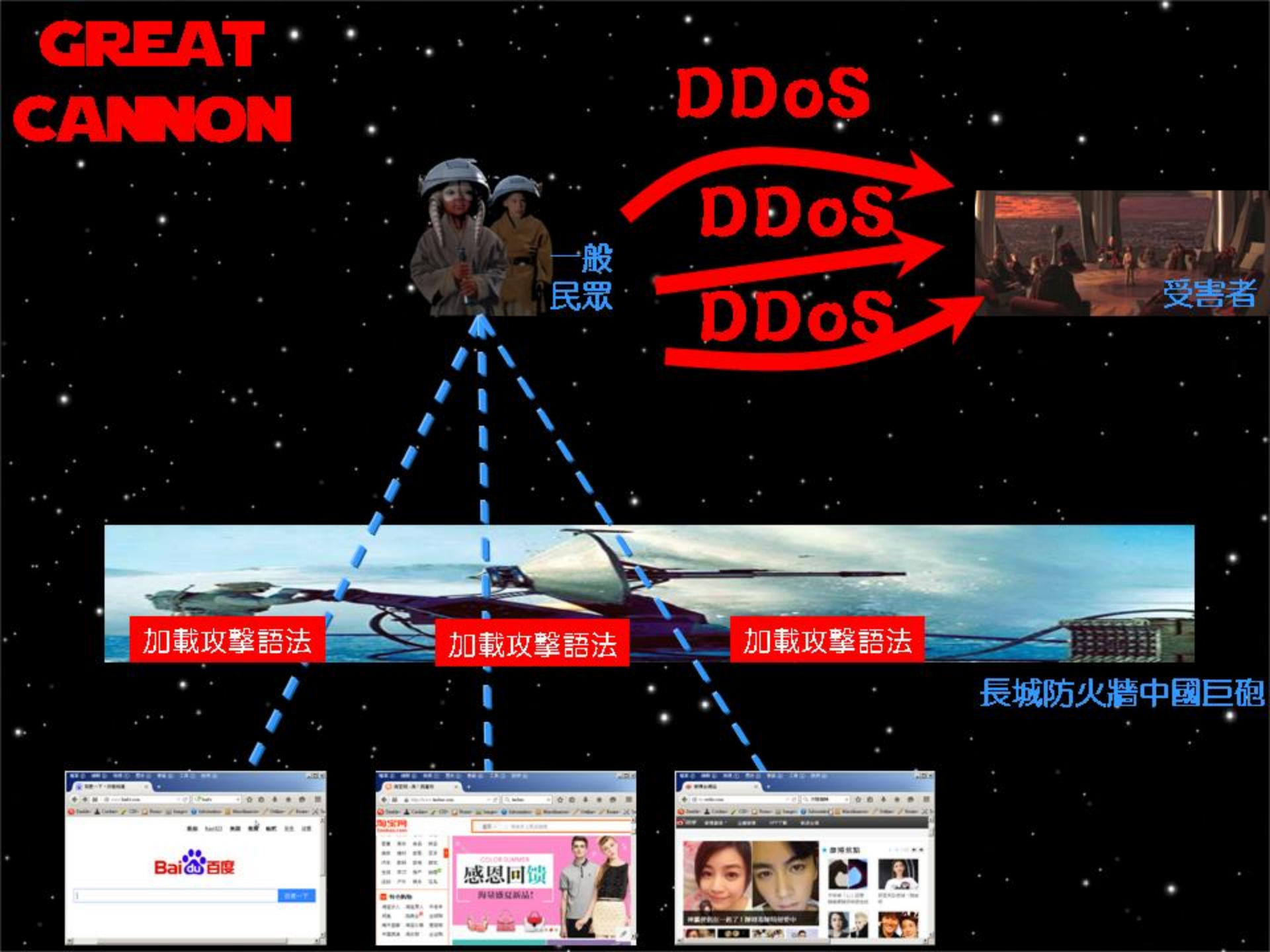
西斯兵法

背叛來自信任


侵入
防毒主機
公安中心
信任


侵入
防毒主機
公安中心
派送後門

GREAT CANNON



西斯兵法

各個擊破

KMPlayer官方證實遭下毒，已交調查單位 | 即時新聞 | iThome online - Windows Inter...

http://www.ithome.c... Google

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

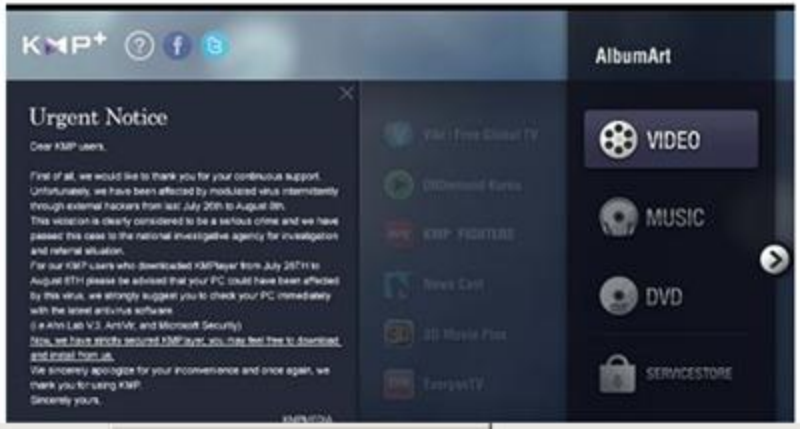
我的最愛 KMPlayer官方證實遭下... 網頁(P) 安全性(S)

KMPlayer官方證實遭下毒，已交調查單位

文/蘇文彬 (記者) 2013-08-12

讚 167 Share +1 6 我要收藏

KMPMEDIA透過KMPlayer發佈緊急訊息，證實遭駭客攻擊散佈惡意程式，從7月26日到8月8日安裝軟體的用戶可能受到攻擊，建議用戶以防毒軟體掃毒，為打擊犯罪KMMEDIA已將資料交付調查。



網際網路 105%

侵入
KMPlayer
更新中心
更新
正常
裝正版KMPlayer
從一般網路更新

侵入
KMPlayer
更新中心
更新
後門
裝正版KMPlayer
從某公司網路更新

西斯兵法

變鬼變怪

快速變種

POISON IVY

2011年 RSA SecurID 資安事件使用的遠端遙控病毒，
被用於多起國際惡意軟體大規模攻擊事件中...

四部曲

曙光乍現

李老師說...

事實上...

上了雲端，
你就不會死

兔崽的年代
外洩的年代

免费的年代 外挂的年代

檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)

《星球大战1-6》高清迅雷…

搜尋或輸入網址 搜尋

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools

，他们去了克鲁斯肯，并与银河系主席会晤，商讨帕尔帕亭在银河系扩展势力一事。同时金指出要将阿纳金训练成为绝地武士，但遭到绝地议会的极力反对，因为他们看出在阿纳金内心深处充满愤怒和仇恨，但金没有理会，仍要坚持训练阿纳金。

后来，金和克诺比再次返回纳波星球，协助对抗达斯马尔的入侵。这是一场激战。最后，金被达斯马尔所杀，在愤怒的克诺比剑下，达斯马尔也难逃一死。战后，为实现金的遗愿，克诺比继续训练阿纳金。

下载地址：

《星球大战1》BD1280高清下载——迅雷快传

《星球大战1》BD1280高清下载——迅雷链接

《星球大战1》BD1024MKV高清下载——迅雷快传

《星球大战1》BD1024MKV高清下载——迅雷链接

《星球大战1》BD1280MKV国英双语高清下载——迅雷快传

《星球大战1》BD1280MKV国英双语高清下载——迅雷链接

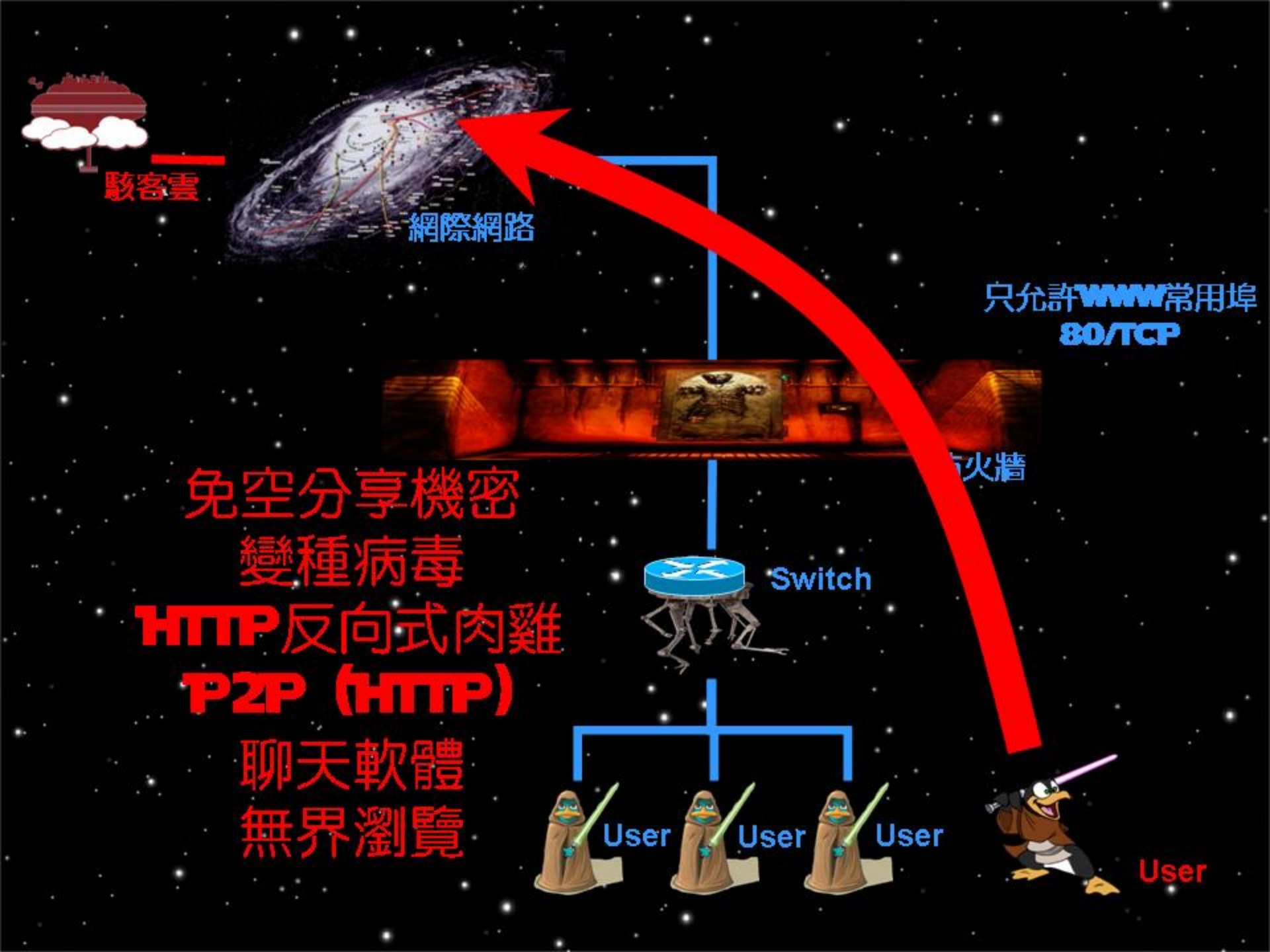
《星球大战1》720P高清种子下载——迅雷快传

《星球大战1》720P国英双语高清种子下载——迅雷快传

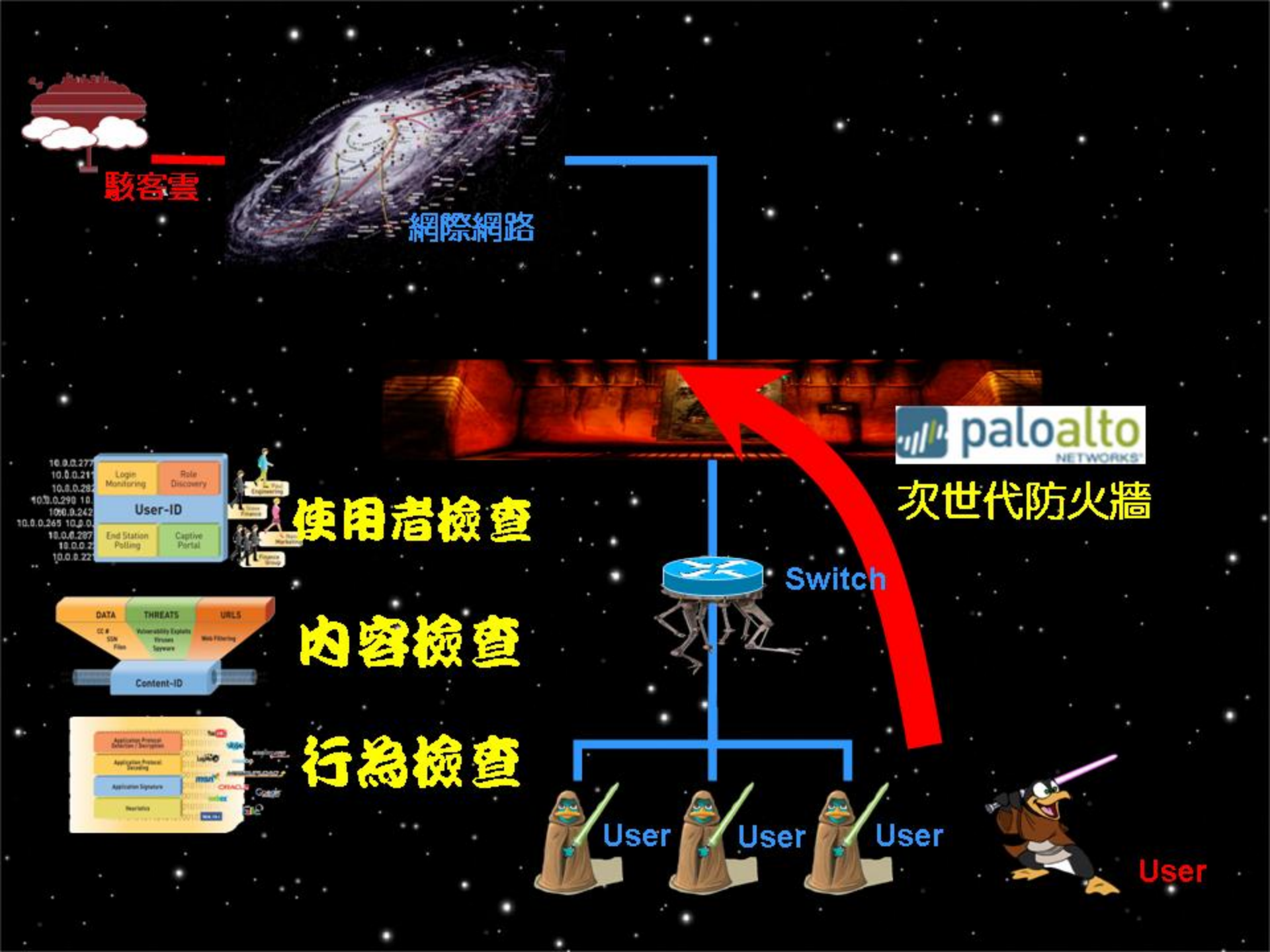
《星球大战1》1080P高清种子下载——迅雷快传

正在連線到 img.funshion.com…

要端藏毒更持久


駭客雲
網際網路
只允許WWW常用埠
80/TCP
防火牆
免空分享機密
變種病毒
HTTP反向式肉雞
P2P (HTTP)
聊天軟體
無界瀏覽
Switch
User
User
User
User

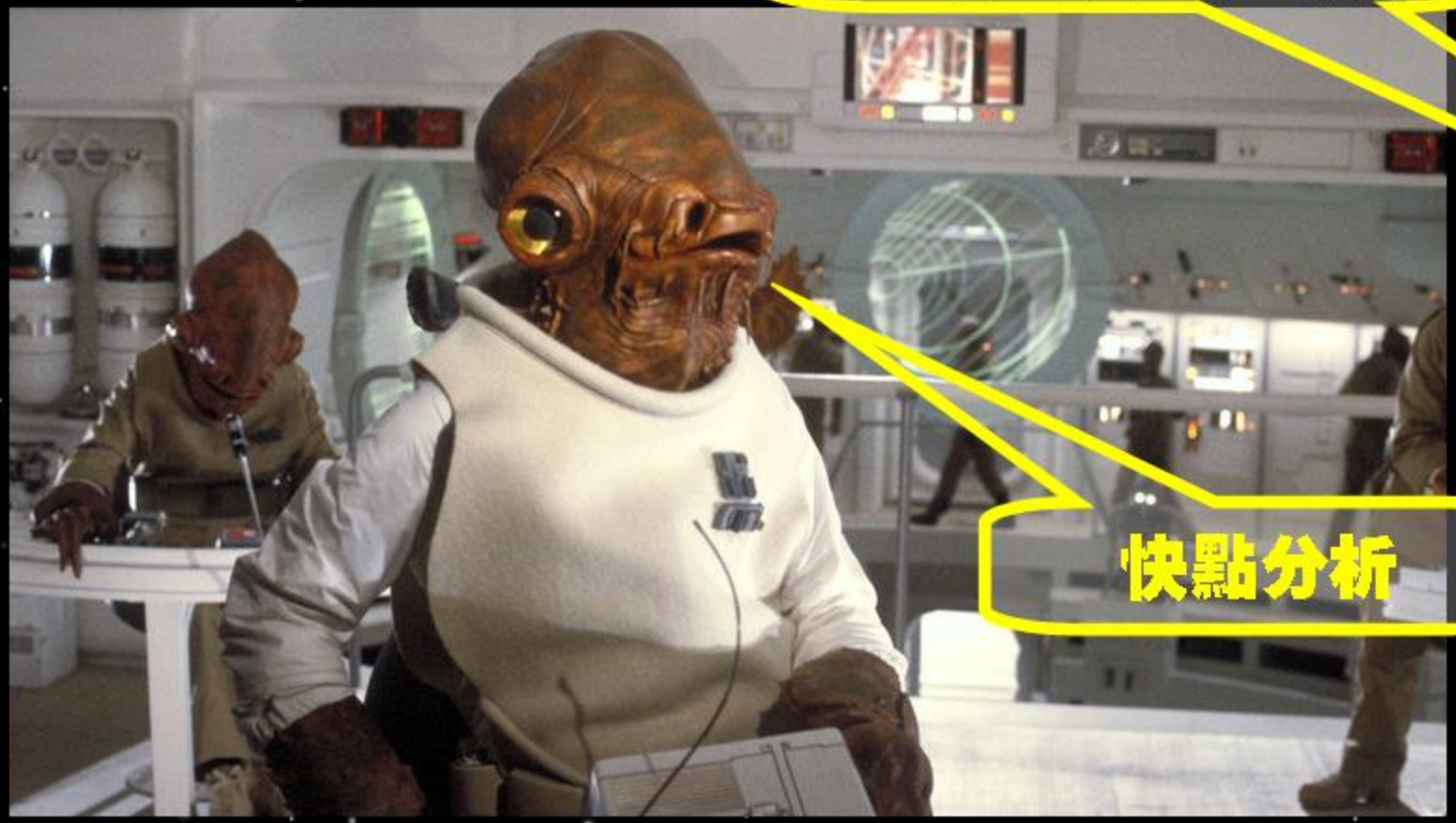
讓子彈…
…飛一會兒…


駭客雲
網際網路
paloalto
NETWORKS
次世代防火牆
Switch
User
User
User
User
使用者檢查
Login Monitoring
Role Discovery
User-ID
End Station Polling
Captive Portal
內容檢查
DATA
THREATS
URLS
Content-ID
行為檢查

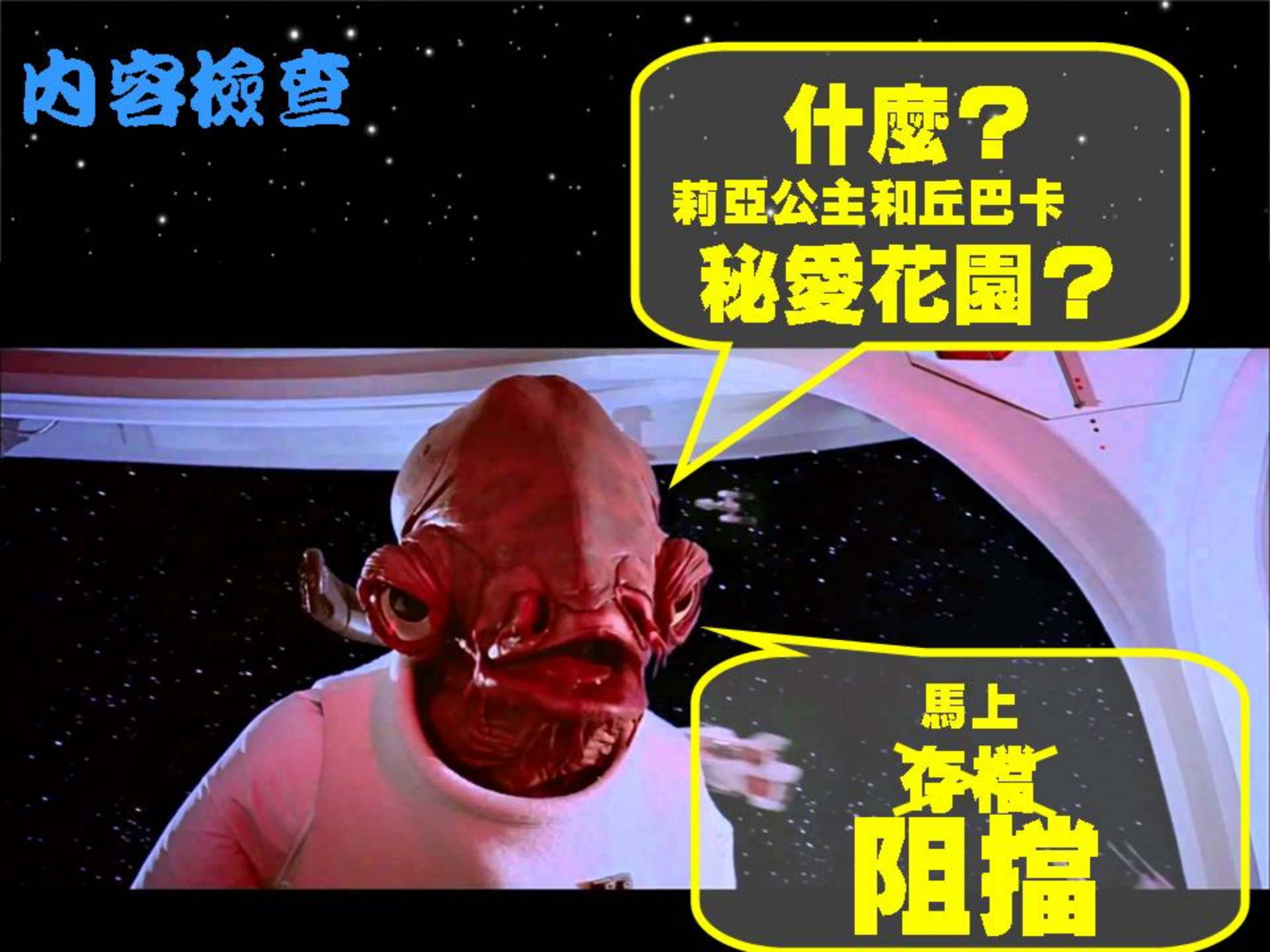
使用者檢查

讚
哼
贊
paloalto NETWORKS
Dashboard
ACC
Monitor
Device
Logout
Time Frame
Last Hour
Sort By
Filter
Help
3.9
Application
facebook
Application Information
Name: facebook
Related: facebook-chat, facebook-mail, facebook-base, facebook-apps
Description:
Additional Information:
Risk
Application
Sessions
1 facebook-base 5,042
2 facebook-chat 421
3 facebook-apps 44
4 facebook-mail 11
Top Sources
Source addr
Source User
Bytes
Sessions
1 10.154.2.33 phillip.blumste 1,158,885 180
allen.cook 822,648 171
3 10.154.12.89 ginger.poppe 2,360,286 140
4 10.154.14.61 natalie.ullrich 681,430 140
5 10.154.12.21 shawn.skilton 453,449 108
FB聊天
FB遊戲
免空網站
FB聊天
FB遊戲
免空網站
FB聊天
FB遊戲
免空網站

內容檢查



內容檢查



WILDFIRE 沙盒

在模擬環境中拆解並執行病毒，記錄它會使用的檔案、回傳資料的目標位址、遠端遙控的方式等等…

完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

Stark Technology Inc.
敦陽科技股份有限公司

敦陽資安專業服務

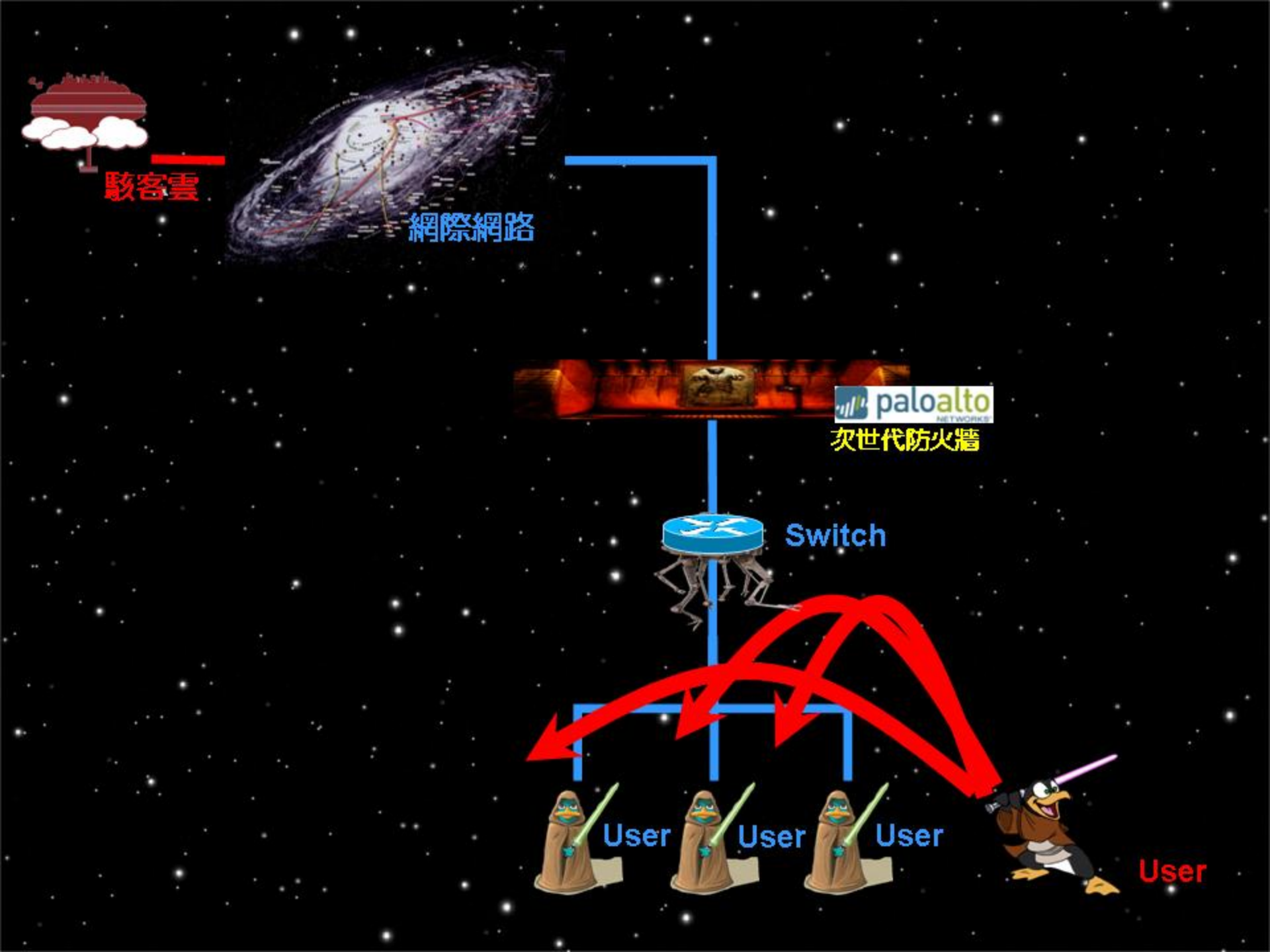
滲透測試服務	安管中心建置服務
網路弱點稽核服務	緊急應變服務
資安紀錄分析服務	社交工程演練服務
資安教育訓練服務	**資安顧問服務**

多功能應用層安全閘道系統

Palo Alto NGFW

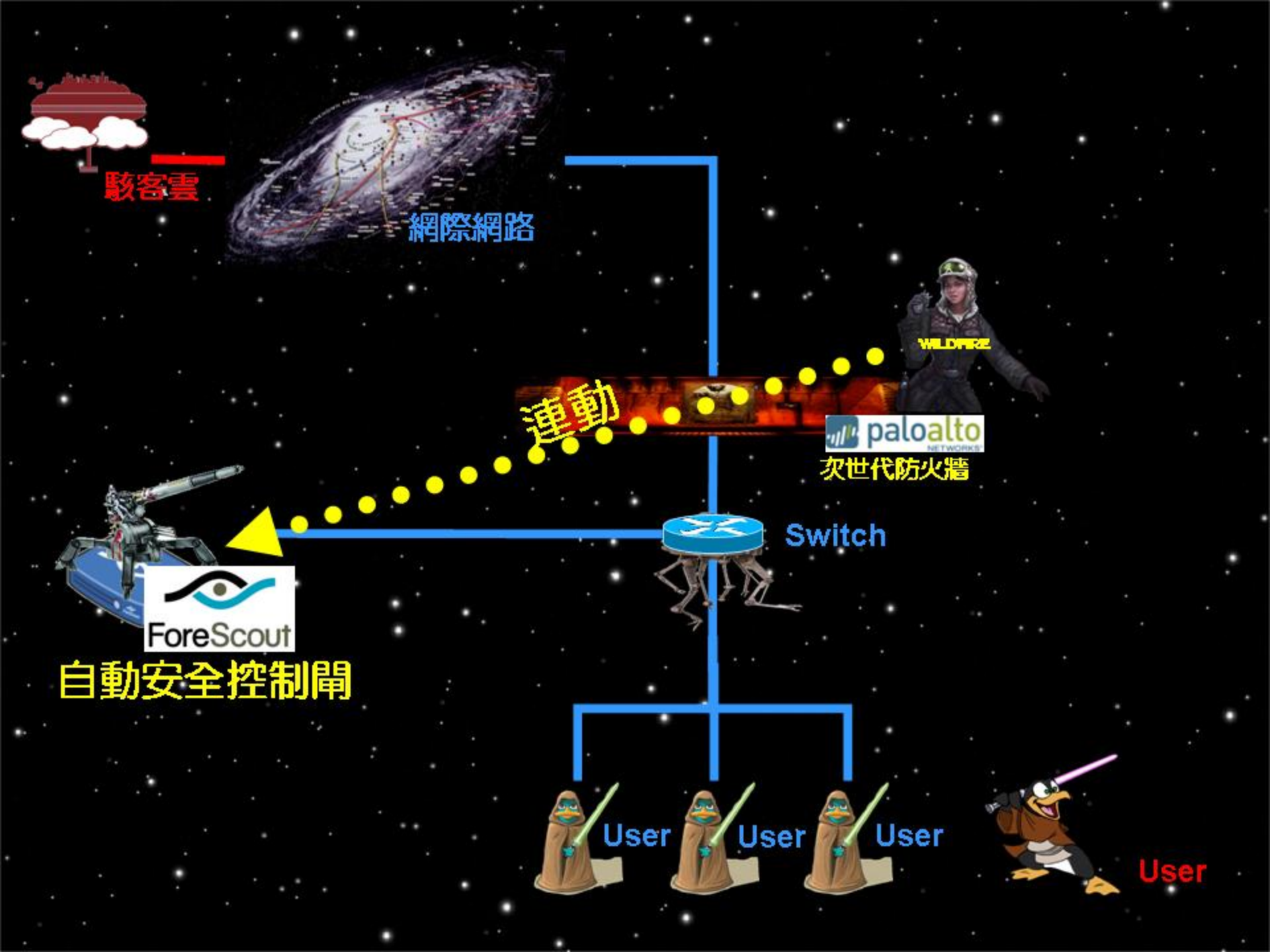
五部曲

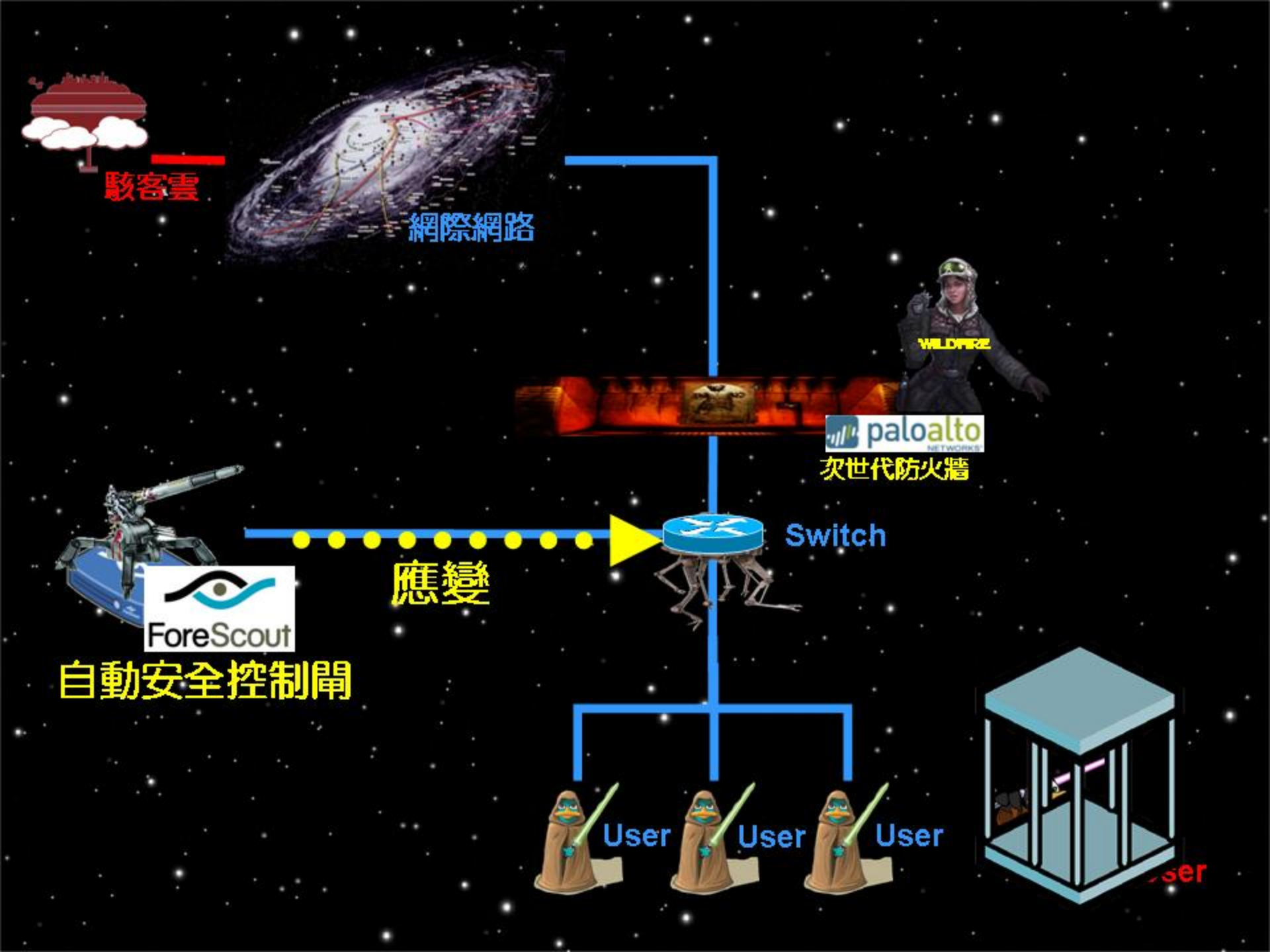
帝國大反擊


駭客雲
網際網路
paloalto
NETWORKS
次世代防火牆
Switch
User
User
User
User

我要…
打十個！

沙盒報告！
駭客雲
路
WILDFIRE
paloalto
NETWORKS
次世代防火牆
Switch
User
User
User


駭客雲
網際網路
連動
WILDFIRE
paloalto
NETWORKS
次世代防火牆
Switch
ForeScout
自動安全控制閘
User
User
User
User


駭客雲
網際網路
WILDFIRE
paloalto
NETWORKS
次世代防火牆
Switch
應變
ForeScout
自動安全控制閘
User
User
User

ForeScout
網路隔離
聯合沙箱分析技術，自動阻斷中毒肉雞防止擴散，
或者將肉雞集中到虛擬觀察網段。

完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

Stark Technology Inc.
敦陽科技股份有限公司

敦陽資安專業服務

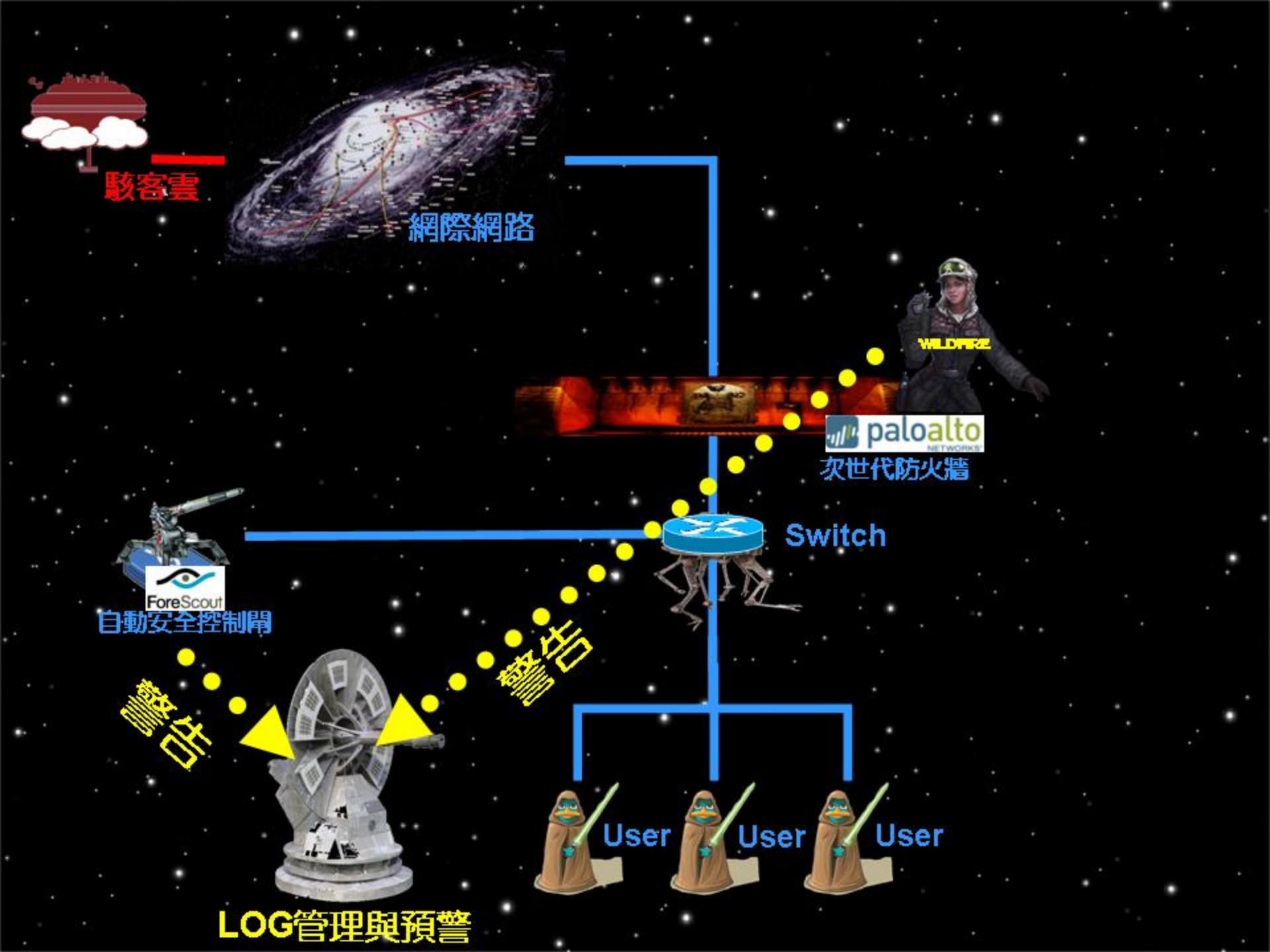
滲透測試服務	安管中心建置服務
網路弱點稽核服務	**緊急應變服務**
資安紀錄分析服務	社交工程演練服務
資安教育訓練服務	**資安顧問服務**

網路自動安全控制閘

ForeScout CounterACT

Clientless

六部曲
絕地大反攻


駭客雲
網際網路
WILDFIRE
paloalto
NETWORKS
次世代防火牆
Switch
ForeScout
自動安全控制閘
警告
警告
User
User
User
LOG管理與預警

中央預警
綜合不同來源的記錄，即時反應進行中的資安事故。

ArcSight
收集儲存
軌跡調查
稽核報表
關聯分析
異常告警
異質平台日誌
事件整合
資安事件分析
告警機制
處置回應
Security Information & Event Management
資安設備
網路設備
主機
應用程式

完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

Stark Technology Inc.
敦陽科技股份有限公司

敦陽資安專業服務

滲透測試服務	安管中心建置服務
網路弱點稽核服務	緊急應變服務
資安紀錄分析服務	社交工程演練服務
資安教育訓練服務	資安顧問服務

LOG管理與預警

HP ArcSight SIEM/Logger

ArcSight

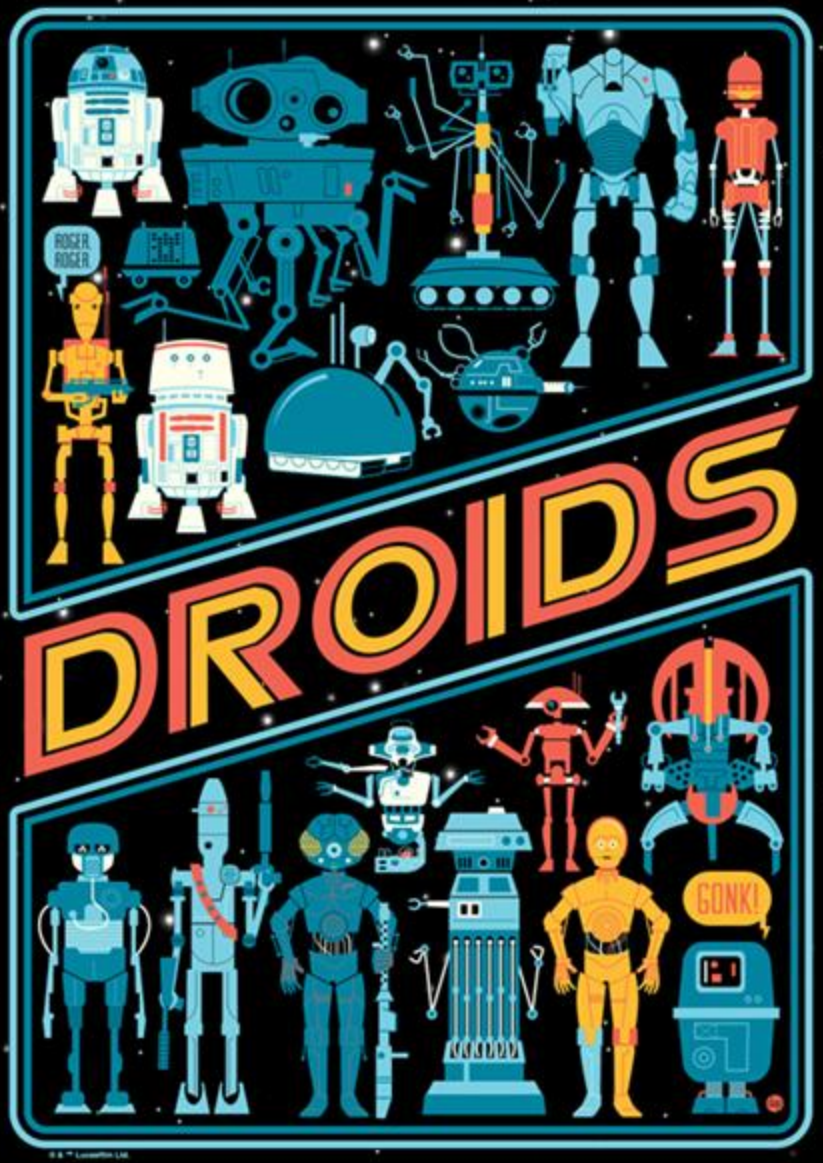
七部曲

靈力覺醒

敦陽的

業務

敦陽的技術



SITH EMPEROR
LORD KAAN
ADAS
DARTH KRAYT
DARTH BANE
ANDEDDU
EXAR KUN
DARTH PLAGUEIS
DARTHS REVAN & MALAK
DARTH TRAYA (LADY OF BETRAYAL)
DARTH SCION (LORD OF PAIN)
DARTH NIHILUS (LORD OF HUNGER)
DARTH MALGUS
DARTHS SIDIOUS & VADER
DARTH TYRANUS
DARTH MAUL

敦陽雲資安顧問

SITH EMPEROR
LORD KAAN
ADAS
DARTH KRAYT
DARTH BANE
ANDEDDU
EXAR KUN
DARTH PLAGUEIS
DARTHS REVAN & MALAK
DARTH TRAYA (LADY OF BETRAYAL)
DARTH SCION (LORD OF PAIN)
DARTH NIHILUS (LORD OF HUNGER)
DARTH MALGUS
DARTHS SIDIOUS & VADER
DARTH TYRANUS
DARTH MAUL

敦陽雲資安顧問

我

完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

Stark Technology Inc.
敦陽科技股份有限公司

敦陽資安專業服務

滲透測試服務	安管中心建置服務
網路弱點稽核服務	緊急應變服務
資安紀錄分析服務	社交工程演練服務
資安教育訓練服務	資安顧問服務

高階應用層交付暨網頁防火牆

資料庫稽核與防護

資料防洩方案

APT防護

多功能應用層安全閘道系統

網路自動安全控制閘

LOG管理與預警

STAR WARS VII
2015.12.18

有沒有疑問？