駭客攻擊手法新趨勢

講師：楊伯瀚

講師經歷

- 楊伯瀚 *(lucifer.yang@sti.com.tw)*
- 現任: 敦陽科技 資安專業服務處 顧問
- 專長
  - 滲透測試
  - 網頁應用程式安全
  - 系統入侵事件分析
  - 資安事件處理
- 資安認證
  - CISSP
  - CEH (Certified Ethical Hacker) /CEI (Instructor)
- Cert/CC Advanced Incident Handling 講師
  - CISM

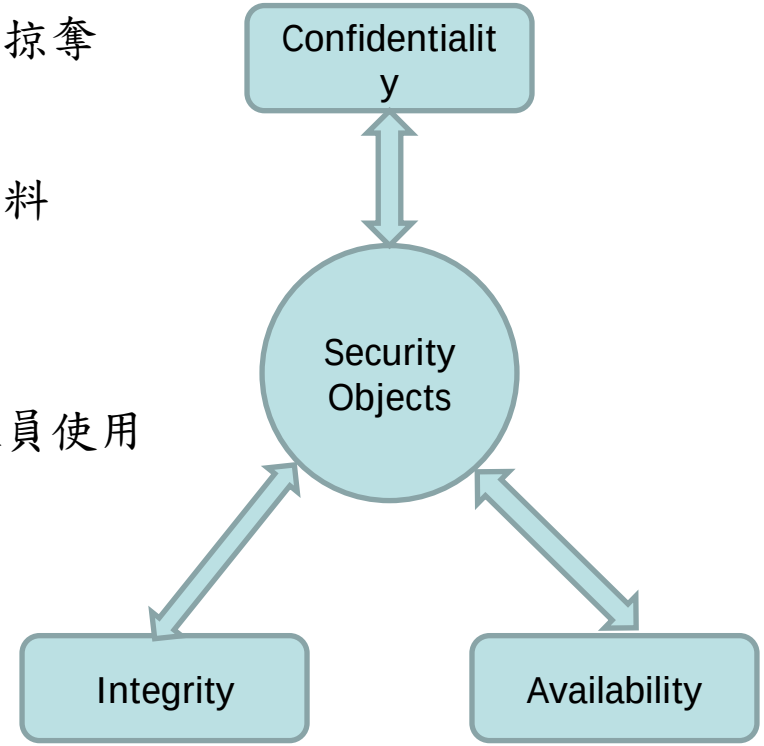
大綱

- 入侵趨勢案例研討
- DoS 與 DDoS 攻擊
- 進階持續性威脅(APT)概念與案例
- 勒索病毒案例分析
- 資安防護技術與缺陷

入侵趨勢案例研討

資安三原則

- Confidentiality –機密性
  - 確保資料傳遞與存取的私密性
  - 避免未經授權的存取或有意無意的揭露與掠奪
- Integrity –完整性
  - 避免非經授權的使用者或處理程序竄改資料
- Availability –可用性
  - 讓資料隨時保持在可用狀態
  - 讓資料即時而且可靠的提供給各層級的人員使用
  - 確保該服務的品質與永不中斷
- Non-repudiation –不可否認性
  - 防止存心不良者否認其所做過的事情



傳統攻擊手法

Heartbleed攻擊示意圖

當使用者登入使用有問題的OpenSSL版本，作為網站傳輸加密的工具時，網站在執行OpenSSL心跳服務時，會因為該版本的OpenSSL具有Heartbleed漏洞，會隨機外洩記憶體中64KB的機敏資料。駭客可以使用工具，取得記憶體外洩資料中包括帳號、密碼甚至是加密私鑰等，網站機敏資料讓駭客一覽無遺。

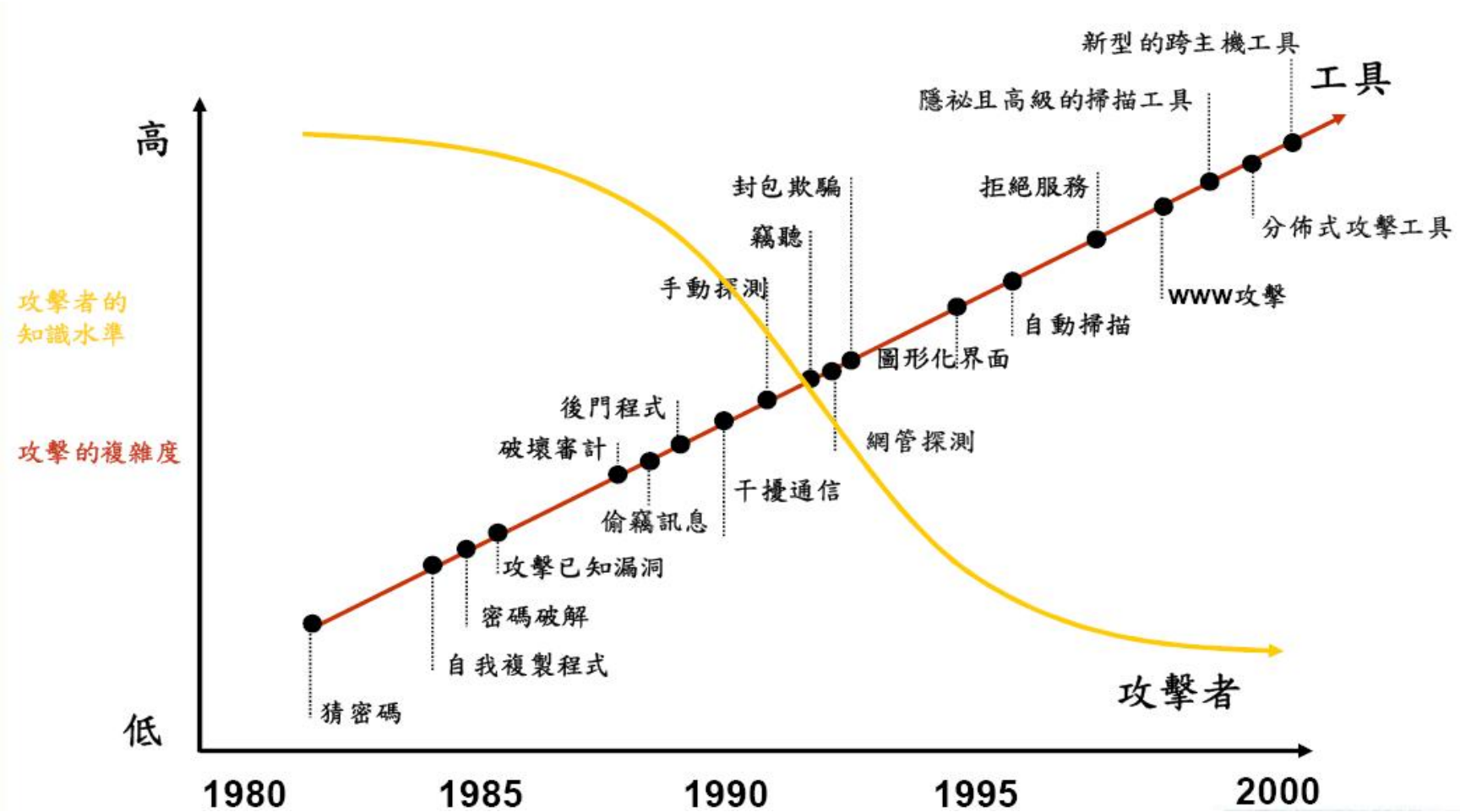
資料來源：iThome整理，2014年4月

OpenSSL 漏洞 CVE-2014-0160

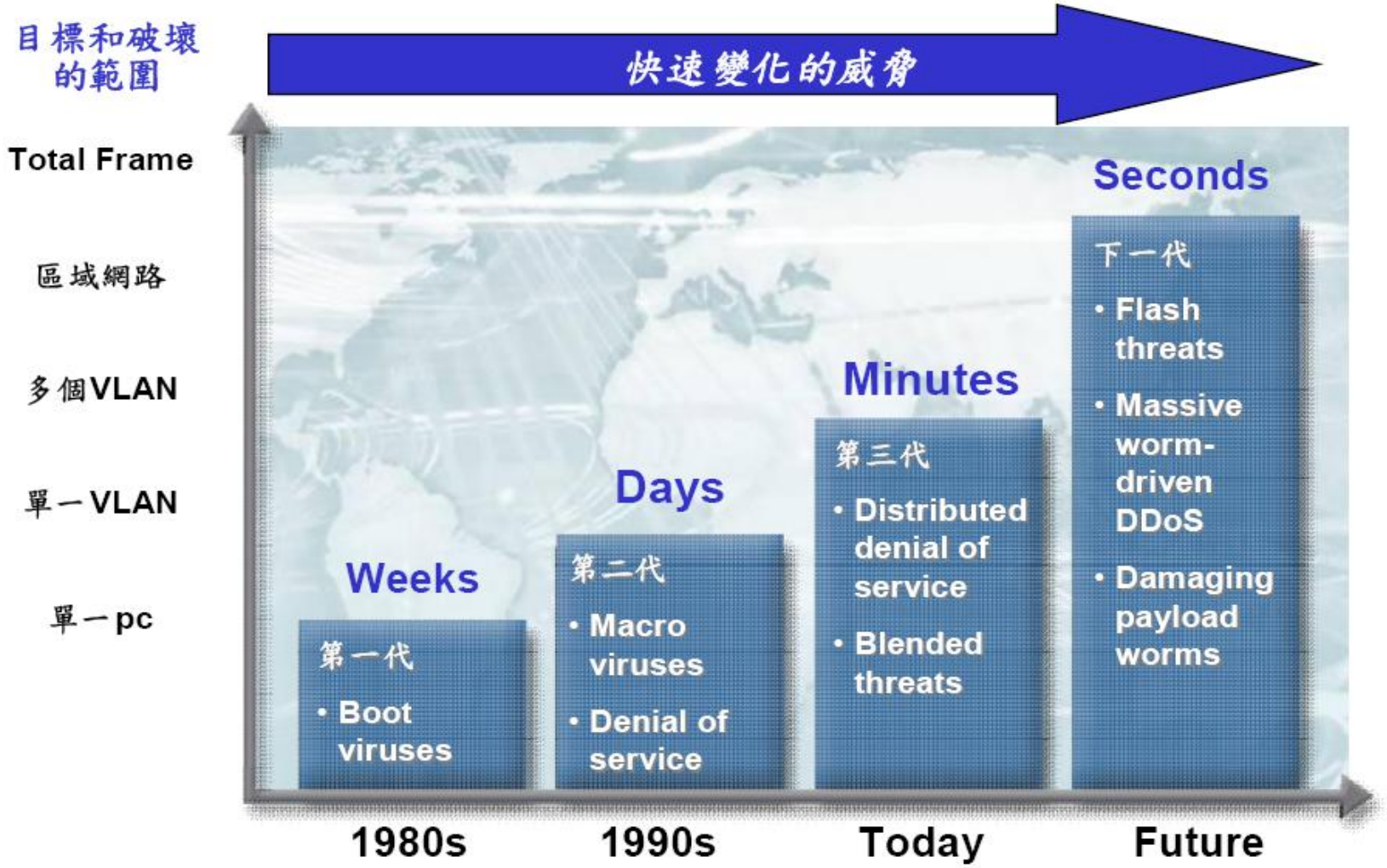
零時差攻擊

- zero-day attack 已是一個趨勢
- 此種態勢憑藉著被廣泛傳播的攻擊，將會嚴重的威脅到Internet以及其眾多的使用者或機器。
- 雖然供應商(OS、防毒廠商)已然了解此種形式，但他們仍然束手無策。屆時他們將無法及時的提供修正檔或是補強措施。

攻擊複雜度與攻擊者的技術水準



攻擊範圍和時間變化


目標和破壞的範圍
快速變化的威脅
Total Frame
區域網路
多個VLAN
單一VLAN
單一pc
Seconds
下一代
• Flash threats
• Massive worm-driven DDoS
• Damaging payload worms
Minutes
第三代
• Distributed denial of service
• Blended threats
Days
第二代
• Macro viruses
• Denial of service
Weeks
第一代
• Boot viruses
1980s
1990s
Today
Future

當今威脅情勢分析

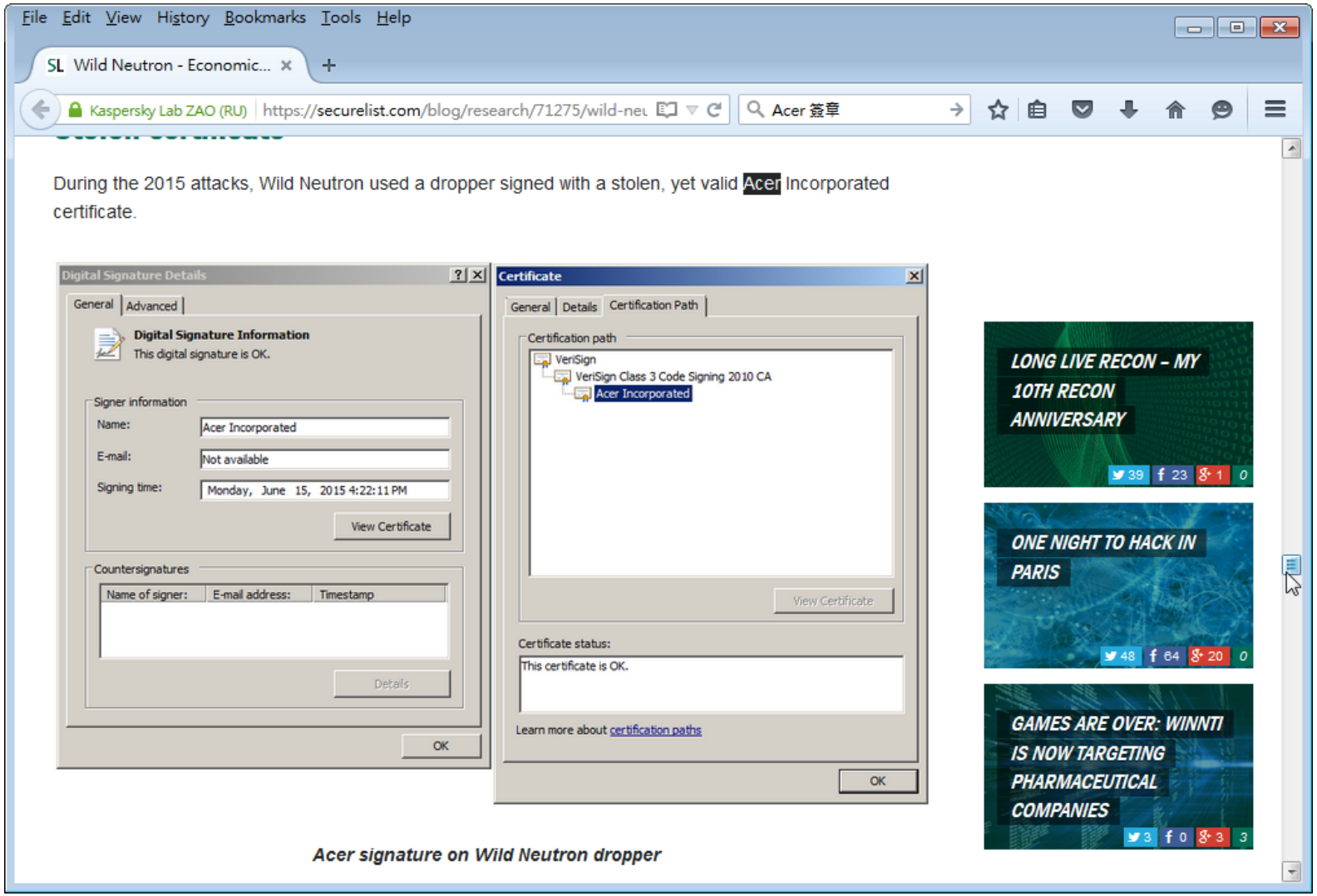
- 威脅的複雜性日益增高
  - 90% 透過email繁殖與散撥，如mass mailing worms
  - 50%+ 經由Webpage讓使用者在無知的狀況下受感染
  - 10% 因系統本身的漏洞(弱點)，透過以internet為途徑被攻擊
  - 77% 擁有多重的散佈管道
  - 87% 會引發其他的攻擊行為
- 威脅以多重方式與途徑的攻擊傳染能力大增
  - 現今的攻擊大多具備多種攻擊途徑
  - 單一的防禦措施或防禦點，已無法滿足企業面對攻擊的需求
  - 資訊安全須以系統的角度來思考部署企業安全防護網

完整的資訊安全

- 資訊安全的演進過程中，我們可以看到：
  - 資料加密在技術上的持續提升
  - 強化的預設安全措施
  - 廣泛且及時的病毒防護
  - 自動化的作業系統補丁
- 但仍持續受到virus、worm 以及spy-bot的威脅
- 最大的安全漏洞並非在系統開發或網路技術，而是人！

1億筆 Facebook 資料

Acer憑證外洩，用於科技間諜案



Acer signature on Wild Neutron dropper

惡意程式散佈途徑與管道

入侵途徑及管道	說明
電子郵件	電子郵件本身夾帶隱藏惡意程式的WORD的或其他類型檔案，利用OFFICE程式的漏洞，開啟後便連帶安裝後門或木馬程式。
系統本身漏洞	對目標系統或網路之漏洞進行攻擊，進而取得控制權，常見的方式包含：網芳相關、RPC-DCOM、IIS、IE弱點攻擊等等。
網站注入攻擊	使用特殊字元，使網頁應用程式略過安全性檢查，或輸入錯誤資料，得到錯誤訊息進而推敲資料庫的格式及內容。
惡意網頁	駭客先攻陷某一網站，並在網頁上加入一些惡意程式碼，使瀏覽用戶不自覺就被植入木馬程式。或是網路釣魚方式。
系統不當權限設定	防火牆規則不嚴謹、防毒軟體未更新，讓駭客利用掃描工具直接獲得帳號密碼。

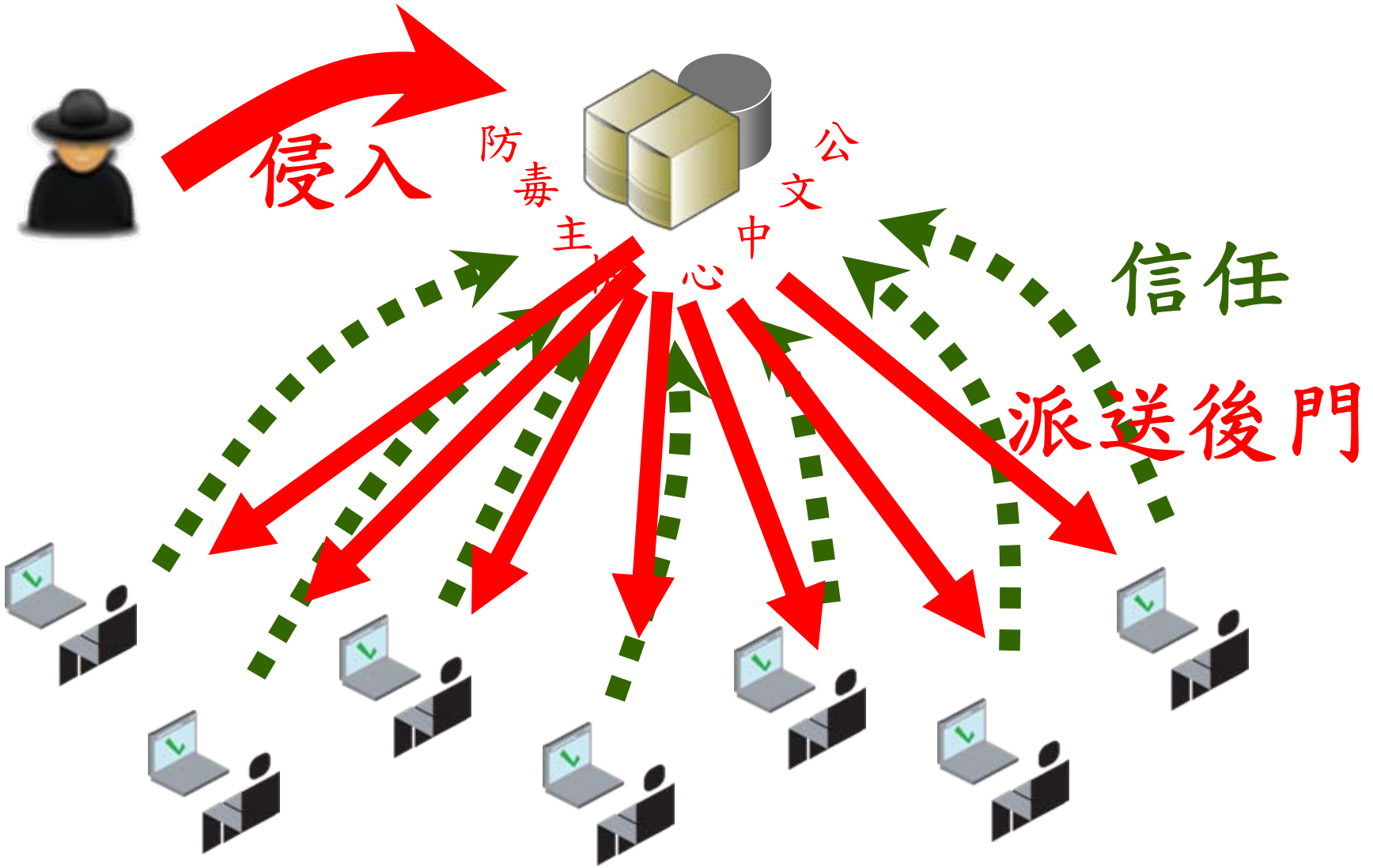
3萬2千臺電腦下午2點集體當機

韓國史上最大駭客事件

防毒公司淪為派毒工具

韓國遭到大規模駭客攻擊，多家銀行、保險公司、電視臺、甚至有電信公司受駭，超過32,000臺電腦當機，硬碟開機磁區損毀，無法重新提供服務，資安專家剖析，造成巨大災情的關鍵是，防毒軟體的更新主機被駭，反而成為散播惡意程式的攻擊跳板

韓國銀行



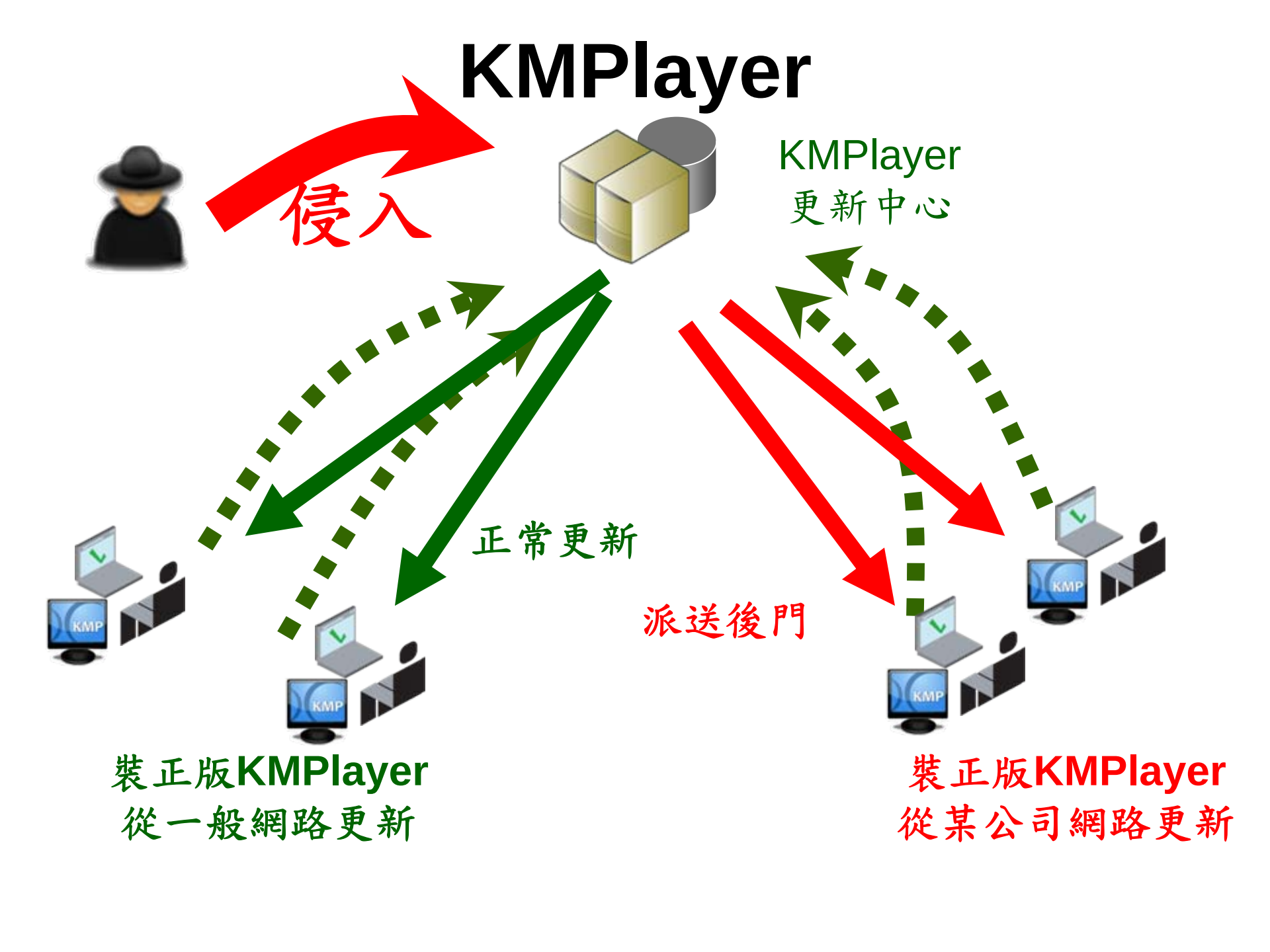
不可信任的信任軟體


檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
絕對驚嚇！Kaspersky被駭…
www.gameapps.hk/index.php/online/10717-2015-06-12-17-38-20
搜尋
絕對驚嚇！Kaspersky被駭客成功入侵！
六月 13 2015
讚 30
g+1 1
相信不少公司都有安裝防毒來做網絡防衛，但是事實證明，這並沒有什麼X用，因爲即使是大名鼎鼎的Kaspersky也沒能百分之百保護好自己公司的電腦。
KASPERSKY
師父!!!
救我呀
Google play

KMPlayer


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。
KMP+
AlbumArt
Urgent Notice
Dear KMP users,
First of all, we would like to thank you for your continuous support.
Unfortunately, we have been affected by modulated virus intermittently through external hackers from last July 26th to August 8th.
This violation is clearly considered to be a serious crime and we have passed this case to the national investigative agency for investigation and referral situation.
For our KMP users who downloaded KMPlayer from July 26TH to August 8TH please be advised that your PC could have been affected by this virus, we strongly suggest you to check your PC immediately with the latest antivirus software.
(i.e Ahn Lab V3, AntiVir, and Microsoft Security)
Now, we have strictly secured KMPlayer, you may feel free to download and install from us.
We sincerely apologize for your inconvenience and once again, we thank you for using KMP.
Sincerely yours,
VIDEO
MUSIC
DVD
SERVICESTORE
網際網路
105%

KMPlayer


侵入
KMPlayer
更新中心
正常更新
派送後門
KMP
KMP
KMP
KMP
裝正版KMPlayer
從一般網路更新
裝正版KMPlayer
從某公司網路更新

常見駭客工具介紹

工具類別	功能及影響
後門程式	木馬程式，具備遠端遙控、遠端存取資料、資料傳輸、側錄等等
帳號破解工具	獲取帳號檔並破解之
弱點掃描工具	掃描主機的漏洞，進而入侵
連線中繼程式	APR封包傳送中間攔截
遠端遙控程式	利用圖形化介面遠端遙控被入侵的電腦
鍵盤及密碼側錄程式	記錄你鍵盤所打的字以及程式發送的密碼，並利用EMAIL傳送一份到駭客手上

系統癱瘓


File Edit View History Bookmarks Tools Help
紐約證券交易所當機前夕...
www.appledaily.com.tw/realtim
股市癱瘓
娛樂
時尚
生活
社會
國際
財經
地產
紐約證券交易所當機前夕　匿名者曾發言警告

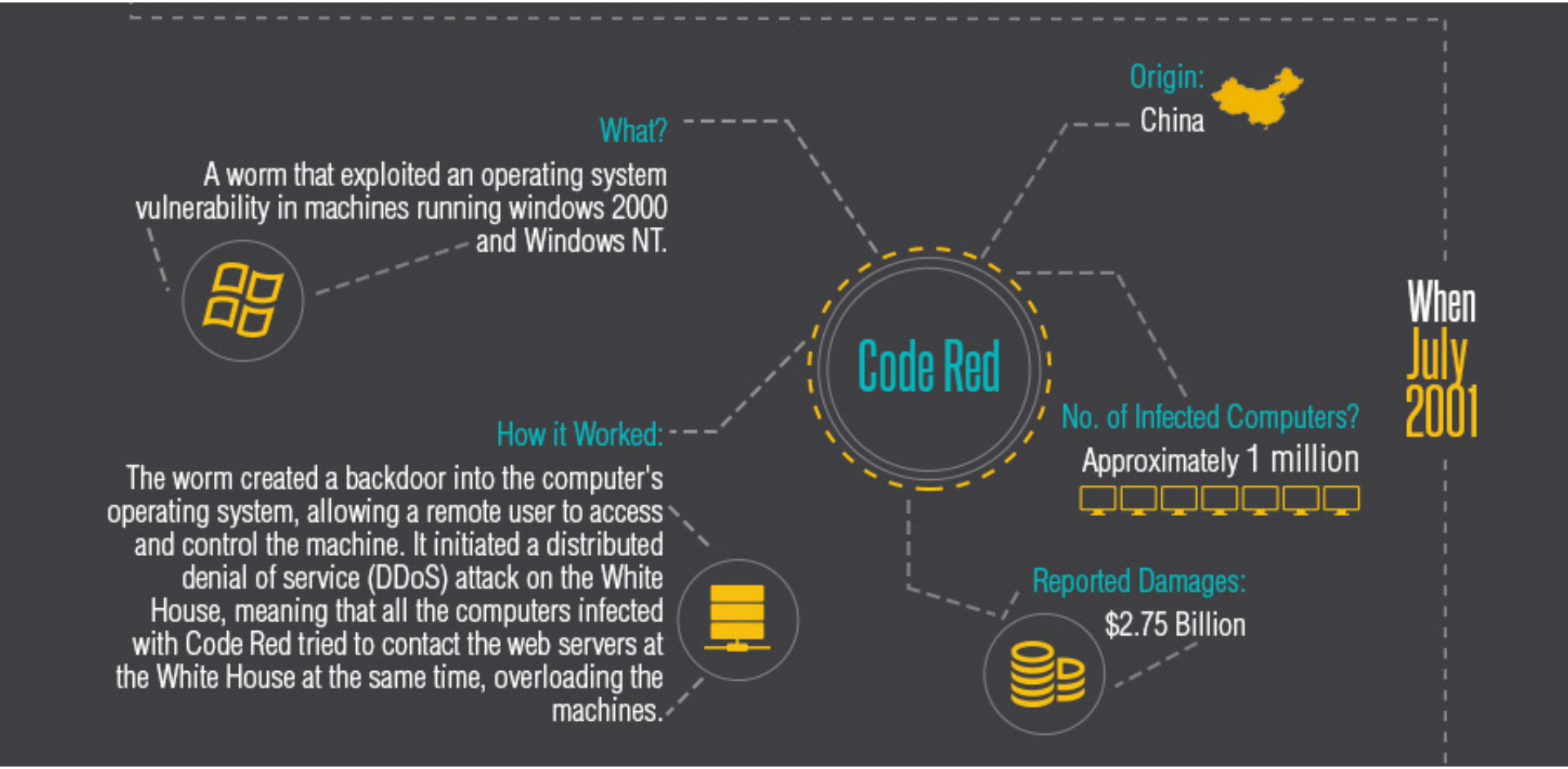
針對式的攻擊


File Edit View History Bookmarks Tools Help
專門提供駭客服務的Hacki...
www.ithome.com.tw/news/97241
Hacker Team
iThome 新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群 搜尋
專門提供駭客服務的Hacking Team自己也被駭了
Hacking Team為專門提供政府、執法、情報組織駭客服務及工具的義大利合法公司，本周傳出遭駭客入侵，駭客在網路上公佈Hacking Team的400GB機密資料，並入侵其Twitter帳號。
1.5萬 按讚加入iThome粉絲團 分享 190 +1 7
文/ 陳曉莉 | 2015-07-07 發表
HackingTeam
About us
The Solution
Customer Policy
Careers
Contacts
Deploy
A SECRET
agent.
Total control over your targets.
Log everything you need. Always.
Anywhere they are.
WE'RE HIRING!
NEW RELEASE
REMOTE CONTROL SYSTEM
GALILEO
openstack
Taiwan 201
August 11st TIC
Mark Collier
OpenStack Foundation COO
滿足所有角色需求的開源雲技術盛
iThome 電腦報
按讚追蹤 iThome 最新報導
1.5萬
openstack Day
專門協助各國政府執行監控任務並開發間諜軟體的義
熱門新聞

前、後期駭客手法比較

項目	早期駭客手法	新型駭客手法
掃描方式	• 大規模 • 從不同的網段 • 單一掃描來源	• 小規模隨機 • 在相同網段或信任網段 • 分散掃描來源
攻擊方式	• 單純 • 漏洞攻擊	• 未知形態 • 社交工程 • 網站漏洞攻擊
後門及木馬運用模式	• 植入後馬上使用 • 本機開啟 Listen Port	• 潛伏等待 • 主動向外連線、匿蹤
駭客工具	• 一般網路上常見工具	• 自製工具、Rootkit • 惡意網站、網頁、電子郵件
目的	• 竊取資料檔案 • 偷取密碼 • 炫耀	• 竊取資料檔案 • 偷取密碼 • 生財工具

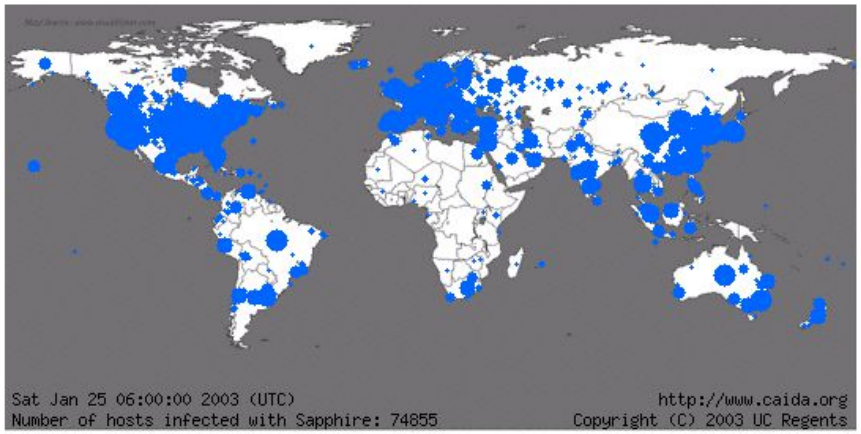
CodeRed ：Server漏洞與破壞病毒結合



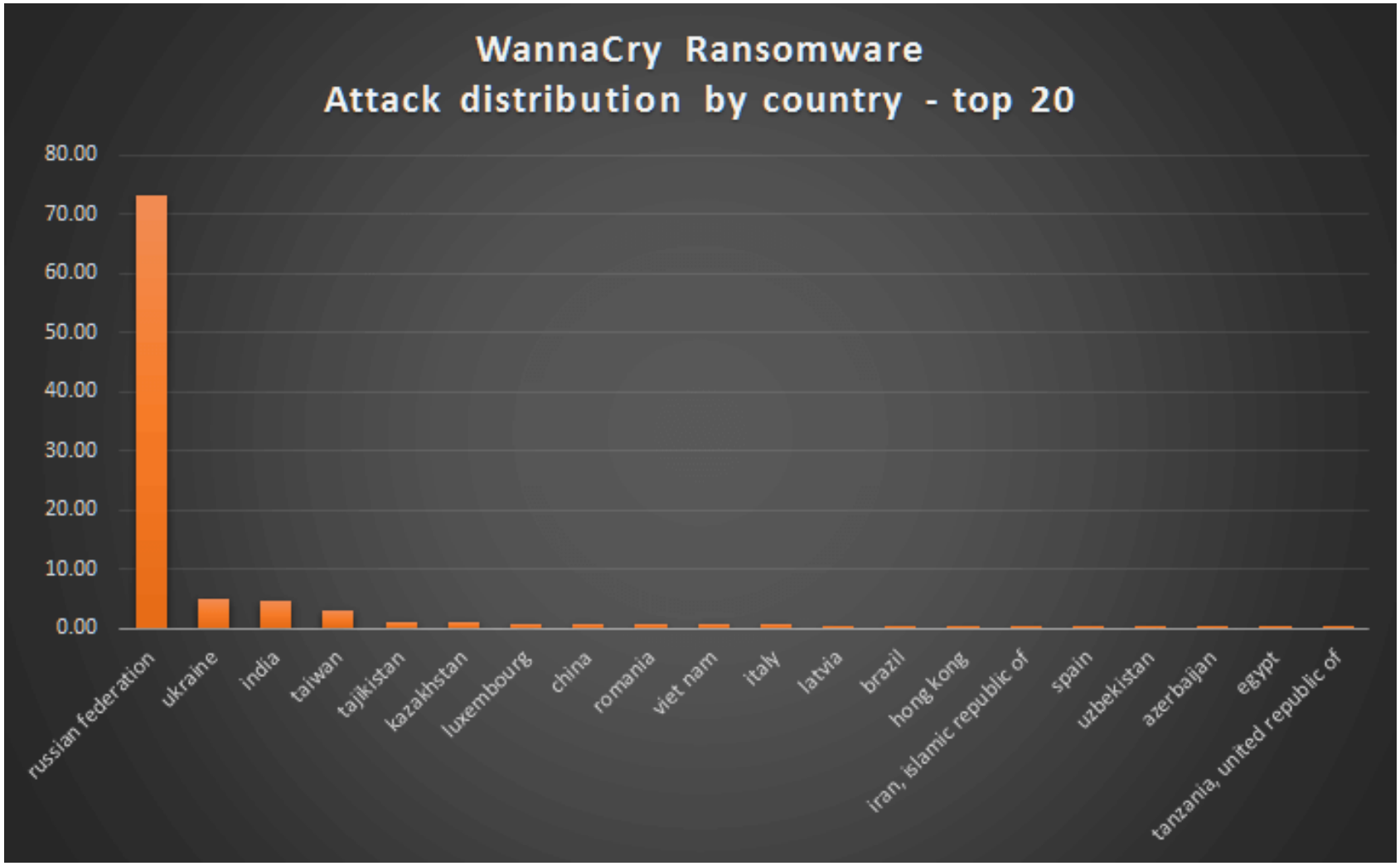
SQL Slammer ：系統漏洞造成網路癱瘓

Sapphire/Slammer Worm

- was the fastest computer worm in history
  - doubled in size every 8.5 seconds
  - infected more than 90 percent of vulnerable ~75K hosts within 10 minutes.



WannaCry ：Client漏洞與勒索病毒結合



資訊發展的趨勢

- 更貼近生活的應用
  - 手機網路化
  - 食衣住行電子化
  - 醫療生化晶片化
  - 網路依存度過高
- 更強大的計算能力
  - 雲端運算
  - 虛擬化環境

員工使用網路潛在的危機

- 網路瀏覽的安全風險
  - 間諜軟體(Spyware)
  - 惡意網站病毒(Malicious Mobile Code)
  - 釣魚詐欺(Phishing Attack)
  - 鍵盤側錄攻擊(Key-logger)
- 網路資源的誤用
  - 濫用網路存取(Internet Access)
  - 頻寬的誤用:
    - 串流媒體使用(Streaming Media)
    - 網路收音機(Internet radio)
- 欲禁止與管理的使用
  - 即時通訊(Instant Messaging)
  - P2P傳輸(Peer-to-peer file sharing)
- 惡意的意圖
  - 透過網路閘道的機密資料外洩
  - 內部網路的駭客行為(Employee Hacking)

IT 監守自監


檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
入侵永豐餘總裁信箱偷看…
www.appledaily.com.tw/realti
搜尋
入侵永豐餘總裁信箱偷看信　資訊經理判賠
永豐餘
蘋果即時
永豐餘集團外觀。資料照片
最新
字級：A- A A+
20170422 08:07
放假騎越野車受傷
邦賈納進傷兵名單(0)
20170422 08:06
賤男暴打元配　小
三叫囂「老子我要
弄死你」(0)
分享FB
分享g+
分享Plurk
分享Twitter
2017年04月20日15:56
傳送
讚
10
G+1
0
永豐餘集團子公司前徐姓資訊處長，利用曾設計、維
護集團的「Armada郵件系統」機會，竟竊用集團總
裁何壽川帳號，偷看何的信件，直到2012年才被查

不偷資料不破壞

iThome

美聯儲員工濫用組織伺服器挖礦賺比特幣，遭革職及罰款5000美元

該名員工利用職務之便，在其中一伺服器上安裝比特幣採礦軟體，並連上比特幣網路，美國聯邦儲備系統理事會確認後已將他革職，該員工也因侵佔政府資產被判處12個月緩刑、罰款5000美元。

文/ 陳曉莉 | 2017-02-02 發表

讚 4.3萬 按讚加入iThome粉絲團 讚 248 分享 G+

印表機不設防

File Edit View History Bookmarks Tools Help

別輕忽印表機安全，白帽...

www.ithome.com.tw/news/111674 80% Search

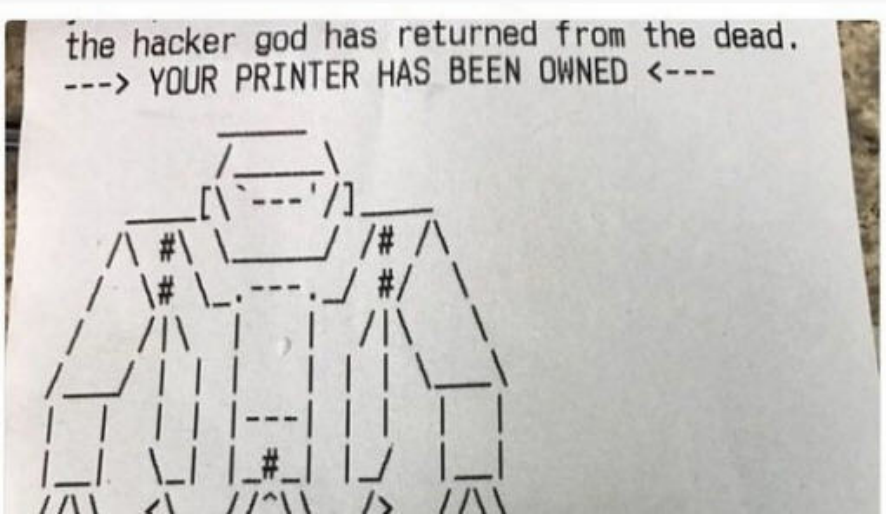
iThome

別輕忽印表機安全，白帽駭客入侵15萬台網路印表機示警

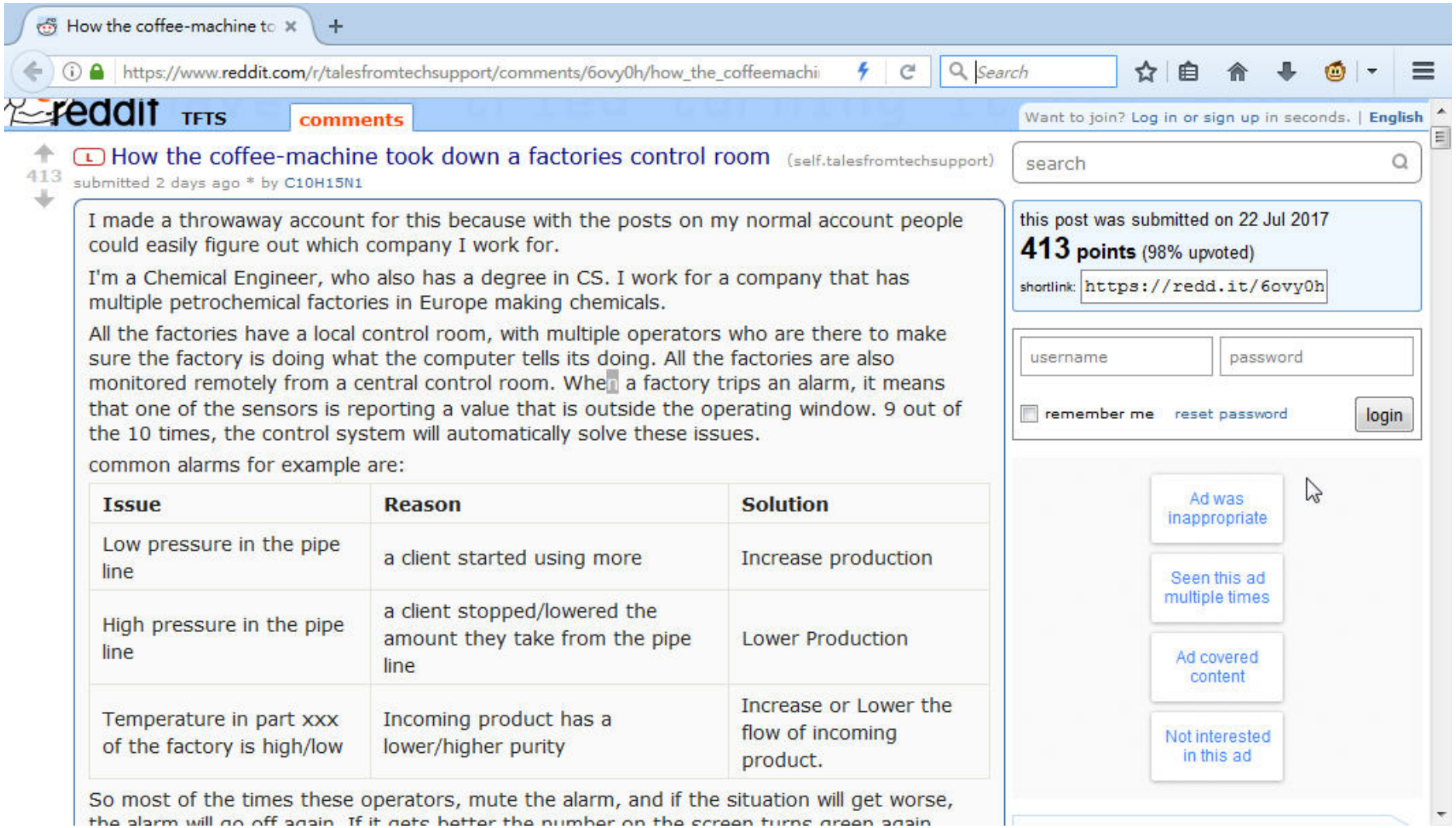
為喚起外界重視印表機安全，署名為Stackoverflowin的白帽駭客上周入侵15萬台網路印表機，遙控這些印表機列印出文字及圖案訊息，包括Canon、Epson、HP、Lexmark到Brother等主要品牌均受影響。

文/ 陳曉莉 | 2017-02-06 發表

3.7萬 按讚加入iThome粉絲團 分享 300 G+1 1



咖啡機維護不周害工廠中毒



饕客即駭客：自動販賣機漏洞

▲零食自動販賣機的失竊案對美國中央情報局來說實質損失不大，但面子可能就掛不住了。（圖／翻攝自天空新聞台）

賭場漁缸漏洞

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

完勝電影橋段 黑客用智能…

https://unwire.hk/2017/07/22/sma

搜尋

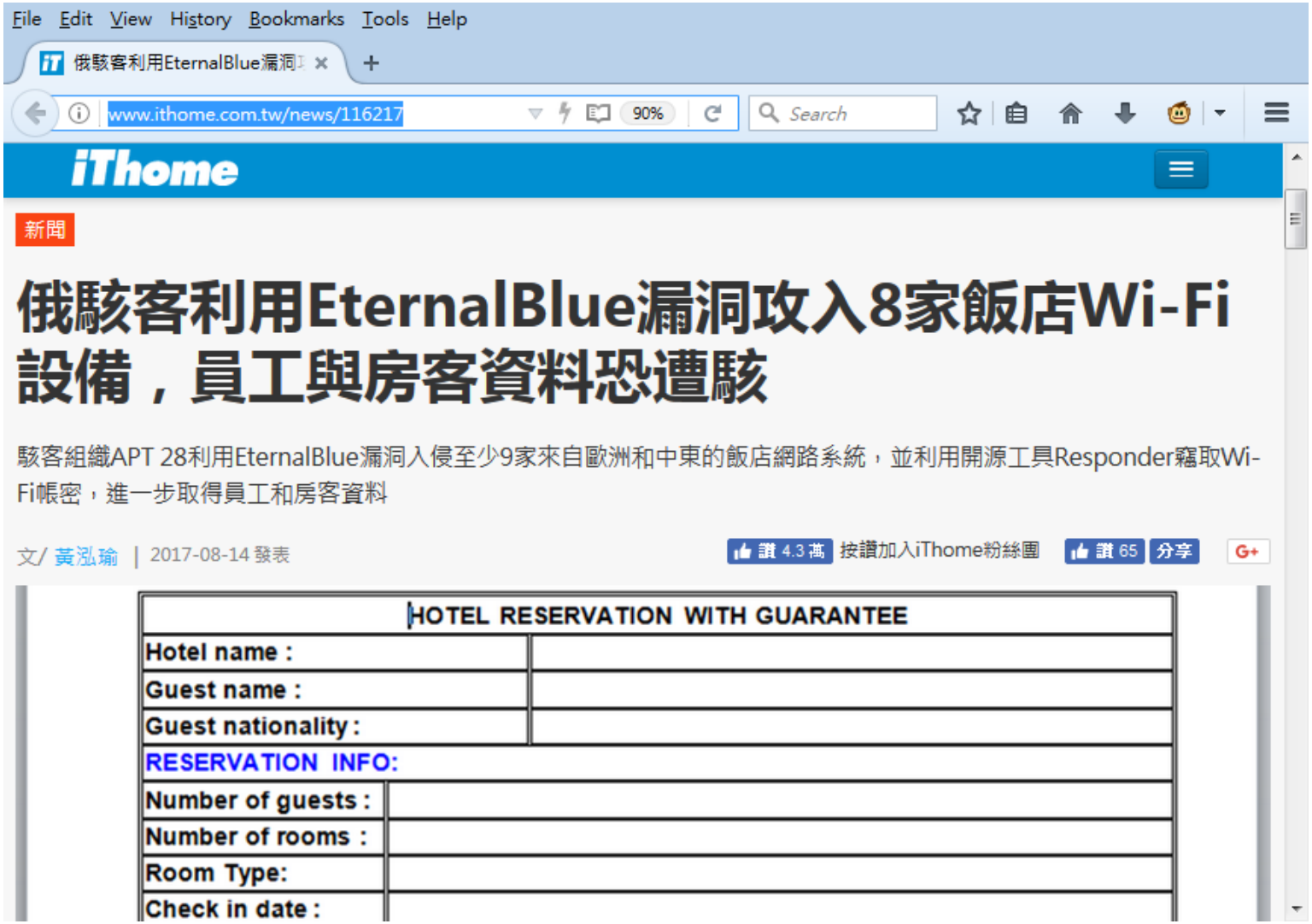
完勝電影橋段 黑客用智能魚缸入侵賭場

讚好此文: 讚好 33 分享

七月 22, 2017 • 作者忘記分類 •

賭場每天的金錢往來非常龐大，理應擁有很好的網絡保安措施，想不到一間位於北美的賭場，早前竟然被黑客成功入侵。賭場系統被入侵，情節其實並非如荷里活電影般曲折離奇，黑客只是藉著一個擁有連線功能智能魚缸的漏洞，就成功進入了賭場的網絡。

員工旅行去


File Edit View History Bookmarks Tools Help
俄駭客利用EternalBlue漏洞
www.ithome.com.tw/news/116217
90%
Search
iThome
新聞
俄駭客利用EternalBlue漏洞攻入8家飯店Wi-Fi設備，員工與房客資料恐遭駭
駭客組織APT 28利用EternalBlue漏洞入侵至少9家來自歐洲和中東的飯店網路系統，並利用開源工具Responder竊取Wi-Fi帳密，進一步取得員工和房客資料
文/ 黃泓瑜 | 2017-08-14 發表
讚 4.3 萬 按讚加入iThome粉絲團
讚 65 分享
G+
HOTEL RESERVATION WITH GUARANTEE
Hotel name :
Guest name :
Guest nationality :
RESERVATION INFO:
Number of guests :
Number of rooms :
Room Type:
Check in date :

人體藏毒


DNA 也可變身成惡意軟體
https://technews.tw/2017/08/14/dna-malicious-progra-hacker/
DNA 也可變身成惡意軟體，科學家嘗試用其感染電腦
作者 林 亭妤 | 發布日期 2017 年 08 月 14 日 9:00 | 分類 生物科技 , 科技趣聞 , 電腦
Follow
G+
讚 111
分享
gcgaggaaaggcgtatatgcggagt
gagagcgctcttatcggcgatta
gtgcggagtcgatgcgatcgg
gcgaggctagcgtatgcta

資訊人員的取捨

安全
Security

效能
Performance

便利
Convenient

管理/實作能力
Administration

成本
Cost

DoS 與 DDoS 攻擊

DOS/DDOS

- DOS – Denial Of Service
  - 藉由各種的攻擊手法，使資訊服務無法正常運作
- DDOS – Distributed DOS
  - 由多重來源進行攻擊，使資訊服務無法正常運作
- 目的
  - 勒索獲利
  - 打擊競爭對手
  - 政治意圖
  - 引人注意
  - 練功

卡巴斯基實驗室最新DDoS趨 ×

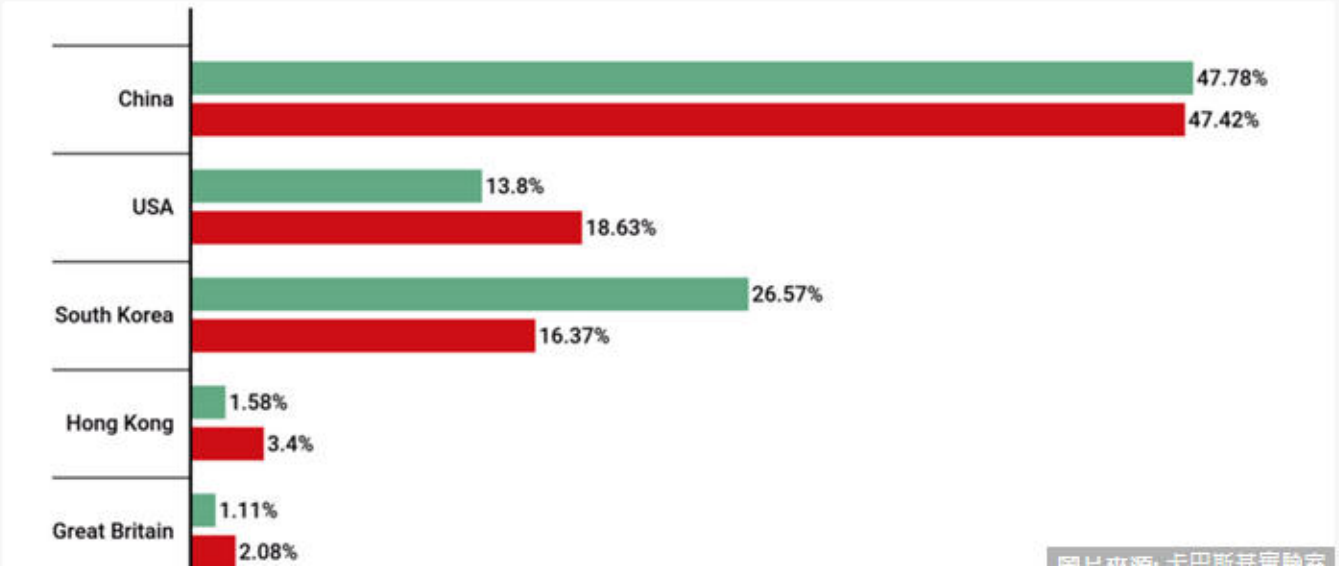
www.ithome.com.tw/ne 90% Search

iThome

卡巴斯基實驗室最新DDoS趨勢報告：勒索型DDoS攻擊越來越盛行

報告表示，勒索DDoS門檻低，攻擊者不需要擁有高程度的網路攻擊能力也能發動，造成這類攻擊數量越來越多，攻擊者只要懂得寫威脅信，或是購買現成殭屍網路，就能夠發動。

文/ 黃泓瑜 | 2017-08-07 發表



〈券商遭駭客威脅〉驚！他們集體接到這封恐嚇信...

鉅亨網記者王莞甯 台北　2017/02/03 22:11

相關個股　元富證 8.66 +1.52%　群益證 9.22 +0.11%　中華電 100 0%　大展證 11.9 -0.83%

金雞年開工才 2 天，今 (3) 日就傳出國內多家券商接獲駭客訊息，要求支付價值約新台幣 17 萬元的比特幣，相關消息已獲元富證券 (2856-TW) 與凱基證證實。元富證強調，接獲訊息約半個小時即排除狀況，對投資人交易和資料安全無影響；凱基證則說，有收到威脅信，但該公司系統未遭攻擊也無任何異常狀況發生。

以下為此次駭客對元富證勒索信函：

Right now we will start 15 minutes attack on one of your IPs (202.39.34.23).
It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

今日傳出國內券商包括元富證、元大證、群益證、凱基證和大展證等接獲駭客訊息，要求支付折合新台幣約 17 萬元的比特幣，否則將引爆植入的木馬，證期局已緊急應變處理。

《思科2017年中網路安全報告》預測新型「摧毀服務」攻擊

首頁
台灣思科
新聞中心
思科年度安全報告指出 進階攻擊與惡意傳輸讓網路威脅達至前所未見新高
喜憨兒基金會、思科與岱凱攜手傳愛
思科擴展應用中心基礎架構至存取及廣域網路 增強網路自動化及IT靈活性
思科擴展進階惡意軟體防護及數據中心安全方案應付充斥於終端、網路、雲端的進階威脅
思科持續革新協同合作模式 - 迎接個人化通訊時代的降臨
思科視覺網路指標預測到2018年網路數據年流量成長將高於20% 達到1.6 Zettabytes
思科在美洲x86刀鋒伺服器營收市佔率位居榜首

《思科2017年中網路安全報告》預測新型「摧毀服務」攻擊
資安威脅的規模與影響與日俱增

關鍵產業必須改善資安狀況以配合資訊與營運技術融合的趨勢

【2017年7月26日，台灣訊】——《思科®2017年中網路安全報告》揭露快速演進的資安威脅與不斷擴大規模的攻擊，並預測潛在的「摧毀服務（Destruction of Service，DeOS）」將會竄起。DeOS攻擊能夠徹底崩潰組織的備援與安全網，以致在受到攻擊後無法回復系統與資料。隨著物聯網的興起，關鍵產業將更多營運業務移到網際網路上，促使攻擊的接觸點變得更廣大，而這些攻擊的潛在規模與影響也持續提高。

近期攻擊事件如WannaCry 與Nyetya顯露出快速散播與衝擊層面的廣泛，表面上它們看似傳統的勒索軟體，但實際上它們更具破壞性。思科稱之為「摧毀服務」攻擊，相比傳統網路攻擊，它們可帶來更嚴重的破壞，讓企業完全無法復原。

另外，物聯網持續為這些網路犯罪者提供新的機會，而潛伏其中的許多資安弱點會逐漸被發掘，促使未來更多新型的攻擊手法產生，造成越來越嚴重的影響。最近出現的物聯網僵屍網路（Botnet）已反映出有些攻擊者可能預先打好基礎，伺機發動大規模高影響的攻擊，甚至對整個網際網路造成破壞。

面對這些攻擊，衡量資安措施的成效至關重要。思科持續追蹤「威脅偵測時間（Time-to-

DoS的攻擊目標

- 破壞目標實體設備
- 癱瘓目標服務網路
  - 頻寬消耗(Bandwidth Depletion)
  - 干擾連線 (Disrupt connection)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者

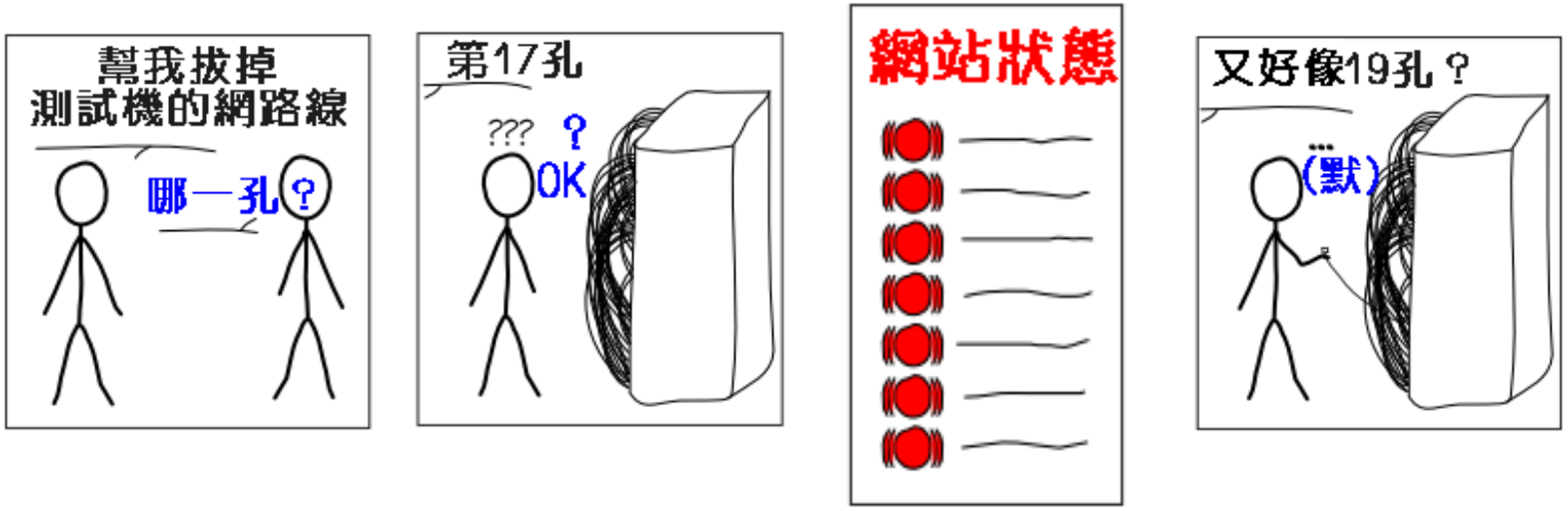
DoS的攻擊目標

- 破壞目標實體設備
- 癱瘓目標服務網路
  - 頻寬消耗(Bandwidth Depletion)
  - 干擾連線 (Disrupt connection)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者

實體破壞

- 機房主機
- 網路設備
- 無線AP
- 網路線
- 網路/實像攝影機
- 硬碟I/O
- 水電資源

實體破壞 – 機房管理



- 某政黨總部機房管理實例

實體破壞 – 乖乖

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

機房乖乖逾期了... @ 呻吟 ...

blog.xuite.net/blue_jacky/mind/60537528-機房乖乖逾

OP)跟移民署的人 (

新增內容 | 管理後台 | 瀏覽模式 | 分享好友 | 站長日誌 登入 | 短網址 | 工具

管電腦凸槌／當機36小時 一個血淋淋的乖乖事件. 乖乖真的很重要...不能亂吃

：昨天去桃園機場拿回移民署備品， 聽到大同的OP(以下簡稱OP)跟移民署的人
對話如下：

OP：「對啊！我們元旦那天有來加班，作一作一堆人就肚子餓了！ 想說機房的一些雜物先收一下，於是就把機房的乖乖收下來吃掉.....」

某A：「不會吧！？你們把那些乖乖吃掉了喔！？」

OP：「對啊！就想說反正我們今年也沒有標到.....」

於是.....

1/3 第二航廈的 E10K 當機，系統切換到一航廈主機

1/5 早上五點多，一航廈 EMC storage 當機，DB crash.....

1/5 11:30，榮登奇摩頭條！ 13:00，內政部長至機場巡視.....

一個血淋淋的乖乖事件..... 乖乖真的很重要...不能亂吃

之前是大同...大同把乖乖吃了...神通接手就掛點了...

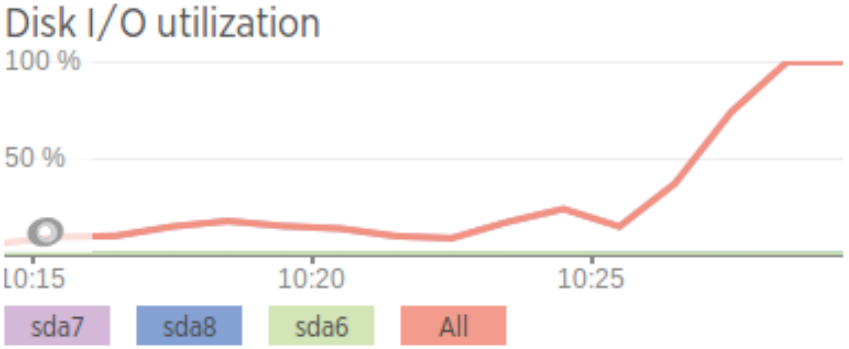
新聞報導

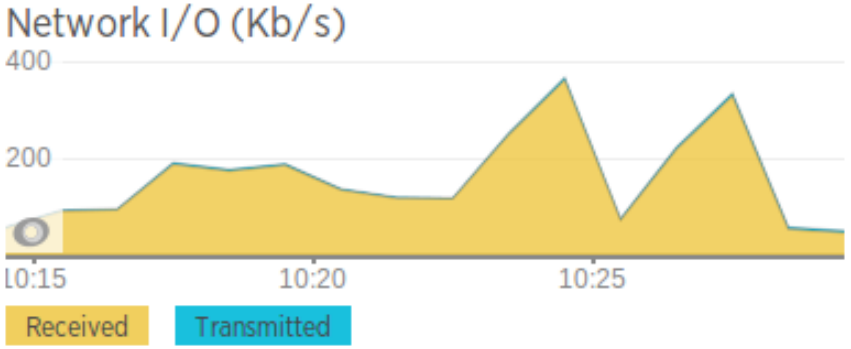
從 pixel.facebook.com 接收資料...

實體破壞 – 硬碟I/O

現在企業級硬碟(理論上)比較難死

另一個實例：
crontab 設定
*/1 * * * * reboot

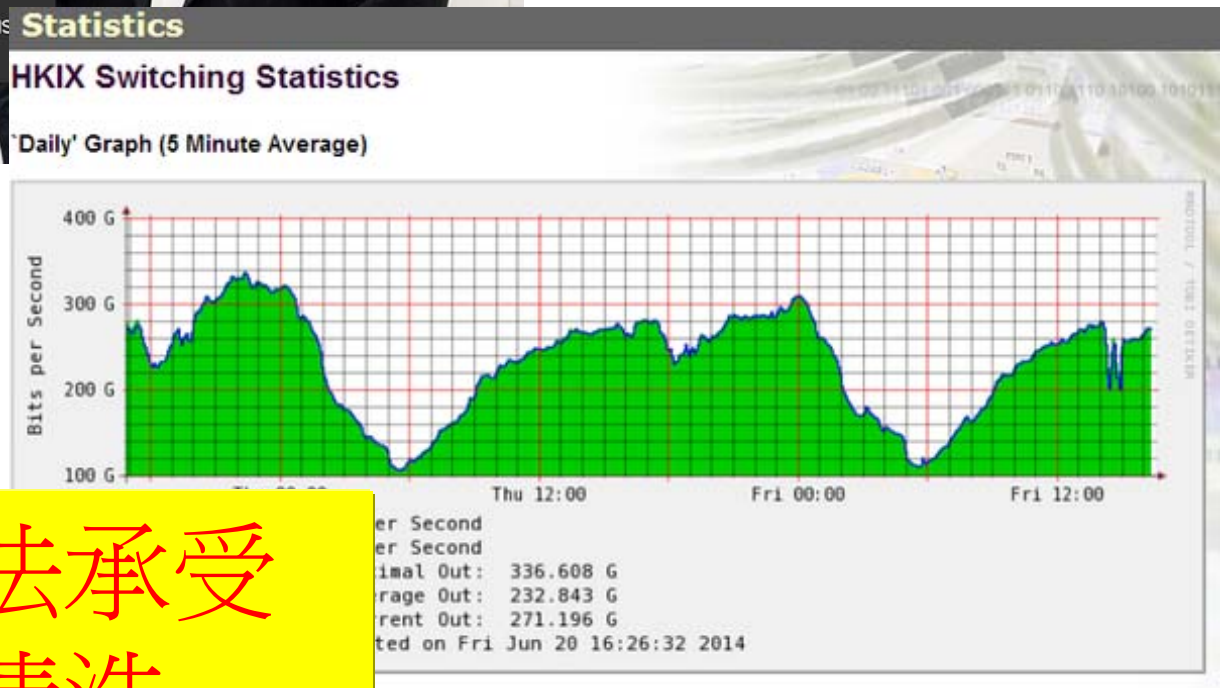




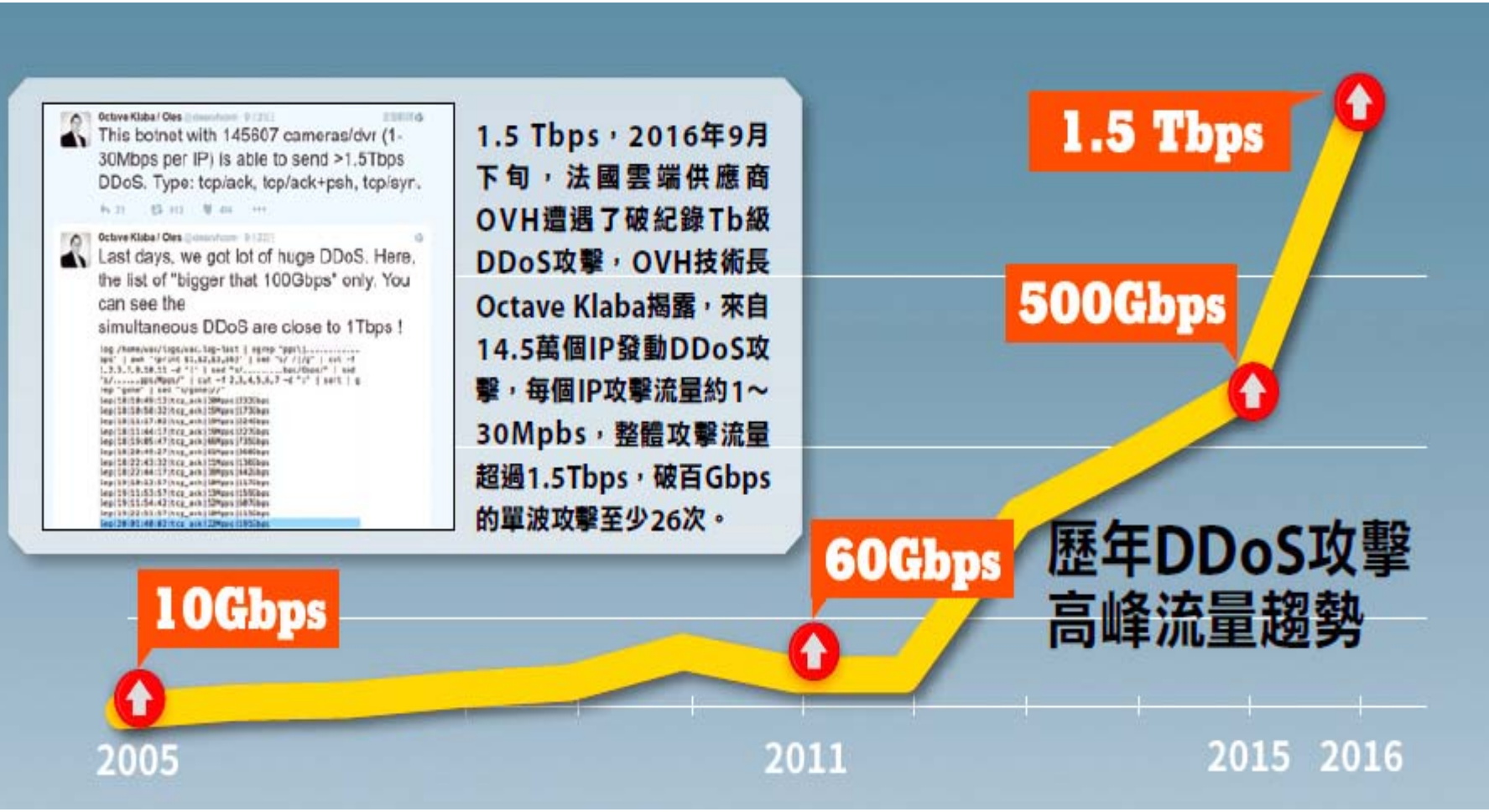
DoS的攻擊目標

- 破壞目標實體設備
- 癱瘓目標服務網路
  - 頻寬消耗(Bandwidth Depletion)
  - 干擾連線 (Disrupt connection)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者


50萬IoT遭駭裝置潛伏全球
殭屍大軍租一天只要7千元
Tb級
DDoS海嘯
來襲
你擋得住嗎？



主機已無法承受
只能靠清洗


Octave Klaba / Oles
This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.
Octave Klaba / Oles
Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the simultaneous DDoS are close to 1Tbps !
1.5 Tbps，2016年9月下旬，法國雲端供應商OVH遭遇了破紀錄Tb級DDoS攻擊，OVH技術長Octave Klaba揭露，來自14.5萬個IP發動DDoS攻擊，每個IP攻擊流量約1～30Mpbs，整體攻擊流量超過1.5Tbps，破百Gbps的單波攻擊至少26次。
1.5 Tbps
500Gbps
60Gbps
10Gbps
歷年DDoS攻擊
高峰流量趨勢
2005
2011
2015
2016

不同層級頻寬消耗

- **頻寬**攻擊：灌爆頻寬，一般採用Stateless(可偽冒來源)
  - SYN Flood
  - ACK/RST Flood
  - UDP/ICMP Flood
  - Fragment Packet Attack
  - Any packet flooding (ip/tcp/udp/icmp/…)
- **網路設備**攻擊：癱瘓路由器、防火牆、負載平衡器、入侵防禦系統 … 等網路設備
  - Syn/ack/rst/connection … 等等
- **增強效果(Amplification)**攻擊：放大攻擊的技巧
  - Fraggle, Smurf, DrDoS, DNS/NTP Amplificationattack

頻寬消耗應對策略

ISP防護中心

中華、臺固、遠傳

流量清洗中心

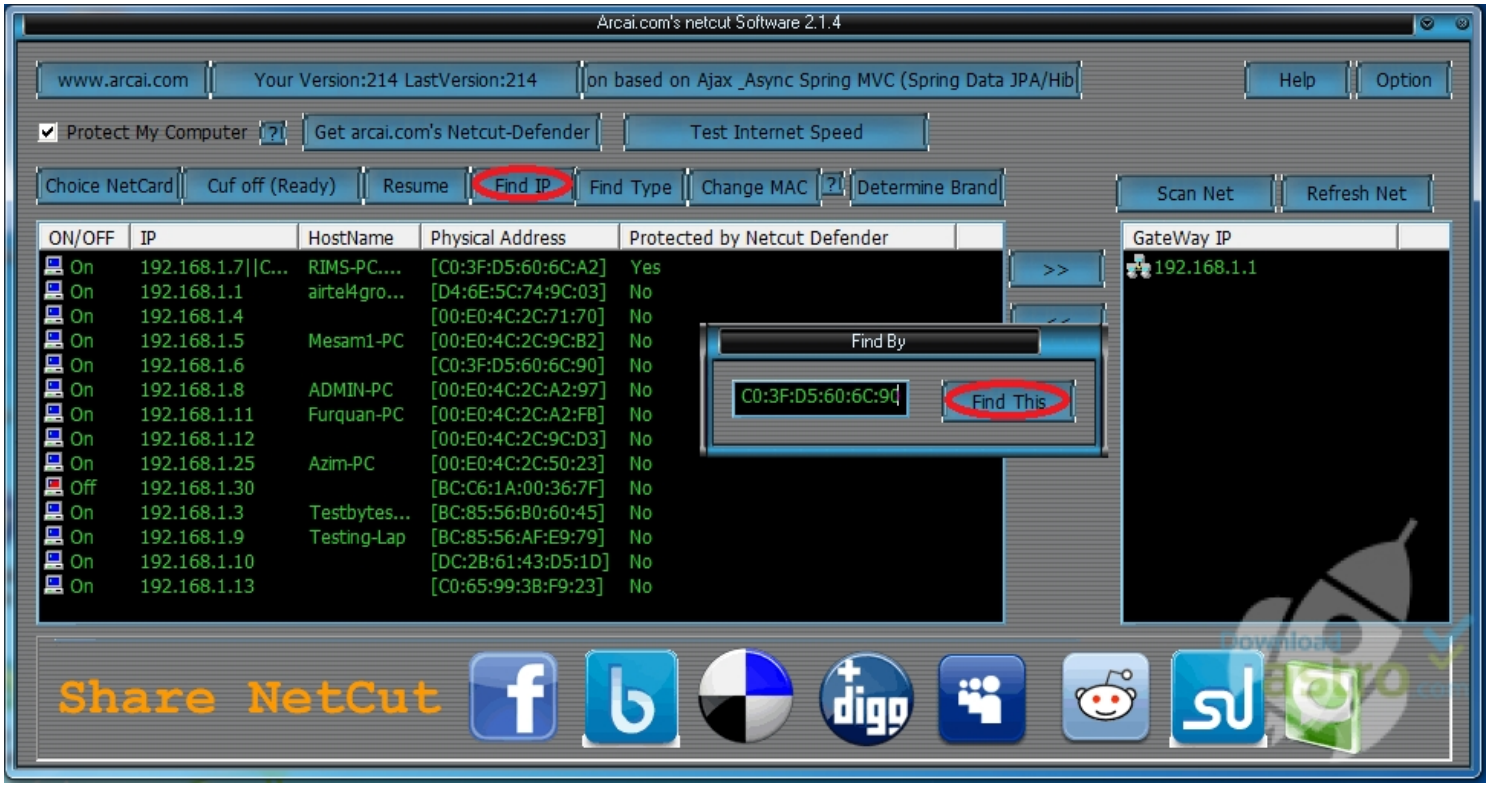
Akamai、Nexusguard

DoS的攻擊目標

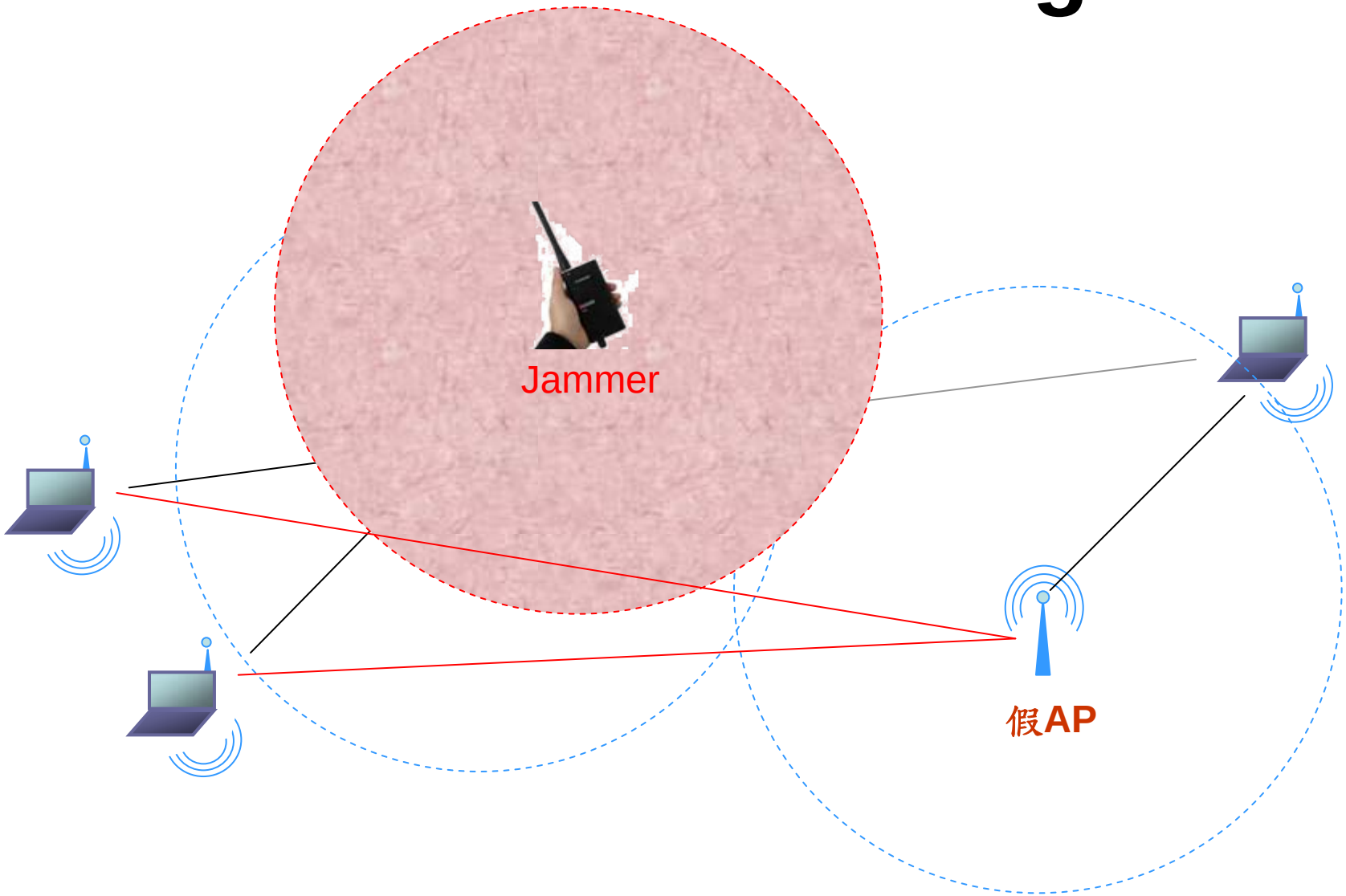
- 破壞目標實體設備
- 癱瘓目標服務網路
  - 頻寬消耗(Bandwidth Depletion)
  - 干擾連線 (Disrupt connection)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者

干擾連線

- NetCut
- (Wireless) De-authentication



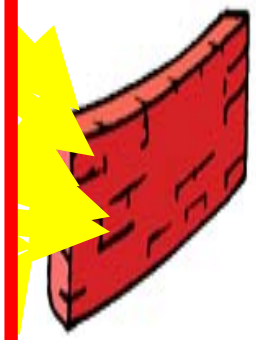
Wireless Jamming



低帶寬DDoS攻擊可癱瘓防火牆

2016-11-14 16:47:00

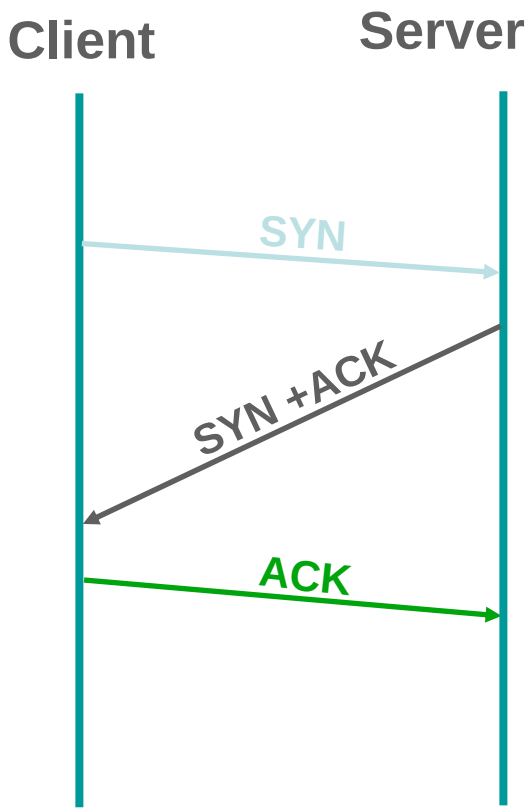
研究人員警告：特定類型的低帶寬分布式拒絕服務(DDoS)攻擊，可以導致某些廣爲使用的企業級防火牆陷入暫時的拒絕服務狀態。



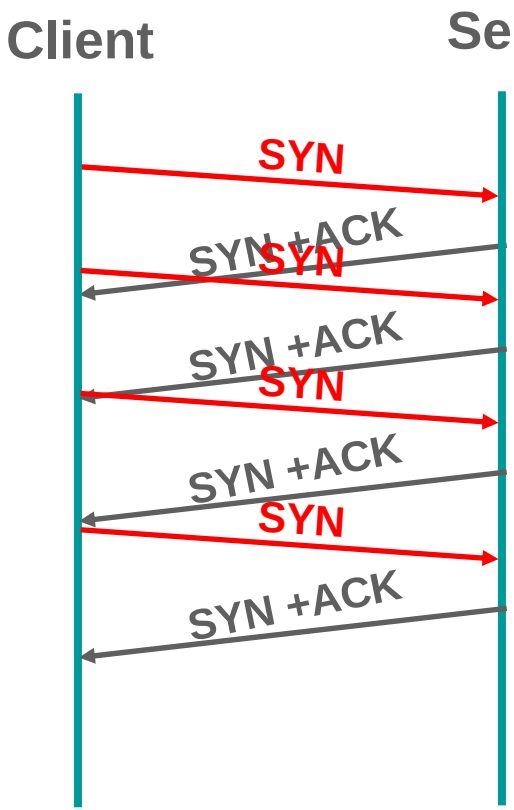
SYN Flood

- 發送大量的 SYN 封包，使網路設備、或伺服器的 Session Table 連線狀態陷入 SYN_RCVD，而無法接受新連線
- 只要 [發送速率] > [Timeout速率]，即可讓服務一直處於癱瘓狀態
- 防護方式
  - SYN Proxy / Server
    - 加大 Table
    - 縮短 timeout
  - SYN Cookie
  - RFC 4987

SYN Flood DDOS Attack



正常建立TCP連線



填滿
Session Table！

SYN Flooding

讓目標設備保持在SYN_RECV

簡單的算式

- SYN 封包
  - IP + TCP Header length = 46 bytes
  - Ethernet Frame size = 64 bytes
  - 實際運作時加上overhead平均長度 = 84 bytes
- 1Mbps 的頻寬約可發出 1560 pps SYN
  - 100Mbps ＝＞ 156,000 pps SYN
    - 已足已癱瘓大部份中階之防火牆
  - 500Mbps ＝＞ 780,190 pps SYN
    - 許多高階設備亦無法承受
- 一般資安設備的 New Session/s 大部份不高

影響攻擊效率的因素

- 頻寬
  - 100 Mbps
    - ~ 156,000 pps
  - 1000 Mbps
    - ~ 1,560,000 pps
  - 10Gbps !?
    - !? !? !? !? !?
- 攻擊程式之效率
- 肉雞等級
  - CPU
  - NIC
- 肉雞平台
  - Linux
  - UNIX-based
  - Windows

經過優化的攻擊程式

- 測試實例
  - On Linux 2.6 kernel
  - Intel chip NIC
  - 一台Thinkpad X220
- 結果：1,000,000 pps

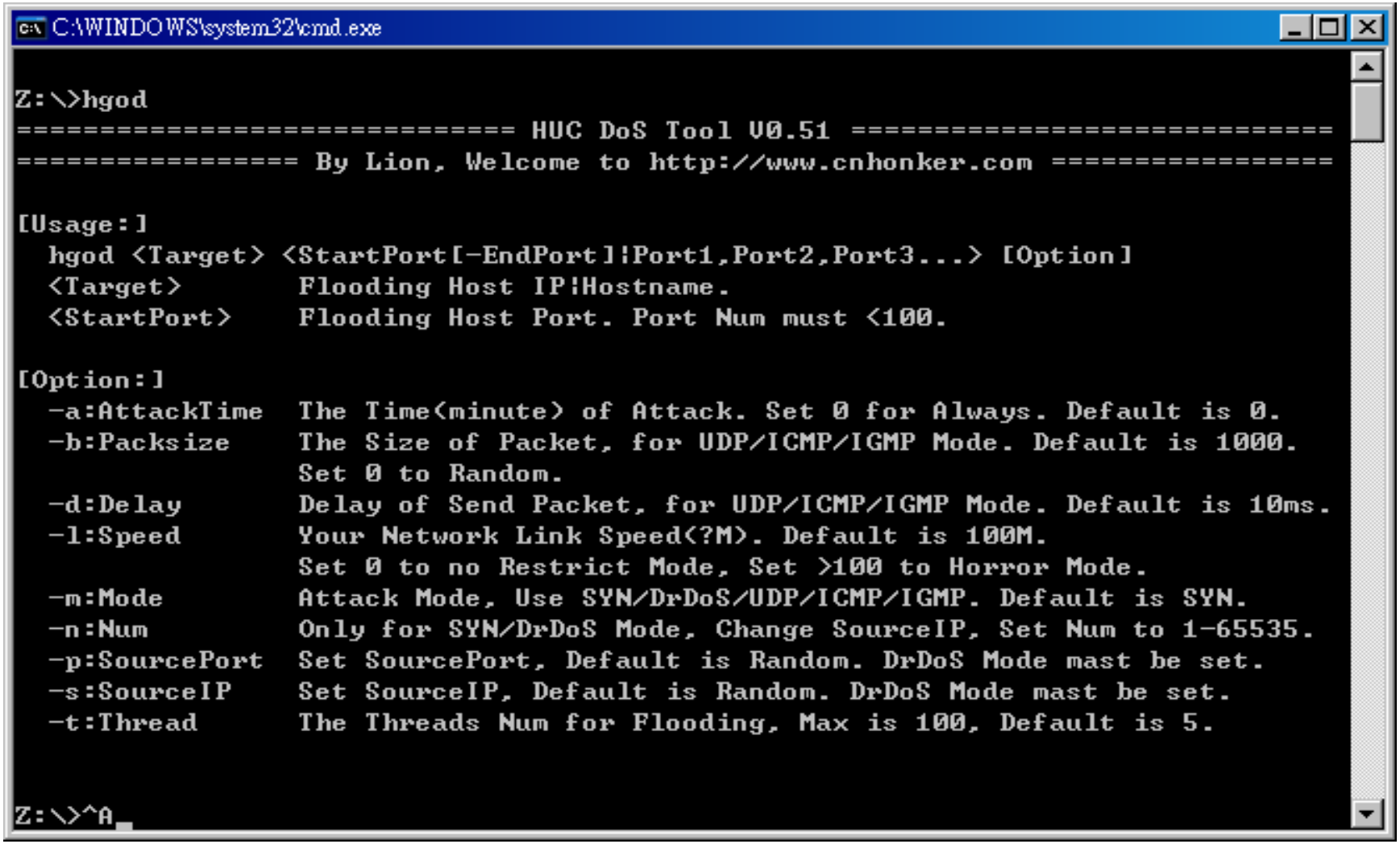
RFC 4987

- TCP SYN Flooding Attacks and Common Mitigations
  - Filtering
  - Increasing Backlog
  - Reducing SYN-RECEIVED Timer
  - Recycling the Oldest Half-Open TCB
  - SYN Cache
  - SYN Cookies
  - Hybrid Approaches
  - Firewalls and Proxies

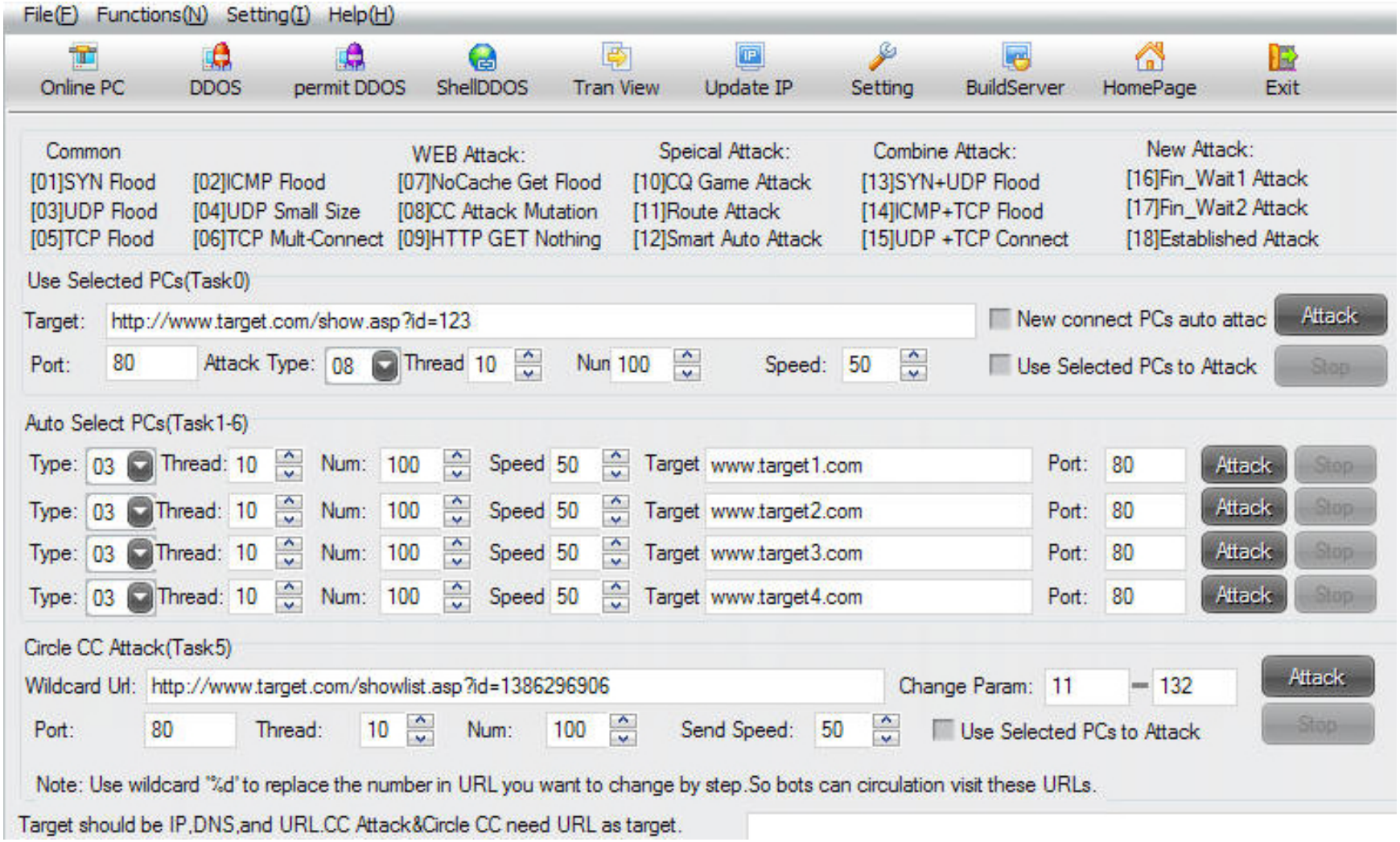
Attack Tools

- http://www.packetstormsecurity.org/
- Before WinXP sp1
  - hping
  - HGod
  - ……..
- After WinXP sp1
  - Using WinPcap
- Linux
  - tfn/tfn2k
  - juno.c
  - synk4.c
  - netflood.cpp
  - d0s.pl

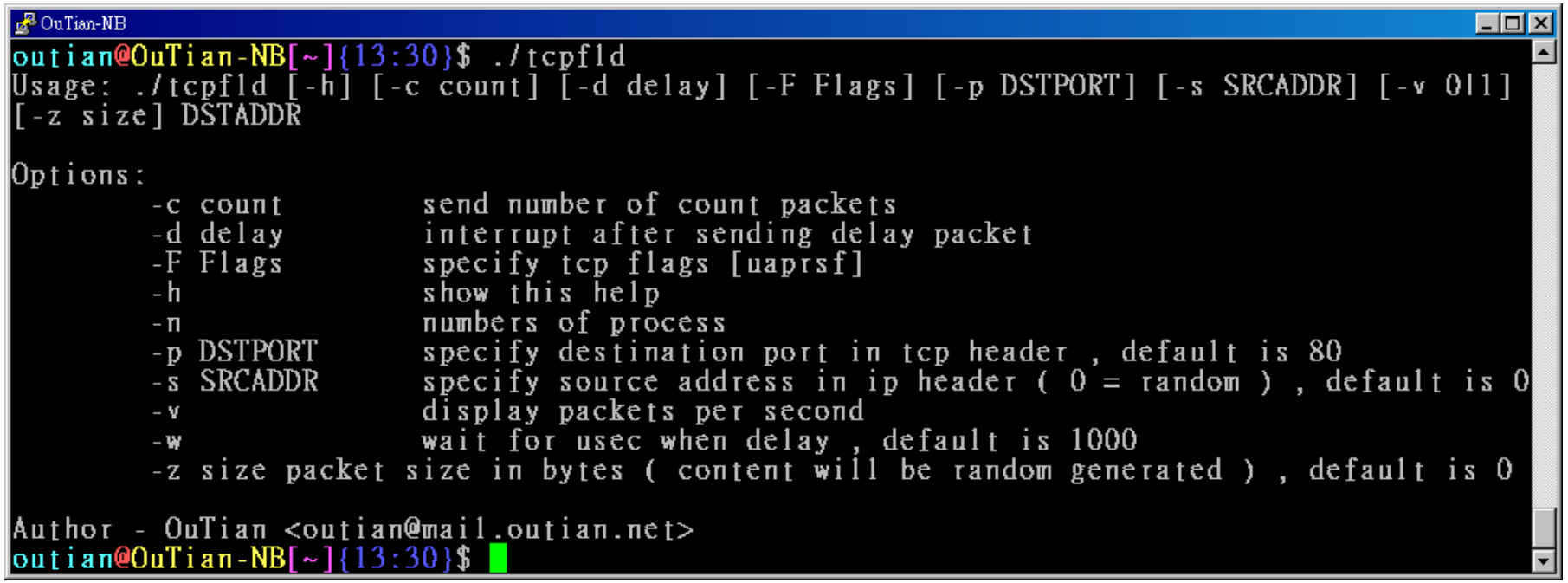
Hgod


C:\WINDOWS\system32\cmd.exe
Z:\>hgod
============================== HUC DoS Tool V0.51 ==============================
================= By Lion, Welcome to http://www.cnhonker.com =================
[Usage:]
hgod <Target> <StartPort[-EndPort]|Port1,Port2,Port3...> [Option]
<Target> Flooding Host IP|Hostname.
<StartPort> Flooding Host Port. Port Num must <100.
[Option:]
-a:AttackTime The Time(minute) of Attack. Set 0 for Always. Default is 0.
-b:Packsize The Size of Packet, for UDP/ICMP/IGMP Mode. Default is 1000.
Set 0 to Random.
-d:Delay Delay of Send Packet, for UDP/ICMP/IGMP Mode. Default is 10ms.
-l:Speed Your Network Link Speed(?M). Default is 100M.
Set 0 to no Restrict Mode, Set >100 to Horror Mode.
-m:Mode Attack Mode, Use SYN/DrDoS/UDP/ICMP/IGMP. Default is SYN.
-n:Num Only for SYN/DrDoS Mode, Change SourceIP, Set Num to 1-65535.
-p:SourcePort Set SourcePort, Default is Random. DrDoS Mode mast be set.
-s:SourceIP Set SourceIP, Default is Random. DrDoS Mode mast be set.
-t:Thread The Threads Num for Flooding, Max is 100, Default is 5.
Z:\>^A

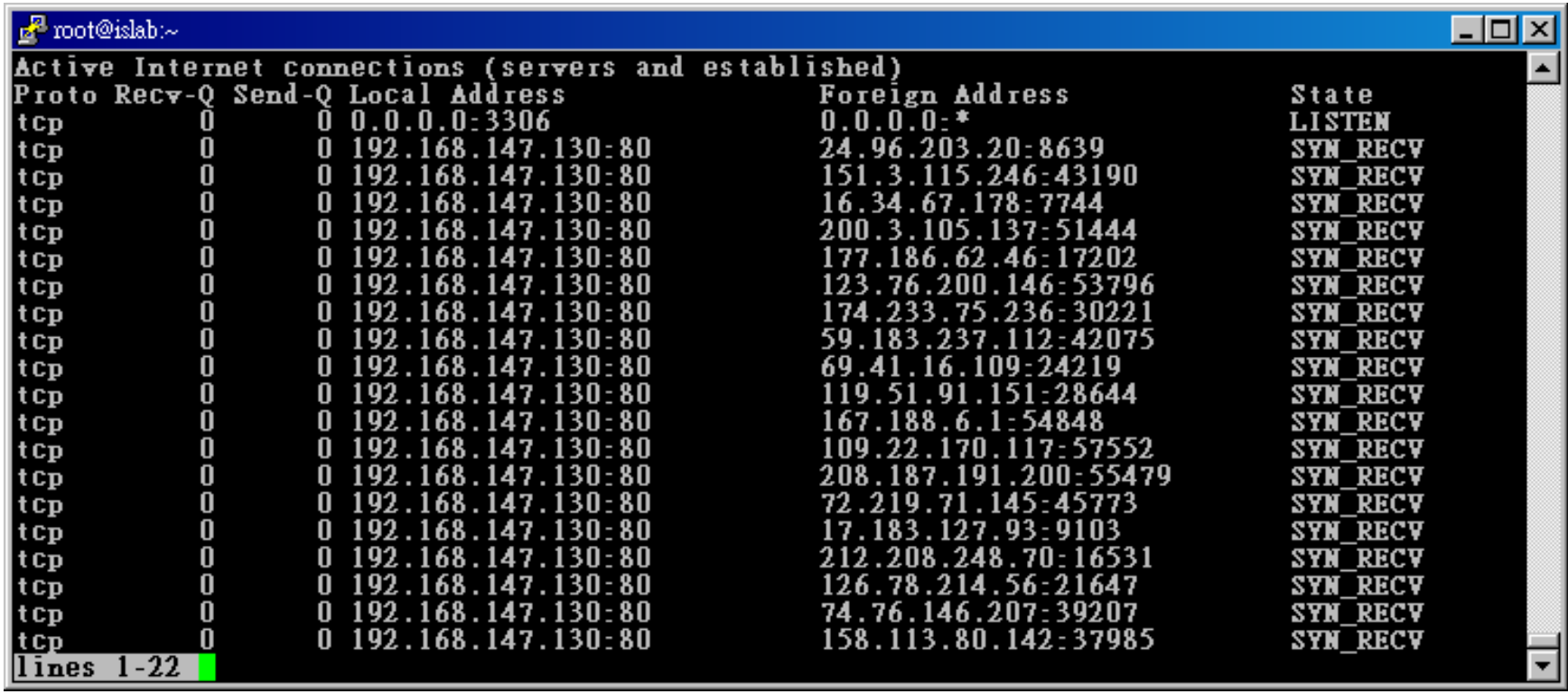
DDoS 工具控制台


File(F) Functions(N) Setting(I) Help(H)
Online PC
DDOS
permit DDOS
ShellDDOS
Tran View
Update IP
Setting
BuildServer
HomePage
Exit
Common
[01]SYN Flood
[02]ICMP Flood
[03]UDP Flood
[04]UDP Small Size
[05]TCP Flood
[06]TCP Mult-Connect
WEB Attack:
[07]NoCache Get Flood
[08]CC Attack Mutation
[09]HTTP GET Nothing
Speical Attack:
[10]CQ Game Attack
[11]Route Attack
[12]Smart Auto Attack
Combine Attack:
[13]SYN+UDP Flood
[14]ICMP+TCP Flood
[15]UDP +TCP Connect
New Attack:
[16]Fin_Wait1 Attack
[17]Fin_Wait2 Attack
[18]Established Attack
Use Selected PCs(Task0)
Target: http://www.target.com/show.asp?id=123
New connect PCs auto attac
Attack
Port: 80
Attack Type: 08
Thread 10
Nun 100
Speed: 50
Use Selected PCs to Attack
Stop
Auto Select PCs(Task1-6)
Type: 03 Thread: 10 Num: 100 Speed 50 Target www.target1.com Port: 80 Attack Stop
Type: 03 Thread: 10 Num: 100 Speed 50 Target www.target2.com Port: 80 Attack Stop
Type: 03 Thread: 10 Num: 100 Speed 50 Target www.target3.com Port: 80 Attack Stop
Type: 03 Thread: 10 Num: 100 Speed 50 Target www.target4.com Port: 80 Attack Stop
Circle CC Attack(Task5)
Wildcard Url: http://www.target.com/showlist.asp?id=1386296906
Change Param: 11 - 132
Attack
Port: 80
Thread: 10
Num: 100
Send Speed: 50
Use Selected PCs to Attack
Stop
Note: Use wildcard '%d' to replace the number in URL you want to change by step.So bots can circulation visit these URLs.
Target should be IP,DNS,and URL.CC Attack&Circle CC need URL as target.

自製工具


OuTian-NB
outian@OuTian-NB[~]{13:30}$ ./tcpfld
Usage: ./tcpfld [-h] [-c count] [-d delay] [-F Flags] [-p DSTPORT] [-s SRCADDR] [-v 0|1]
[-z size] DSTADDR
Options:
-c count send number of count packets
-d delay interrupt after sending delay packet
-F Flags specify tcp flags [uaprsf]
-h show this help
-n numbers of process
-p DSTPORT specify destination port in tcp header , default is 80
-s SRCADDR specify source address in ip header (0 = random) , default is 0
-v display packets per second
-w wait for usec when delay , default is 1000
-z size packet size in bytes (content will be random generated) , default is 0
Author - OuTian <outian@mail.outian.net>
outian@OuTian-NB[~]{13:30}$

攻擊結果


root@islab:~
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN
tcp 0 0 192.168.147.130:80 24.96.203.20:8639 SYN_RECV
tcp 0 0 192.168.147.130:80 151.3.115.246:43190 SYN_RECV
tcp 0 0 192.168.147.130:80 16.34.67.178:7744 SYN_RECV
tcp 0 0 192.168.147.130:80 200.3.105.137:51444 SYN_RECV
tcp 0 0 192.168.147.130:80 177.186.62.46:17202 SYN_RECV
tcp 0 0 192.168.147.130:80 123.76.200.146:53796 SYN_RECV
tcp 0 0 192.168.147.130:80 174.233.75.236:30221 SYN_RECV
tcp 0 0 192.168.147.130:80 59.183.237.112:42075 SYN_RECV
tcp 0 0 192.168.147.130:80 69.41.16.109:24219 SYN_RECV
tcp 0 0 192.168.147.130:80 119.51.91.151:28644 SYN_RECV
tcp 0 0 192.168.147.130:80 167.188.6.1:54848 SYN_RECV
tcp 0 0 192.168.147.130:80 109.22.170.117:57552 SYN_RECV
tcp 0 0 192.168.147.130:80 208.187.191.200:55479 SYN_RECV
tcp 0 0 192.168.147.130:80 72.219.71.145:45773 SYN_RECV
tcp 0 0 192.168.147.130:80 17.183.127.93:9103 SYN_RECV
tcp 0 0 192.168.147.130:80 212.208.248.70:16531 SYN_RECV
tcp 0 0 192.168.147.130:80 126.78.214.56:21647 SYN_RECV
tcp 0 0 192.168.147.130:80 74.76.146.207:39207 SYN_RECV
tcp 0 0 192.168.147.130:80 158.113.80.142:37985 SYN_RECV
lines 1-22

ACK/RST Flood

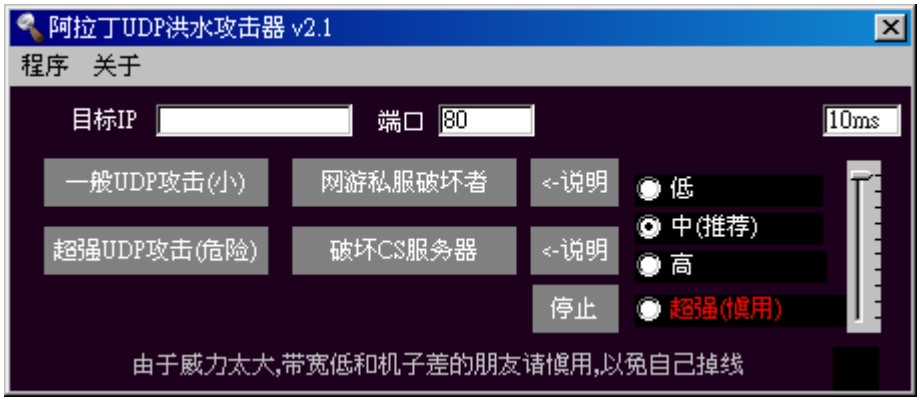
- 假造來源發送大量的ACK/RST封包
- Firewall、Proxy、L4、或任何主機，將需搜尋本身之Session Table，若未存在該連線則回應 RST (或 Drop 封包)
- 兩種效果 –
  - 使網路設備、或主機負荷升高
  - 使Outbound頻寬滿載
- 缺點 –
  - Stateful 設備（例如防火牆）會直接Drop封包

UDP/ICMP Flood

- 假造來源發送大量的UDP/ICMP封包
- 多數攻擊程式在刻製封包的overhead較TCP為低，故封包發送速度快、內容易客製
- 攻擊目的 – 使目標頻寬滿載
- 阻擋方式 –
  - 以Firewall或ACL攔截過濾封包
  - 以IPS辨識非正常協定之封包
  - 設定QOS限制PPS

UDP Flood

- Windows
  - 阿拉丁洪水攻擊器



- Linux
  - pktgen (kernel module)
  - Scapy
    - http://www.secdev.org/projects/scapy/

Fragment Packet Flood

- 發送大封包時，切割為眾多小封包進行傳送
- 使主機或網路設備虛耗大量時間於重組封包，而導致負荷升高、處理速度降低
- 阻擋方式 –
  - 阻擋由外至內的切割封包
  - 禁止特定協定的封包切割行為

增強效果攻擊

- 常用的手法是反彈式攻擊 (Distributed Reflection DoS, DrDoS)：由駭客偽造受害者IP送出詢問封包，路由器會將回應封報寄給第三方受害者。
  - Fraggle
  - Smurf
  - DrDoS
  - DNS/NTP Amplification Attack

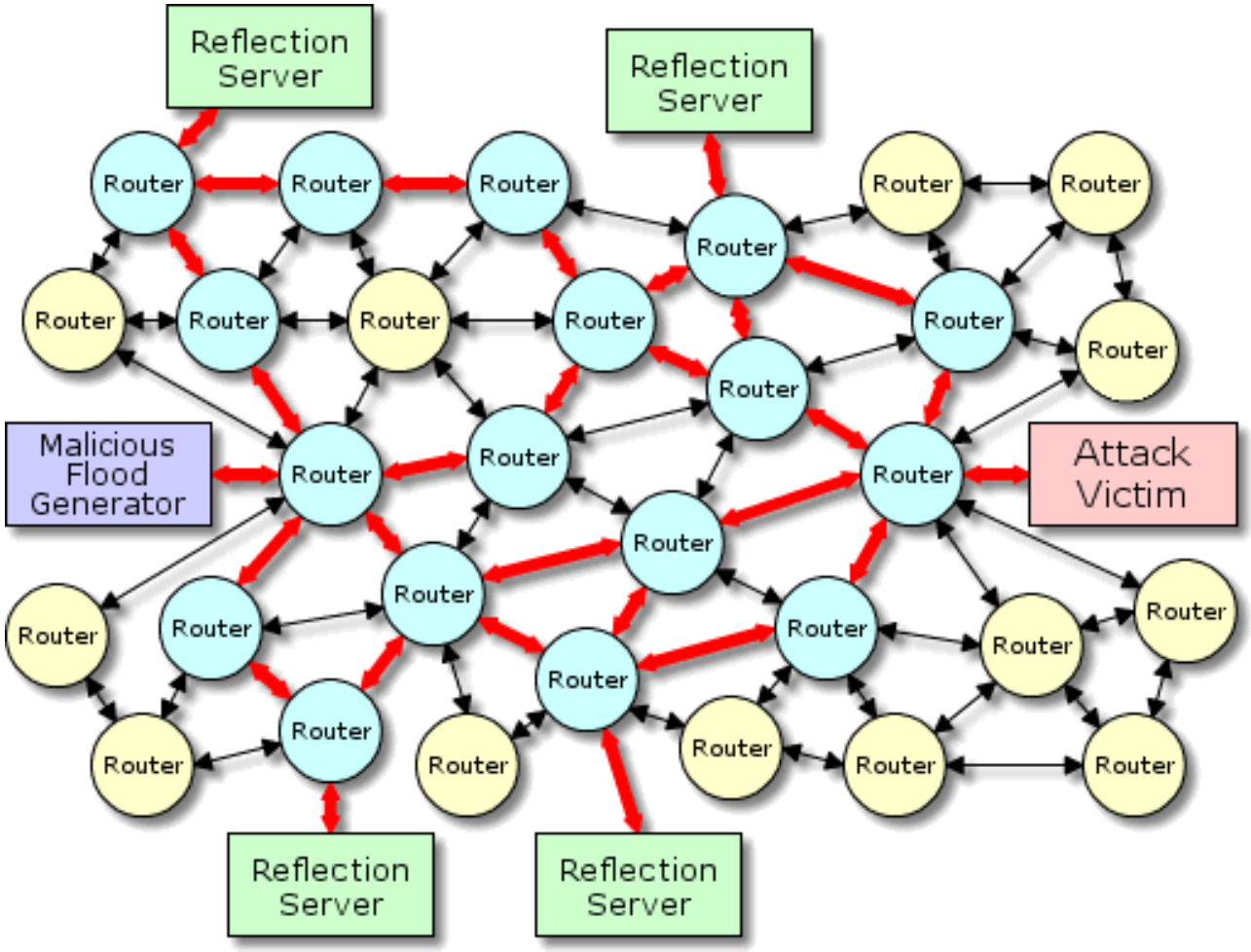
Fraggle

- 假造來源，發送 udp 封包至Broadcast Address
  - port 7 (echo)
  - port 19 (chargen)
- 該網段所有機器將會回應UDP封包至欲攻擊目標，而使網路癱瘓
- 注意 –
  - 目前 Firewall 皆可攔截
  - Internet 上多數Router皆已不轉發目標為Broadcast Address之封包 (no ip directed-broadcast)
  - 關閉該 UDP 服務

Smurf

- 假造來源，發送 icmp echo-request封包至 Broadcast Address
- 該網段所有機器將會回應icmp echo-reply封包至欲攻擊目標，而使網路癱瘓
- 注意 –
  - 目前 Firewall 皆可攔截
  - Internet 上多數Router皆已不轉發目標為Broadcast Address之封包 (no ip directed-broadcast)
  - 目前Windows 已改為不回應 ICMP Broadcast 封包
  - Linux 調過參數後亦可不回應 (net.ipv4.icmp_echo_ignore_broadcasts)

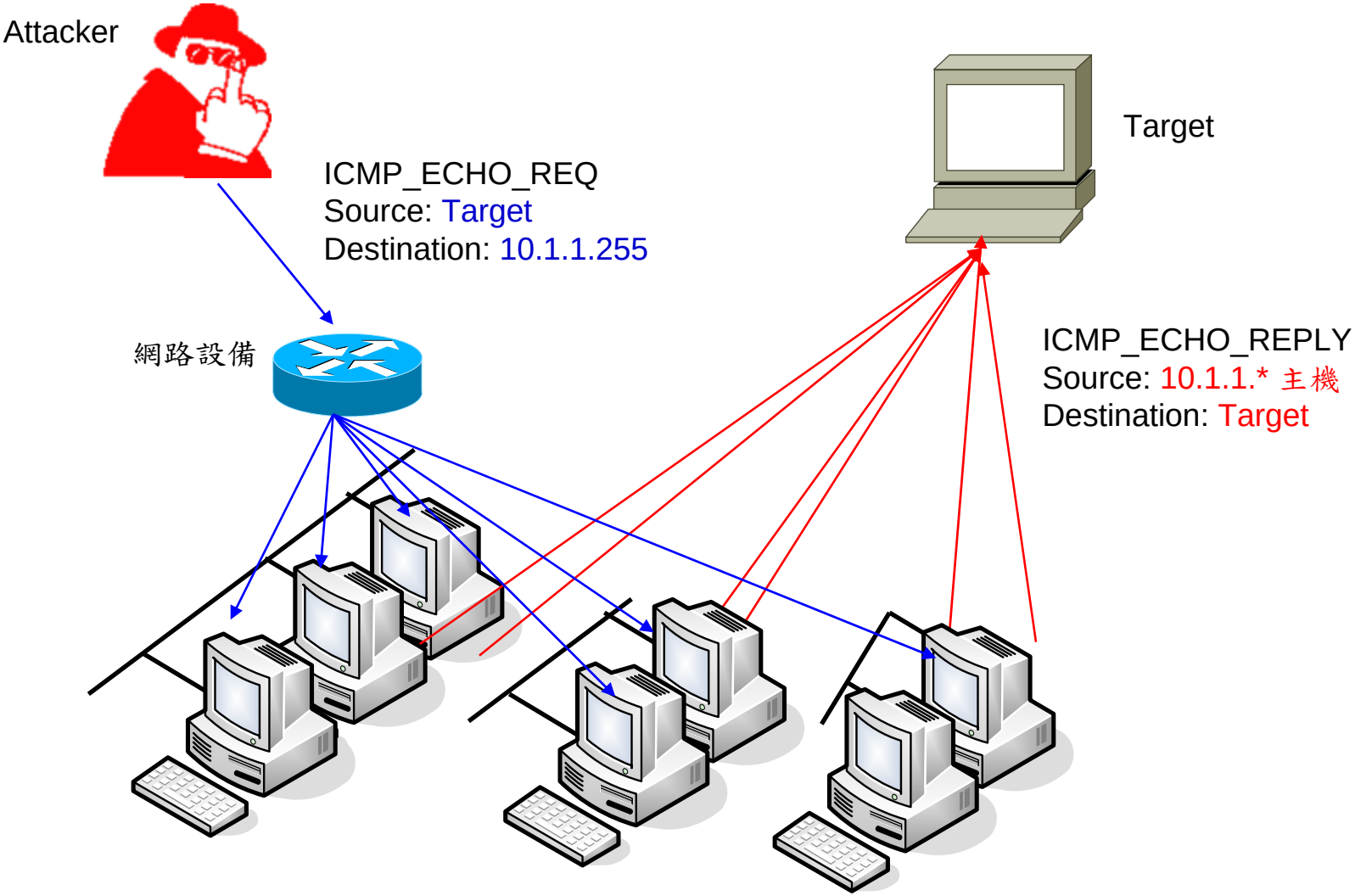
Distributed Reflection DoS



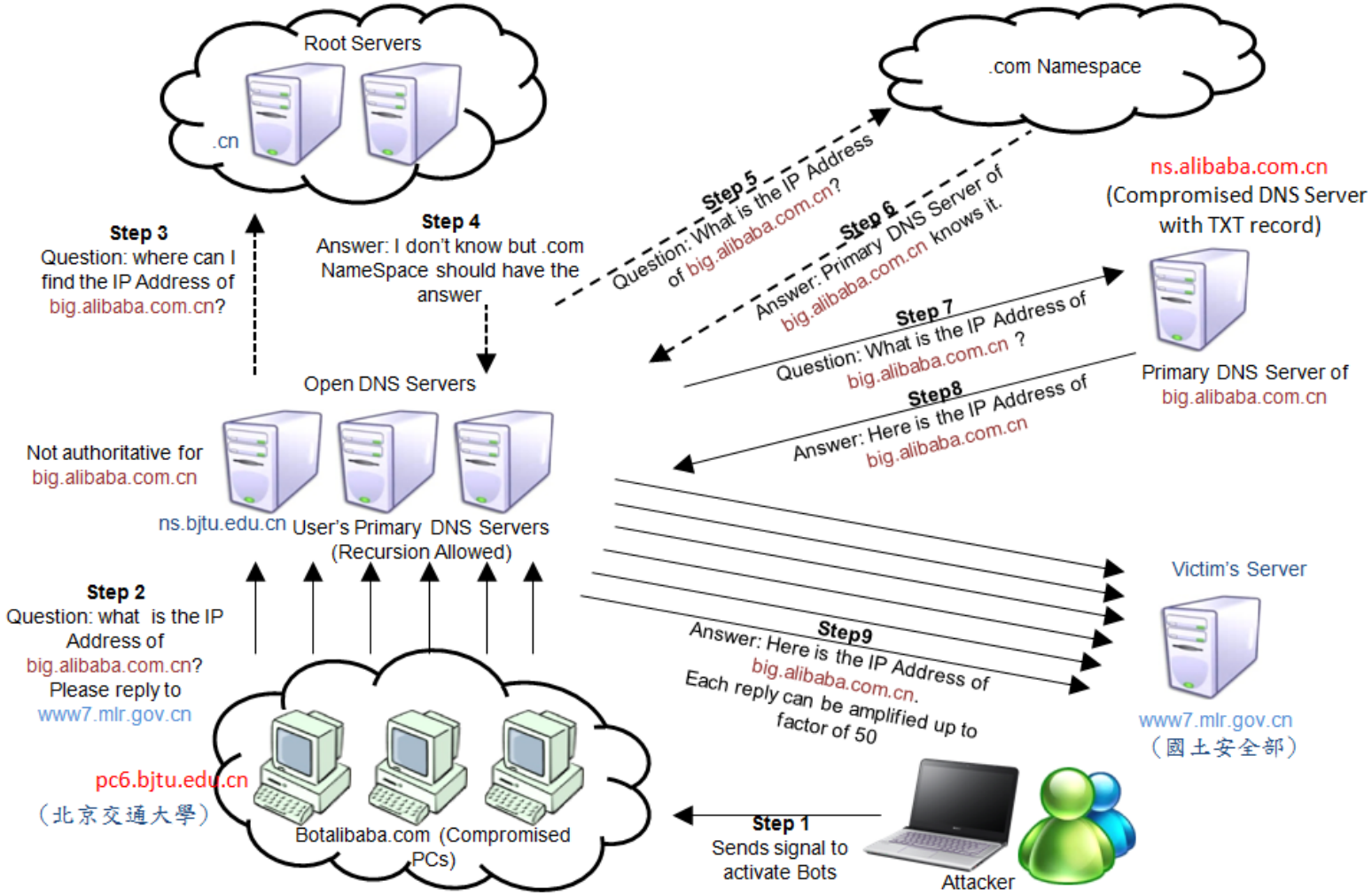
最早被利用是駭客發現網際網路上的路由器幾乎都開放BGP 179埠

偽造受害者IP送去SYN後，讓路由器回應SYN/ACK給受害者

Smurf 示意圖

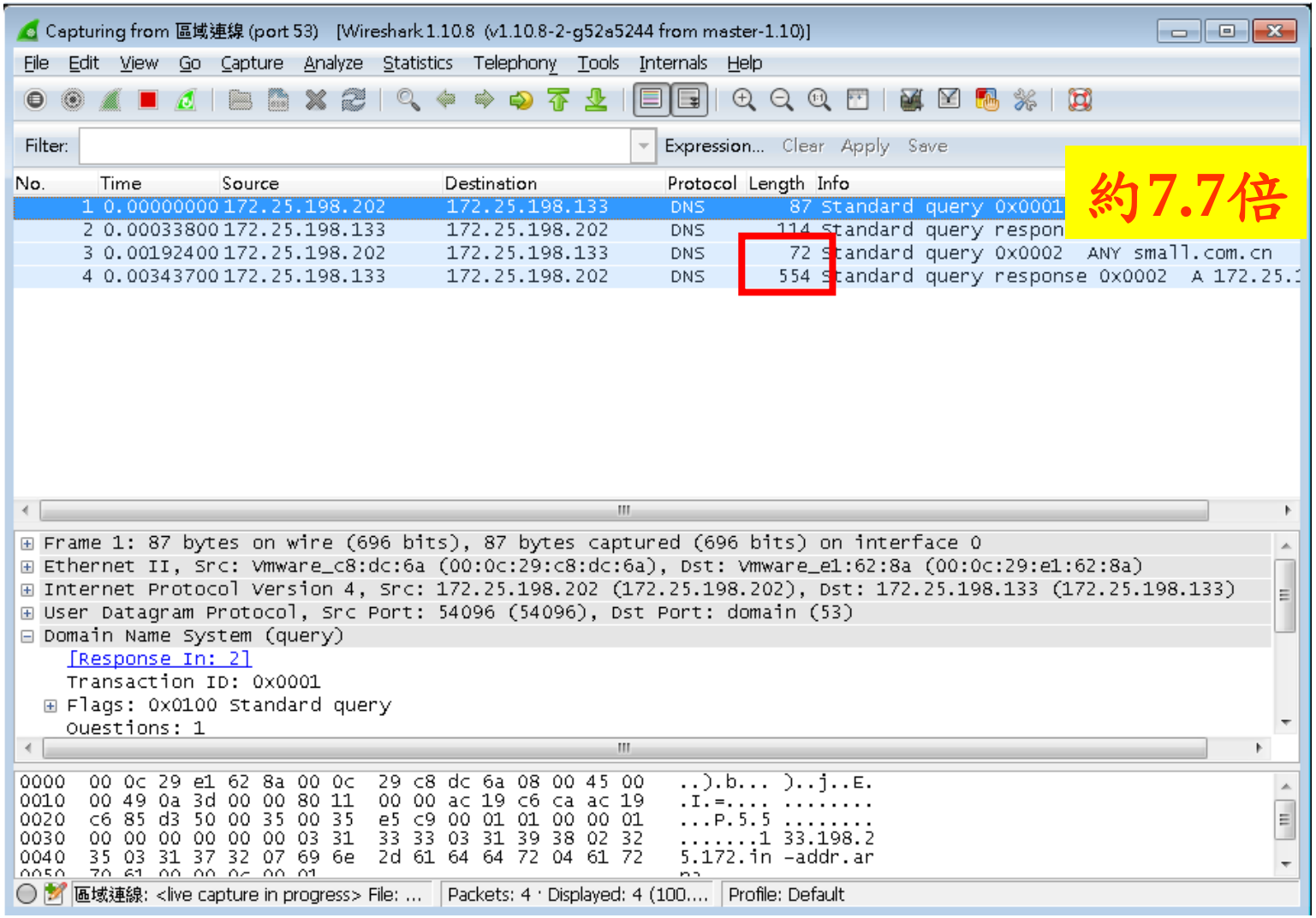

Attacker
Target
ICMP_ECHO_REQ
Source: Target
Destination: 10.1.1.255
網路設備
ICMP_ECHO_REPLY
Source: 10.1.1.* 主機
Destination: Target

最常使用 DNS與NTP




00:00:42.847373 IP 140.113.114.1.32799 > 182.140.167.189.53: 33735 A? cdyhcdcv.www.game776.com. (42)
00:00:42.847388 IP 140.113.114.1.32799 > 182.140.167.189.53: 46431 A? cdyhcdcv.www.game776.com. (42)
00:00:44.022380 IP 140.113.114.1.32799 > 180.153.162.150.53: 27987 A? olwnwbenktwvul.www.game776.com. (48)
00:00:44.022398 IP 140.113.114.1.32799 > 180.153.162.150.53: 16001 A? olwnwbenktwvul.www.game776.com. (48)
00:00:44.022432 IP 140.113.114.1.32799 > 182.140.167.166.53: 58339 A? mraf.www.game776.com. (38)
00:00:44.022442 IP 140.113.114.1.32799 > 182.140.167.166.53: 579 A? mraf.www.game776.com. (38)
00:00:44.022502 IP 140.113.114.1.32799 > 182.140.167.166.53: 50210 A? elabct.www.game776.com. (40)
00:00:44.022503 IP 140.113.114.1.32799 > 182.140.167.189.53: 59774 A? grwfupgzwtmb.www.game776.com. (46)
00:00:44.022515 IP 140.113.114.1.32799 > 182.140.167.166.53: 2966 A? elabct.www.game776.com. (40)
00:00:44.022515 IP 140.113.114.1.32799 > 182.140.167.189.53: 522 A? grwfupgzwtmb.www.game776.com. (46)
00:00:44.022555 IP 140.113.114.1.32799 > 182.140.167.189.53: 33715 A? chargtabgpcjyrgr.www.game776.com. (50)
00:00:44.022557 IP 140.113.114.1.32799 > 182.140.167.189.53: 39252 A? clkvejijqbmxozcx.www.game776.com. (50)
00:00:44.022571 IP 140.113.114.1.32799 > 182.140.167.189.53: 4954 A? chargtabgpcjyrgr.www.game776.com. (50)
00:00:44.022572 IP 140.113.114.1.32799 > 182.140.167.189.53: 37047 A? clkvejijqbmxozcx.www.game776.com. (50)
00:00:44.023270 IP 140.113.114.1.32799 > 182.140.167.166.53: 47666 A? chuxohah.www.game776.com. (42)
00:00:44.023280 IP 140.113.114.1.32799 > 182.140.167.166.53: 7365 A? chuxohah.www.game776.com. (42)
00:00:44.023340 IP 140.113.114.1.32799 > 182.140.167.166.53: 1007 A? itujqrmdylupkt.www.game776.com. (48)
00:00:44.023341 IP 140.113.114.1.32799 > 182.140.167.166.53: 61675 A? knkvctmx.www.game776.com. (42)
00:00:44.023352 IP 140.113.114.1.32799 > 182.140.167.166.53: 38398 A? itujqrmdylupkt.www.game776.com. (48)
00:00:44.023353 IP 140.113.114.1.32799 > 182.140.167.166.53: 17491 A? knkvctmx.www.game776.com. (42)
00:00:44.023409 IP 140.113.114.1.32799 > 182.140.167.166.53: 39355 A? gnalwvoruhyd.www.game776.com. (46)
00:00:44.023419
00:00:44.023480
00:00:44.023480
00:00:44.023497
00:00:44.023497 IP 140.113.114.1.32799 > 180.153.162.150.53: 53616 A? yripszkpwp.www.game776.com. (44)
短時間大量詢問不存在網域

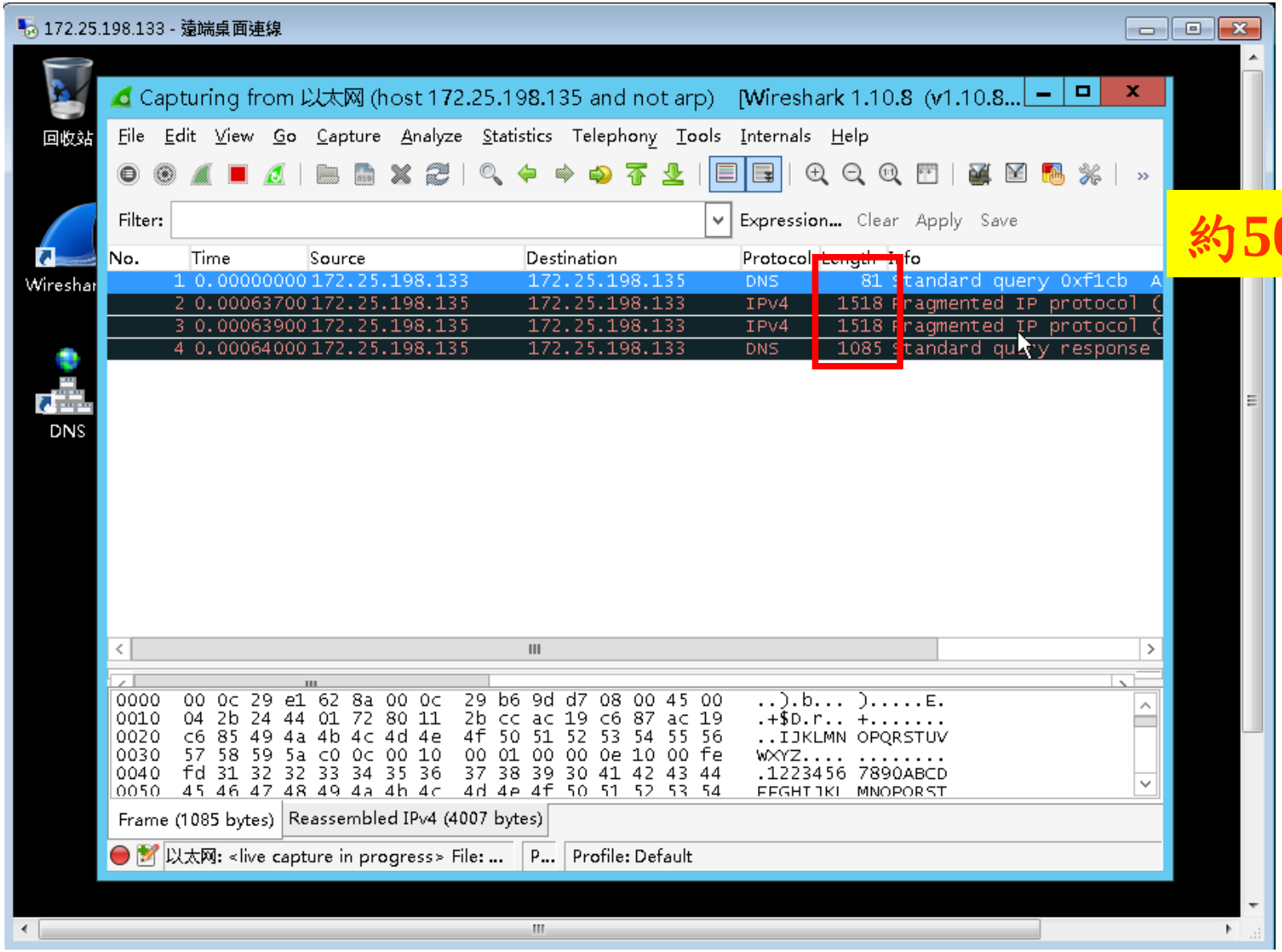
傳統DNS放大率


Capturing from 區域連線 (port 53) [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.00000000 172.25.198.202 172.25.198.133 DNS 87 Standard query 0x0001
2 0.00033800 172.25.198.133 172.25.198.202 DNS 114 Standard query respon
3 0.00192400 172.25.198.202 172.25.198.133 DNS 72 Standard query 0x0002 ANY small.com.cn
4 0.00343700 172.25.198.133 172.25.198.202 DNS 554 Standard query response 0x0002 A 172.25.
約7.7倍
Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
Ethernet II, Src: Vmware_c8:dc:6a (00:0c:29:c8:dc:6a), Dst: Vmware_e1:62:8a (00:0c:29:e1:62:8a)
Internet Protocol Version 4, Src: 172.25.198.202 (172.25.198.202), Dst: 172.25.198.133 (172.25.198.133)
User Datagram Protocol, Src Port: 54096 (54096), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x0001
Flags: 0x0100 Standard query
Questions: 1
0000 00 0c 29 e1 62 8a 00 0c 29 c8 dc 6a 08 00 45 00 ..).b...)..j..E.
0010 00 49 0a 3d 00 00 80 11 00 00 ac 19 c6 ca ac 19 .I.=.... ....
0020 c6 85 d3 50 00 35 00 35 e5 c9 00 01 01 00 00 01 ...P.5.5 ....
0030 00 00 00 00 00 00 03 31 33 33 03 31 39 38 02 32 ....1 33.198.2
0040 35 03 31 37 32 07 69 6e 2d 61 64 64 72 04 61 72 5.172.in -addr.ar
區域連線: <live capture in progress> File: ...
Packets: 4 · Displayed: 4 (100....
Profile: Default

EDNS0

- 傳統 DNS UDP 封包回應限制 512 bytes
- DNSSEC 需要納入數位簽章，因此需要採用 EDNS0，將 UDP 封包上限擴展到 4,096 bytes。
- 通常使用TXT Record填入，利用query ANY攻擊

EDNS0放大率



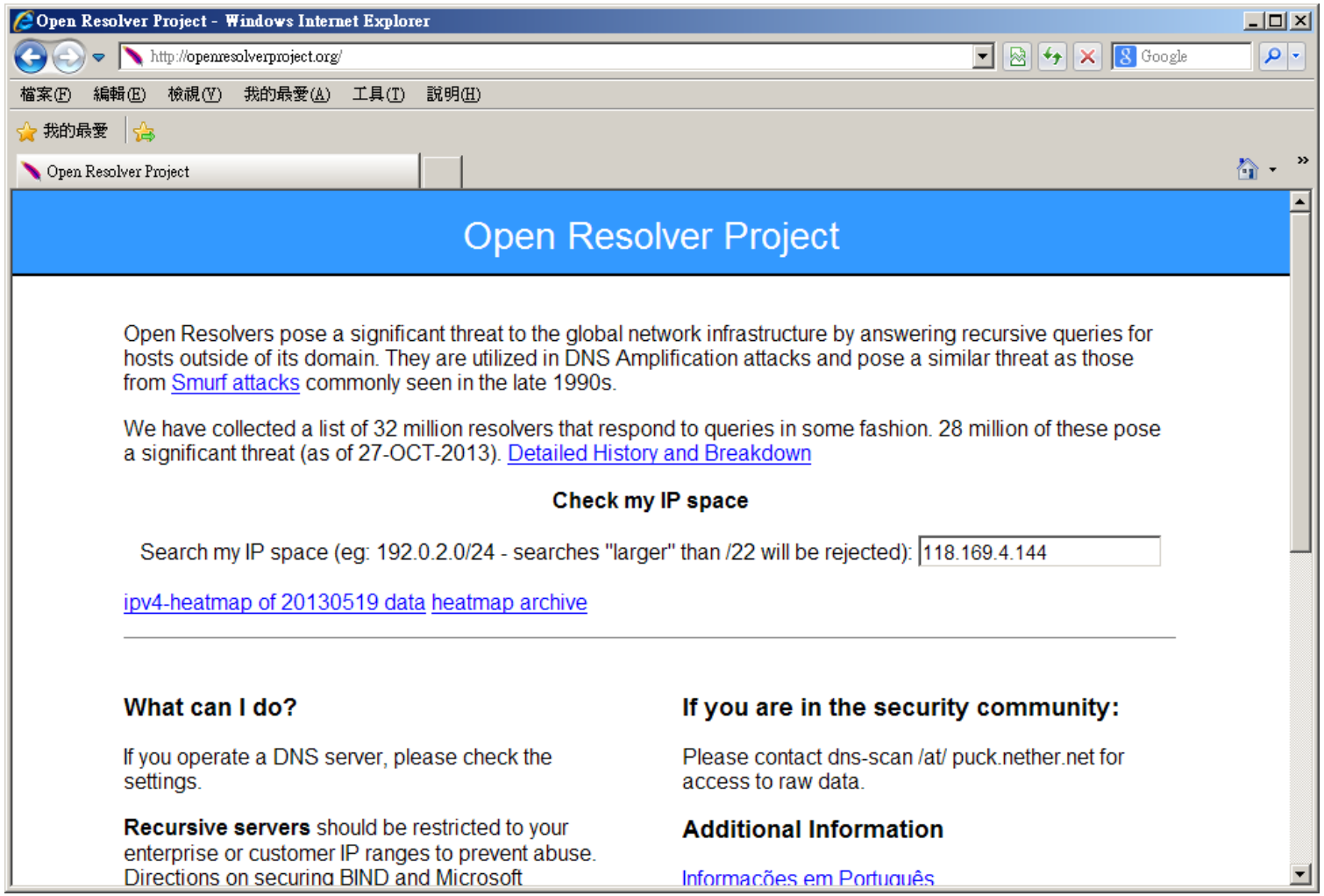
約50.9倍

DNS攻擊事件-ANY 放大攻擊

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31697
;; flags: qr rd ra; QUERY: 1, ANSWER: 11, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;wradish.com.                   IN      ANY

;; ANSWER SECTION:
wradish.com.            3053    IN      SOA     ns19.domaincontrol.com. dns.jomax.net. 2014042218 28800 7200 604800 600
wradish.com.            53      IN      A       50.63.202.55
wradish.com.            3053    IN      MX      0 smtp.secureserver.net.
wradish.com.            3053    IN      MX      10 mailstore1.secureserver.net.
wradish.com.            3053    IN      NS      ns19.domaincontrol.com.
wradish.com.            3053    IN      NS      ns20.domaincontrol.com.
wradish.com.            3053    IN      TXT     "test test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststt
est test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test tests" "ttest test teststtest test teststtest test testst
test test teststtest test teststtest test teststtest test teststtest test teststtest test test test teststtest test teststtest test teststtest test teststtest test teststtest tes
t teststtest test teststtest" " test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest te
st teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtes" "t test teststtest test test test teststtest test teststtest test te
ststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test test
sttest tes" "t te"
wradish.com.            3053    IN      TXT     "asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfas
dfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf " "asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasd
f asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf"
wradish.com.            3053    IN      TXT     "tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyy
yy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy ttttttttttttt" "yyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyy
yyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyy
y tttttttttttttyyyyyyyy tttt" "tttttttttyyyyyyyy tttttttttttttyyyyyyyy tttttttttttttyyyyyyyy"
wradish.com.            3053    IN      TXT     "hkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsd
fhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfh" "alsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfas
dfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasd
hfasdfhalsdfhkhkhaksdfhasdhf" "asdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhak
sdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfh" "asdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdf
hkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfhalsdfhkhkhaksdfhasdhfasdfha
lsdf"
wradish.com.            3053    IN      TXT     "asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer2
34234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 as" "dfasfwerwer234234234 asdfasfwerwer234234234 asdfa
sfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234 asdfasfwerwer234234234
"

;; Query time: 22 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Nov 25 12:03:35 2014
;; MSG SIZE  rcvd: 3798

1-167-189-114 :: ~ »
```

DNS 回應 3798 Bytes

Open Resolver Project



DrDOS 使用 NTP

```
06:44:26.741649 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
06:44:26.741678 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
06:44:26.741738 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
06:44:26.741751 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
06:44:26.741763 IP x.x.x.x.123 > x.x.x.x.80: NTPv2, Reserved, length 440
```

Figure 19: Traffic snippet of an NTP attack that targeted a security company

	SJC	LON	HKG	DCA
Peak bits per second (bps)	35.00 Gbps	**80.00 Gbps**	**26.00 Gbps**	**55.00 Gbps**
Peak packets per second (pps)	9.00 Mpps	**19.00 Mpps**	**7.00 Mpps**	**15.00 Mpps**

Figure 20: Attack metrics from each of four scrubbing center location for the attack against a security company

DrDOS UDP 放大比率

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

https://www.us-cert.gov/ncas/alerts/TA14-017A

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

How to Exploit BitTorrent for···

thehackernews.com/2015/08/bittorrent-dos-attack.html

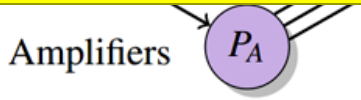
搜尋

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

How to Exploit BitTorrent for Large-Scale DoS Attacks

Sunday, August 16, 2015 Mohit Kumar

BitTorrent
下載電影變跳版
(50~120倍)



BitTorrent Can Be Exploited for DoS Attacks

A flaw discovered in several widely used BitTorrent applications, including ***uTorrent***, ***Vuze*** and ***Mainline***, could be used to carry out a devastating distributed denial of service (DDoS) attack that makes it very easy for a single undetectable hacker to bring down large sites.

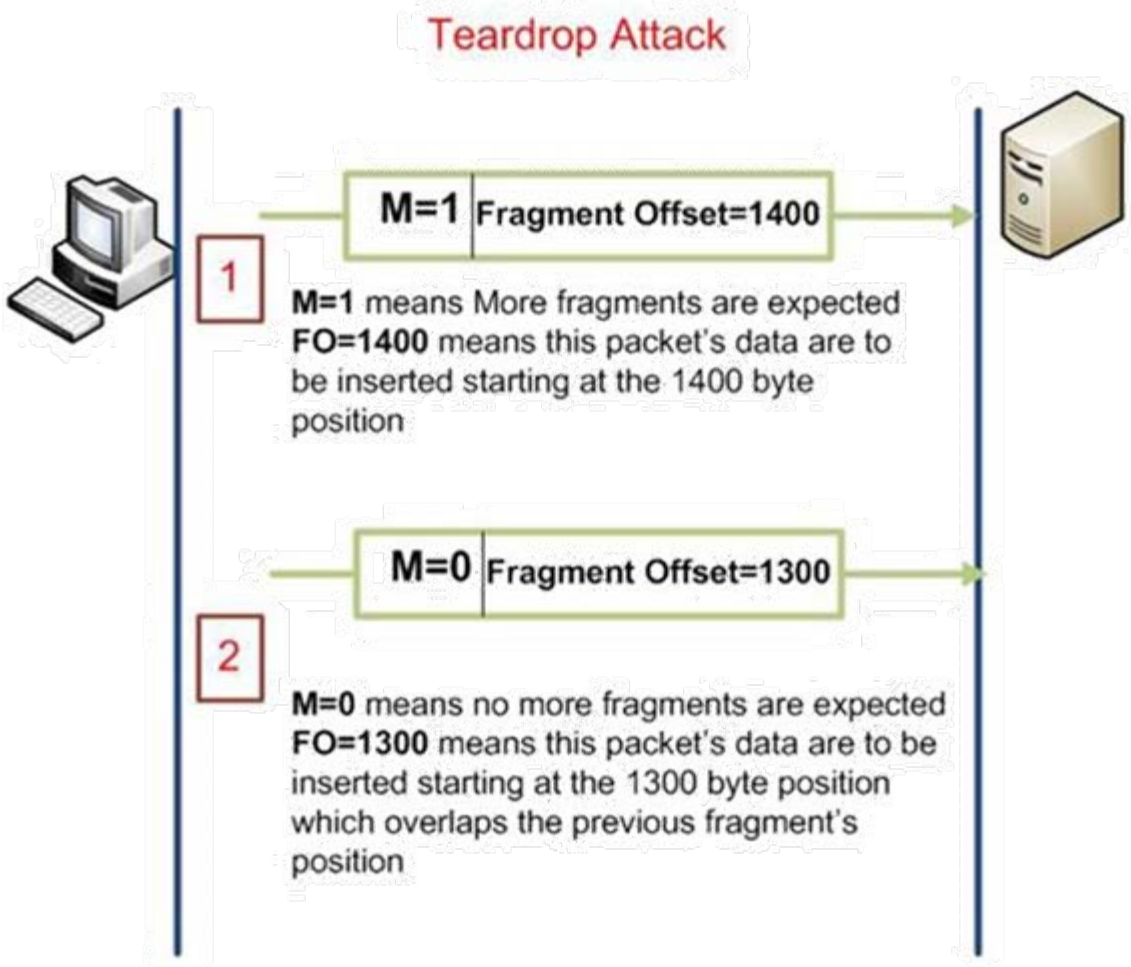
DoS的攻擊目標

- 破壞目標實體設備
- 癱瘓目標服務網路
  - 頻寬消耗(Bandwidth Depletion)
  - 干擾連線 (Disrupt connection)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者

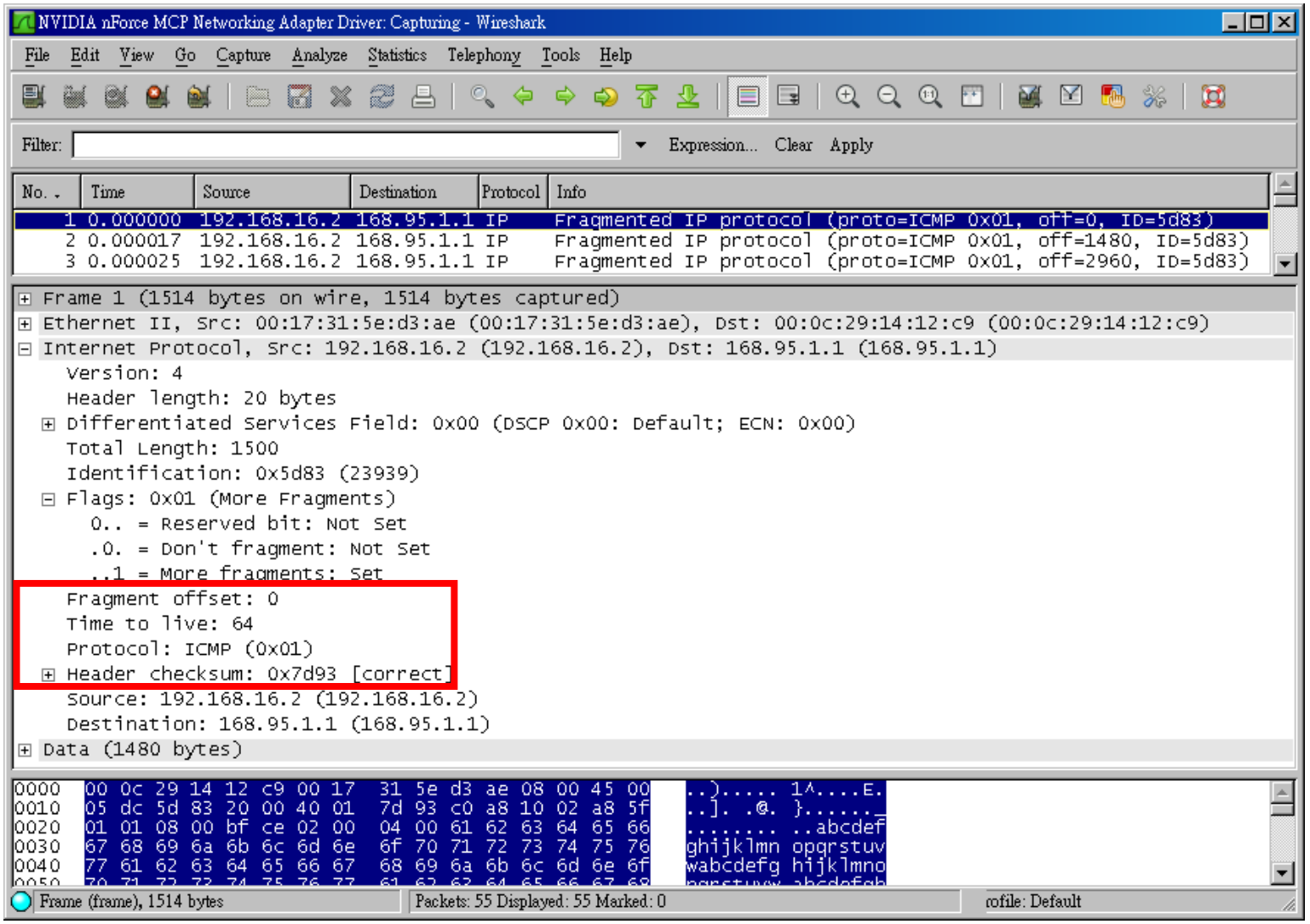
Teardrop

- 利用製造含重疊區段的 TCP 封包，使目標主機因重組封包的bug而Crash
- 目前 Firewall 皆可攔截、即使進到Server亦不受影響
- 影響平台
  - Windows 3.1、95、NT
  - Linux kernel < 2.0.32、2.1.63

Teardrop 示意圖



Fragment Flags



Land

- 發出 Source/Destination IP 皆為目標機的 TCP SYN 封包，使目標機因不斷自我回應而導致Crash
- 目前 Firewall 皆可攔截、即使進到Server亦不受影響
- 影響平台
  - AIX 3
  - FreeBSD 2.2.5
  - IRIX 5.3
  - NetBSD 1.3
  - SunOS 4.1.4
  - Windows 95、NT

Ping of Death

- 發送長度超過 65535 bytes 之 ping 封包
- 經過各router時，由於超過MTU，封包被切割傳遞
- 傳至目標機，進行封包重組時，由於超過了單一封包的長度限制，而導致Crash
- 約 1997-1998 年間，所有的OS皆已修正
- 目前 Firewall 皆可攔截、即使進到Server亦不受影響

Apache Killer 測試方法

- 送出不正常的 Range Request

```
GET / HTTP/1.0
Host: default
Accept-Encoding: gzip
Range: bytes=0-,5-0
```

- 若伺服器回應 206 Partial Content，則代表”可能”存在此弱點
- 經 Patch 過之伺服器應回應 200 OK
- 利用系統弱點造成資源耗盡

ApacheKiller

- 攻擊方法
  - http://www.hackersgarage.com/apache-killer-denial-of-service-flaw-in-apache-webserver.html
- 防禦方法討論串
  - http://marc.info/?l=apache-httpd-dev&m=131418828705324&w=2
- 目前 Apache 官方已修正此弱點，需更新至 2.2.21

IIS HTTP.sys攻擊

微軟IIS驚爆HTTP.sys死亡漏洞，一Ping系統恐癱瘓， SANS警告駭客正大肆搜尋肉票伺服器

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
69832 CVE

National Cyber Awareness System

Vulnerability Summary for CVE-2015-1635

Original release date: 04/14/2015

Last revised: 04/15/2015

Source: US-CERT/NIST

Overview

HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability."

Impact

CVSS Severity (version 2.0):

CVSS v2 Bas

Impact Subs

Exploitability

CVSS Versio

2014/12 – 發現並通報

(半年過去...)

2015/05 – 微軟發布安全更新

MS15-034 /CVE-2015-1635

- 針對Microsoft IIS 7.5 64 bits的png檔案送出特定Range標頭後，會造成系統崩潰
- 範例
  - Range: bytes=24688-18446744073709551615
  - 紅字範圍填入4294967296到18446744073709551615間的數字都會當機，亦即2^32~2^64-1
  - 推測為64 bits系統對png的handler延用了32bits版本的程式
  - 為未公開弱點
- 2014/12 – 微軟/Citrix發現
- 2015/05 – 微軟發布安全更新

DoS的攻擊目標

- 破壞目標實體設備
- 癱瘓目標服務網路
  - 頻寬消耗(Bandwidth Depletion)
  - 干擾連線 (Disrupt connection)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者

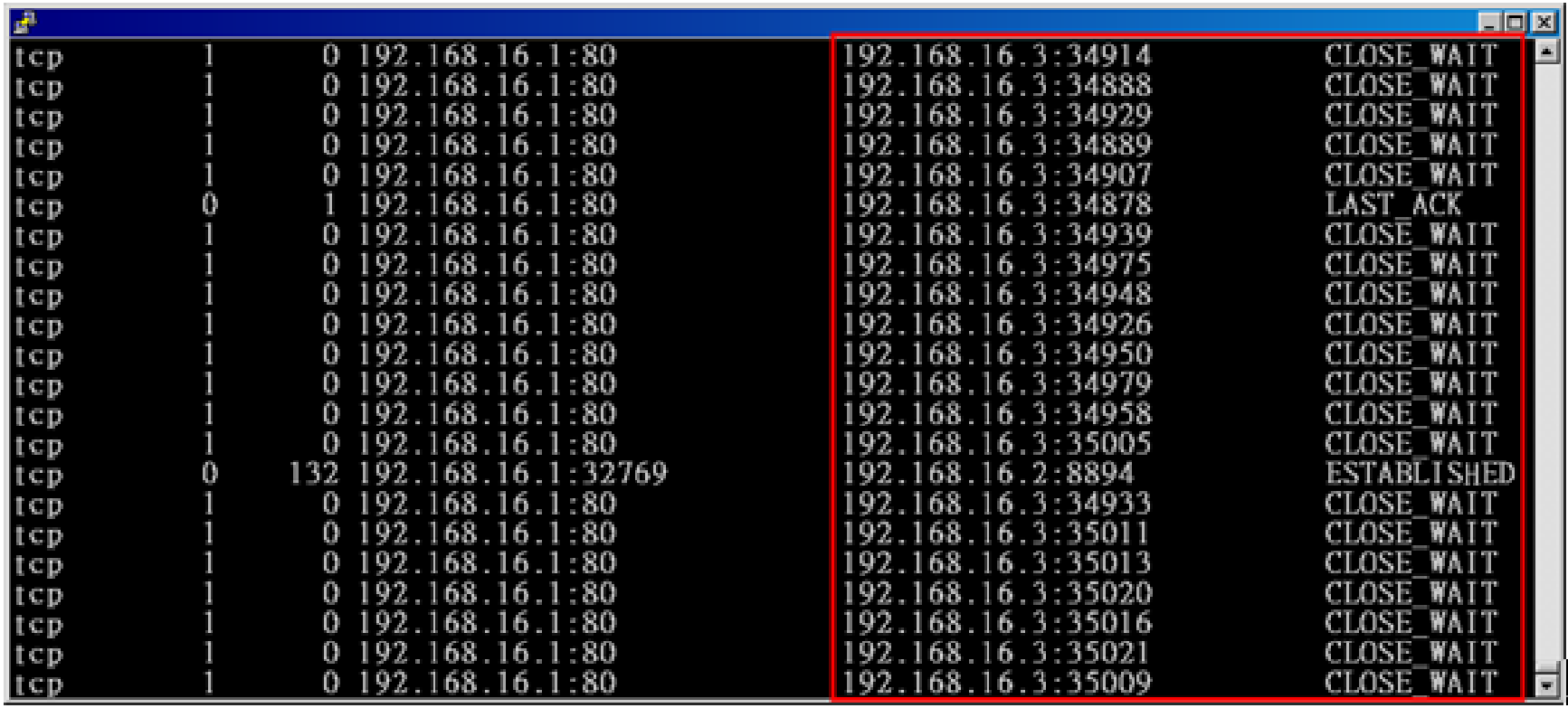
不同層級資源消耗

- 網路層級
  - TCP Connect Flood
  - Zombie Connection
- 應用層
  - SSL Flood
  - HTTP Flood
  - Application Flood

TCP Connect Flood

- 以大量之攻擊來源，與目標服務不斷重覆建立TCP連線、切斷連線、建立連線、切斷連線……等動作
- 網路設備/主機 將因虛耗許多資源於連線之處理，而使負荷升高、服務緩慢
- 阻擋方式 –
  - Firewall/IPS – 限制服務之 Connection Per Second
  - 縮短 timeout 時間
  - 定時抓出超出CPS之來源阻擋
  - 以效能較好之 Proxy/L4 設備代替主機建立連線

攻擊結果

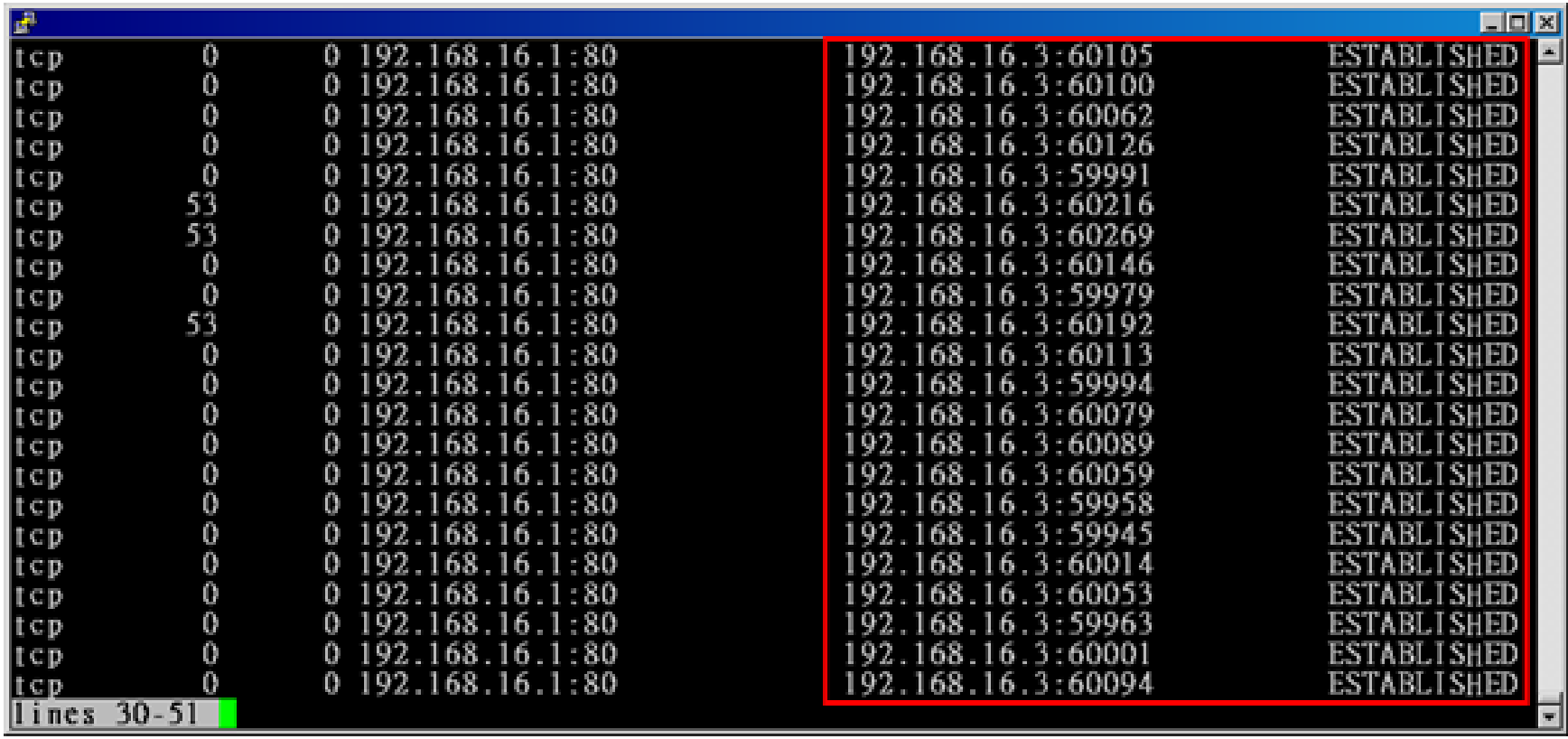


tcp	1	0	192.168.16.1:80	192.168.16.3:34914	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34888	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34929	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34889	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34907	CLOSE_WAIT
tcp	0	1	192.168.16.1:80	192.168.16.3:34878	LAST_ACK
tcp	1	0	192.168.16.1:80	192.168.16.3:34939	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34975	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34948	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34926	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34950	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34979	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:34958	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:35005	CLOSE_WAIT
tcp	0	132	192.168.16.1:32769	192.168.16.2:8894	ESTABLISHED
tcp	1	0	192.168.16.1:80	192.168.16.3:34933	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:35011	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:35013	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:35020	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:35016	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:35021	CLOSE_WAIT
tcp	1	0	192.168.16.1:80	192.168.16.3:35009	CLOSE_WAIT

Zombie Connections

- 以大量之攻擊來源，與目標建立 TCP 連線，並定時發送封包保持連線不切斷
- 網路設備/主機 將因 Session Table 被建滿而導致負荷升高、無法服務
- 阻擋方式 –
  - Firewall/IPS – 限制同一 IP 之可連線數
  - 縮短 idle timeout 時間
  - 定時抓出建立過多連線的來源直接阻擋
  - 以效能較好之 Proxy/L4 設備代替主機建立連線

攻擊結果

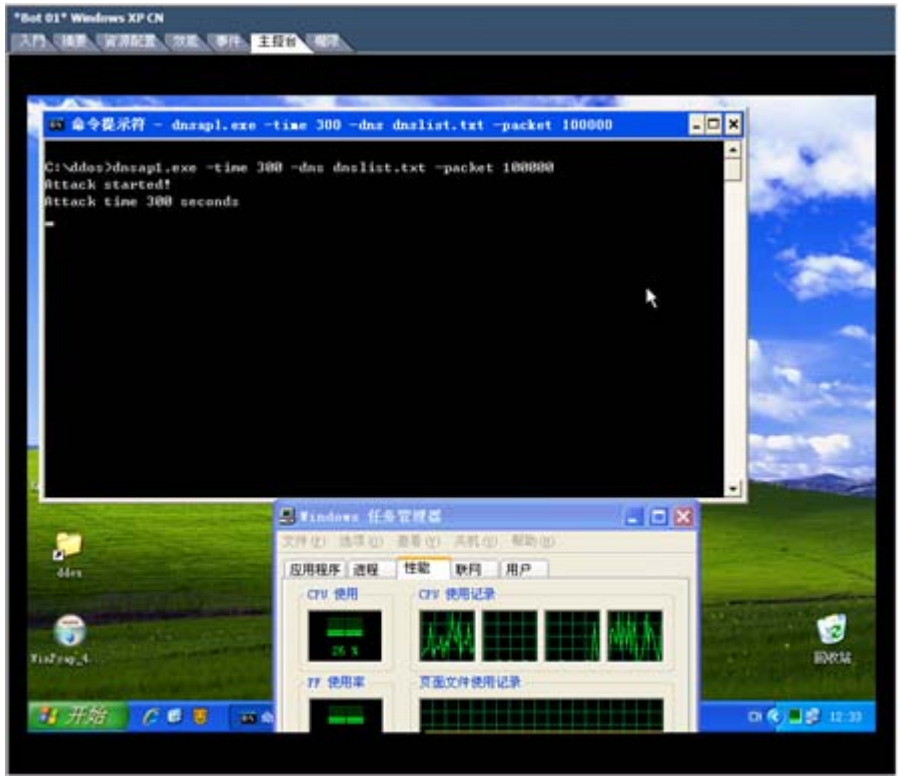


```
tcp        0      0 192.168.16.1:80         192.168.16.3:60105      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60100      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60062      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60126      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:59991      ESTABLISHED
tcp       53      0 192.168.16.1:80         192.168.16.3:60216      ESTABLISHED
tcp       53      0 192.168.16.1:80         192.168.16.3:60269      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60146      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:59979      ESTABLISHED
tcp       53      0 192.168.16.1:80         192.168.16.3:60192      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60113      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:59994      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60079      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60089      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60059      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:59958      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:59945      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60014      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60053      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:59963      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60001      ESTABLISHED
tcp        0      0 192.168.16.1:80         192.168.16.3:60094      ESTABLISHED
lines 30-51
```

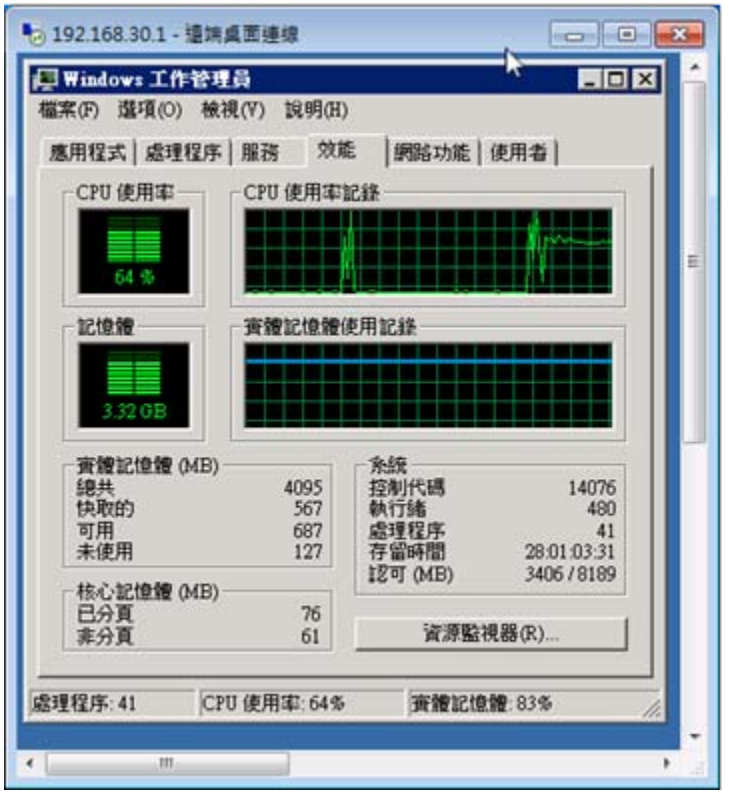
DNS Query Flood

- 快速並大量DNS查詢，攻擊者主機資源消耗輕微，但造成目標主機資源消耗嚴重

Attacker



Victim



Application Flood

- 以大量之攻擊來源，對目標不斷進行應用層之正常行為
- 主機將因不斷處理過量之請求而導致負荷升高、無法服務
- 常見攻擊方式
  - SSL Flood
  - HTTP Flood
  - DNS Flood
  - LOGIN/DB_QUERY Flood

HTTP DoS

- GET with unended request
  - ex: Slowloris
- POST with unreached body
  - ex: OWASP HTTP Post Tool
- HTTP Flood
- CC攻擊
  - Proxy
  - iframe

正常的 HTTP GET

```
GET / HTTP/1.1[\r\n]
Accept: */*[\r\n]
Accept-Language: zh-tw[\r\n]
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1) [\r\n]
Accept-Encoding: gzip, deflate[\r\n]
Host: www.google.com.tw[\r\n]
Connection: Keep-Alive[\r\n]
[\r\n]
```

- 連續兩CRLF後視為請求結束

Slow HTTP GET

- 一個正常完整的HTTP Get Request結尾為連續兩組換行符號CRLF [\r\n]，未收到連續兩組CRLF之前，伺服器會視此Request尚未結束，等待後續的要求
- 伺服器均有設定若使用者端過久未傳送資料，將其視為離線而中斷與其連線(IDLE Timeout)。透過不斷送出HTTP Get Request的Header，且不送出連續兩組CRLF，即可佔用伺服器的連線。
- 攻擊時可同時開啟多個Thread，在各Thread連線逾時之前再送新的Header內容來維持連線，佔住伺服器的可用連線。只要連線數大於系統限制(例如Apache的Max Clients設定)，伺服器一直處於等候這些未完成的連線，無法處理新的連線，即可造成DOS。

Slowloris

GET / HTTP/1.1

Host: www.google.com

Connection: keep-alive

User-Agent: Mozilla/5.0

X-a: baaaaaaa

X-a: b

X-a: b

X-a: b

X-a: b

X-a: b

正常的 HTTP POST

POST /accounts/ServiceLoginAuth HTTP/1.1[\r\n]
Host: www.google.com[\r\n]
Content-Length: 38[\r\n]
Connection: Keep-Alive[\r\n]
[\r\n]
Email=http.dos@gmail.com&Passwd=123456[\r\n]

- 需於post body區接收到Content-Length指定的長度

Slow HTTP POST

- 一個正常完整的HTTP POST Request中會利用Content-Length宣告需POST的位元數
- Web Server在Client未傳送完所宣告的長度前，會持續等待，直到：
  - (1)收到POST data長度與Content-length宣告符合，或
  - (2)逾時
- 建立HTTP連線後，緩慢送出POST字元佔用連線，耗盡網頁伺服器的可用連線數

OWASP HTTP Post Tool

POST /post.aspx HTTP/1.1

*Accept: text/html, */**

Accept-Language: en-US

User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36

Accept-Encoding: gzip, deflate

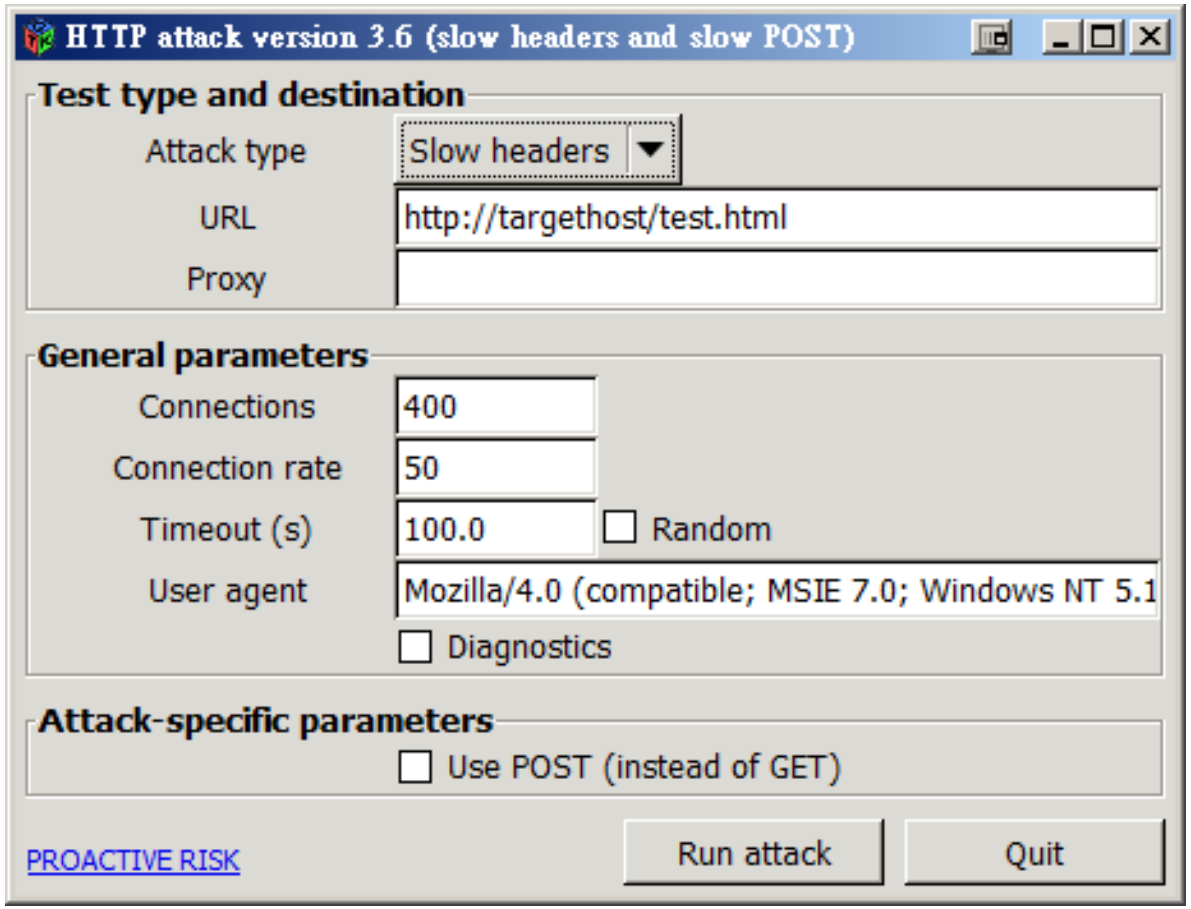
Host: 192.168.37.14

Connection: Close

i(等待)d(等待)= (等待)a (等待) ... ...

OWASP HTTP Post Tool

- https://www.owasp.org/index.php/OWASP_HTTP_Post_Tool



HTTP Flood

- 以大量之攻擊來源，對目標不斷發送 HTTP Request
- 主機將因不斷處理過量之請求而導致負荷升高、無法服務

Evernote DDoS事件

Default Max Connection

- IIS

maxConnections	Optional uint attribute. Specifies the maximum number of connections for a site. Use this setting to limit the number of simultaneous client connections. The default value is 4294967295.

- Apache

MaxClients Directive

Description:	Maximum number of connections that will be processed simultaneously
Syntax:	`MaxClients number`
Default:	`See usage for details`
Context:	server config
Status:	MPM
Module:	beos, leader, prefork, threadpool, worker

The `MaxClients` directive sets the limit on the number of simultaneous requests that will be served. Any connection attempts over the `MaxClients` limit will normally be queued, up to a number based on the `ListenBacklog` directive. Once a child process is freed at the end of a different request, the connection will then be serviced.

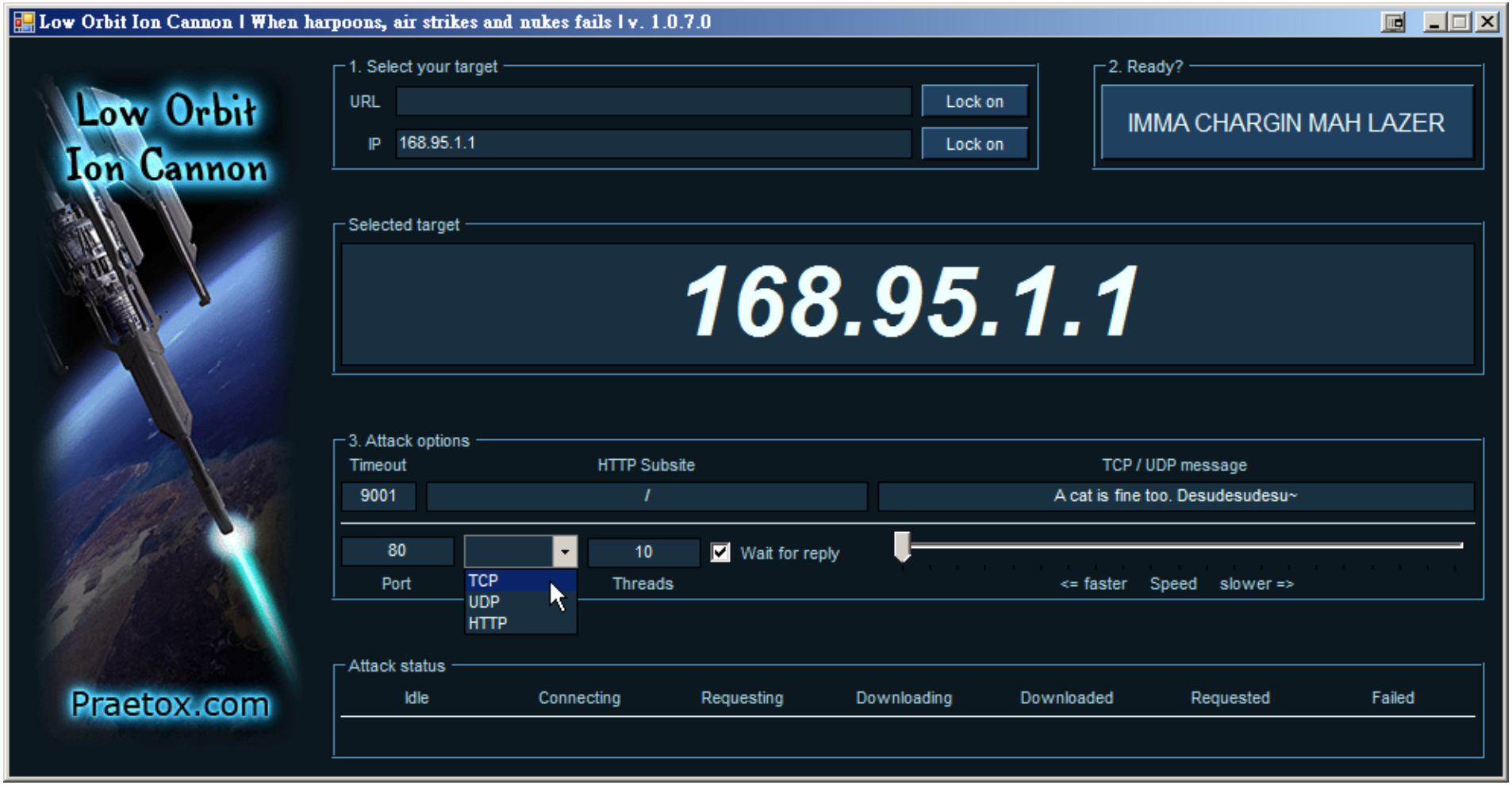
For non-threaded servers (*i.e.*, `prefork`), `MaxClients` translates into the maximum number of child processes that will be launched to serve requests. The default value is 256; to increase it, you must also raise `ServerLimit`.

For threaded and hybrid servers (*e.g.* `beos` or `worker`) `MaxClients` restricts the total number of threads that will be available to serve clients. The default value for `beos` is 50. For hybrid MPMs the default value is 16 (`ServerLimit`) multiplied by the value of 25 (`ThreadsPerChild`). Therefore, to increase `MaxClients` to a value that requires more than 16 processes, you must also raise `ServerLimit`.

HTTP Flood 工具

- ab (Apache Benchmark)
  - http://httpd.apache.org/
- JMeter
  - http://jakarta.apache.org/jmeter/
- Siege
  - http://www.joedog.org/siege/
- Microsoft Web Application Stress Tool
  - http://www.microsoft.com/technet/archive/itsolutions/intranet/downloads/webstres.mspx
- …. Many tools
  - http://www.softwareqatest.com/qatweb1.html

Low Orbit Ion Cannon



H.O.I.C

- 在HTTP GET後方加入隨機變數，混淆防護設備的判斷

JS LOIC

JS LOIC

No need to download, install or setup anything - just click the button, sit and enjoy the show.

Step 1. Select your target:

URL:

http://www.paypal.com/

For current target see: http://anonops.net/

Step 2. Ready?

IMMA CHARGING MAH LAZER

Optional. Options

Requests per second: 10

Append message:

Attack status:

Requested:
0
Succeeded:
0
Failed:
0

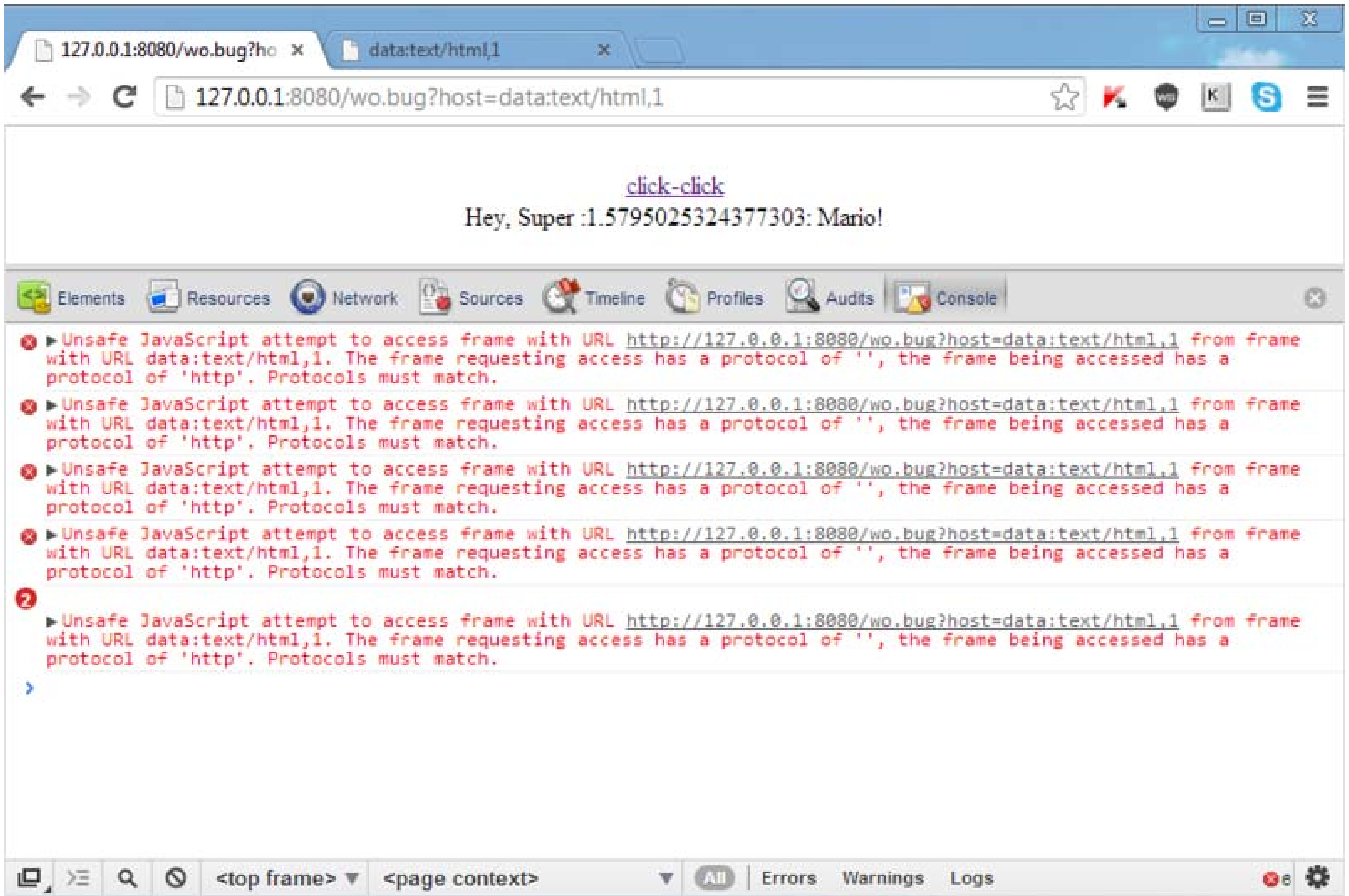
We need your help in support of wikileaks leave this page firing as long as you can. Don't worry if requests show as failed.

活殭屍攻擊


TVBS新聞台
網友串連鍵盤攻擊
菲律賓政府單位官網
分身重複登入
流量爆增
網站當掉
23:08
囚女十年 控嫌4綁架罪 2.4億天價保金硬押

CC 攻擊

- 利用XSS手法將攻擊語法貼到各網站或留言版



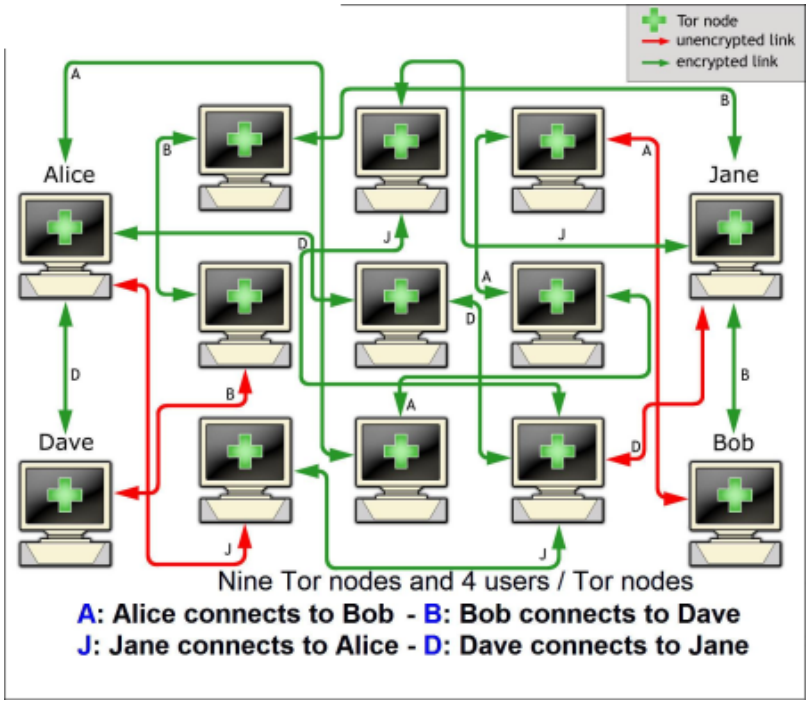
Pingback 遭濫用，16萬WordPress網站淪為DDoS攻擊傀儡

Securi技術長Daniel Cid表示，駭客濫用了Pingback功能，利用至少16.2萬個WordPress網站來癱瘓目標網站。以WordPress架站的使用者，若懷疑自己可能淪為DDoS幫兇，可以檢視網站有否任何XMLRPC檔案的POST請求，倘若當中含有隨機網址的Pingback執行，那麼網站應該已被濫用。

文/ 陳曉莉 | 2014-03-13 發表


AR革命新玩法
我的英雄夢
MY HERO GO
國志
殭屍病毒癱瘓伺服器流程圖
購買殭屍病毒，內含數百萬封電子郵件網址
透過郵件大量撒出
電腦使用者點到病毒後變成殭屍電腦
第三者電腦成中繼站
中毒
駭客可操控所有中毒電腦
連接遊戲網址，使其因流量過大癱瘓
整理：記者楊絳傑

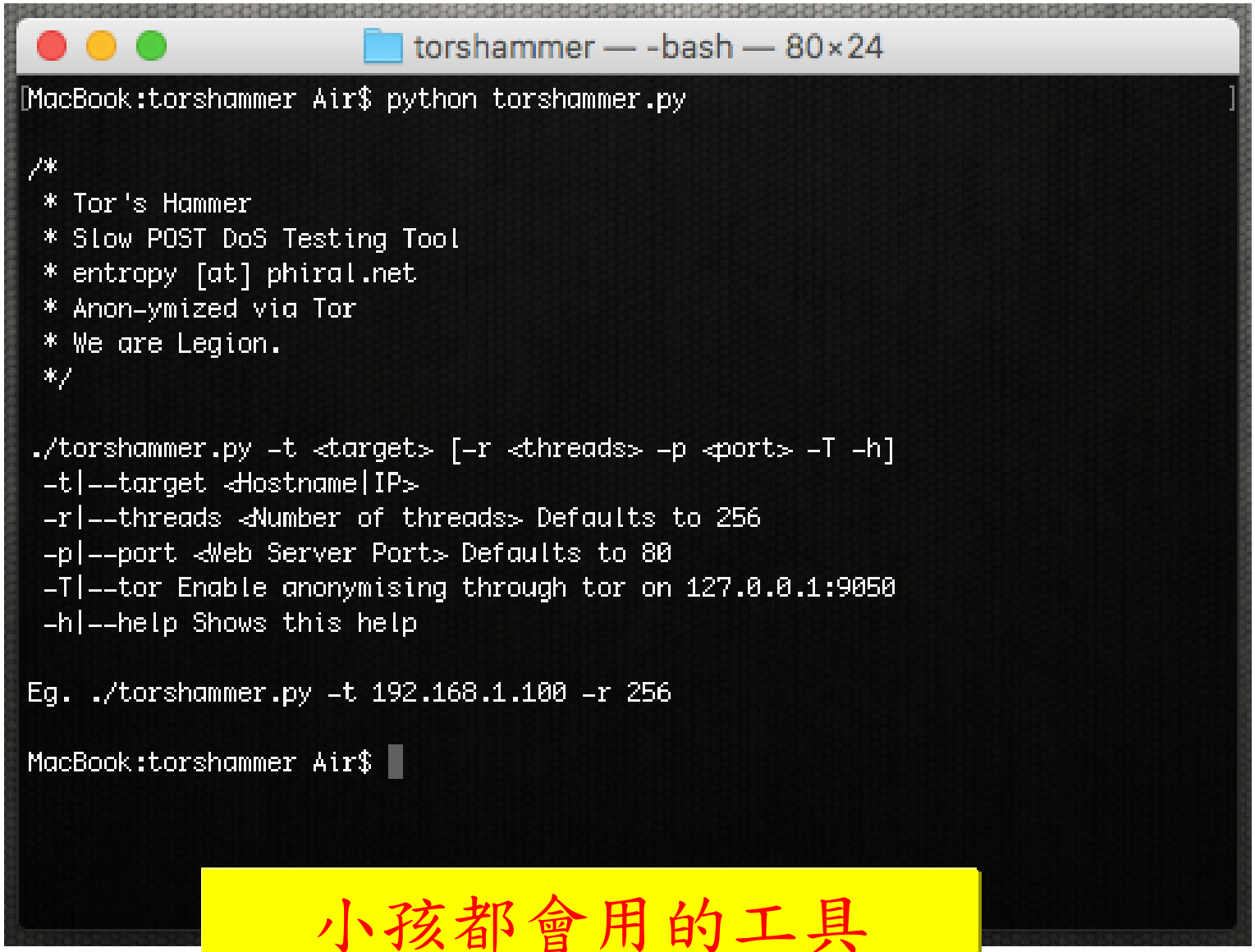
TOR



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。

TOR's Hammer



小孩都會用的工具

SSL Flood

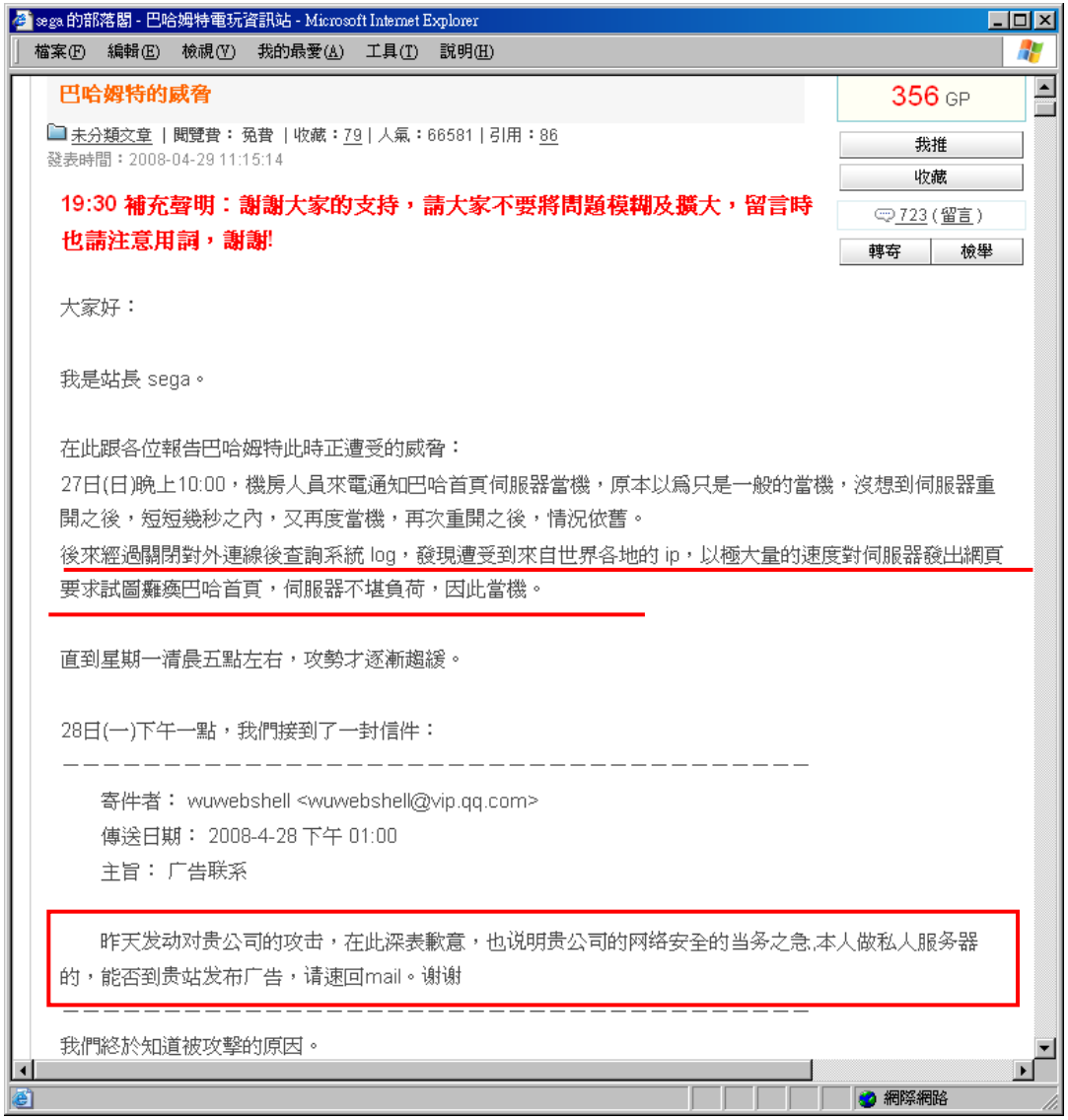
- 以大量之攻擊來源，對目標不斷進行SSL Handshake
- 受攻擊主機將因不斷進行SSL協議交換而導致負荷升高、無法服務

SSL Renegotiation Flood

- SSL協議分為兩層：
  - SSL記錄協議（SSL Record Protocol）：它建立在可靠的傳輸協議（如TCP）之上，為高層協議提供數據封裝、壓縮、加密等基本功能
  - SSL握手協議（SSL Handshake Protocol）：它建立在SSL記錄協議之上，用於在實際的數據傳輸開始前，通訊雙方進行身份認證、協商加密演算法、交換加密密鑰等。
- 在進行negotiation的過程當中，會消耗系統CPU的資源，可利用此特性不斷的與目標Web Server進行SSL negotiation，使目標系統CPU滿載而無法提供服務。
- 範例工具：

  http://www.thc.org/thc-ssl-dos/thc-ssl-dos-1.4.tar.gz

DDoS 勒索



sega 的部落閣 - 巴哈姆特電玩資訊站 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

巴哈姆特的威脅

356 GP

我推 | 收藏 | 723 (留言) | 轉寄 | 檢舉

未分類文章 | 閱覽費：免費 | 收藏：79 | 人氣：66581 | 引用：86

發表時間：2008-04-29 11:15:14

19:30 補充聲明：謝謝大家的支持，請大家不要將問題模糊及擴大，留言時也請注意用詞，謝謝!

大家好：

我是站長 sega。

在此跟各位報告巴哈姆特此時正遭受的威脅：

27日(日)晚上10:00，機房人員來電通知巴哈首頁伺服器當機，原本以為只是一般的當機，沒想到伺服器重開之後，短短幾秒之內，又再度當機，再次重開之後，情況依舊。

後來經過關閉對外連線後查詢系統 log，發現遭受到來自世界各地的 ip，以極大量的速度對伺服器發出網頁要求試圖癱瘓巴哈首頁，伺服器不堪負荷，因此當機。

直到星期一清晨五點左右，攻勢才逐漸趨緩。

28日(一)下午一點，我們接到了一封信件：

寄件者： wuwebshell <wuwebshell@vip.qq.com>

傳送日期： 2008-4-28 下午 01:00

主旨： 广告联系

昨天发动对贵公司的攻击，在此深表歉意，也说明贵公司的网络安全的当务之急,本人做私人服务器的，能否到贵站发布广告，请速回mail。谢谢

我們終於知道被攻擊的原因。

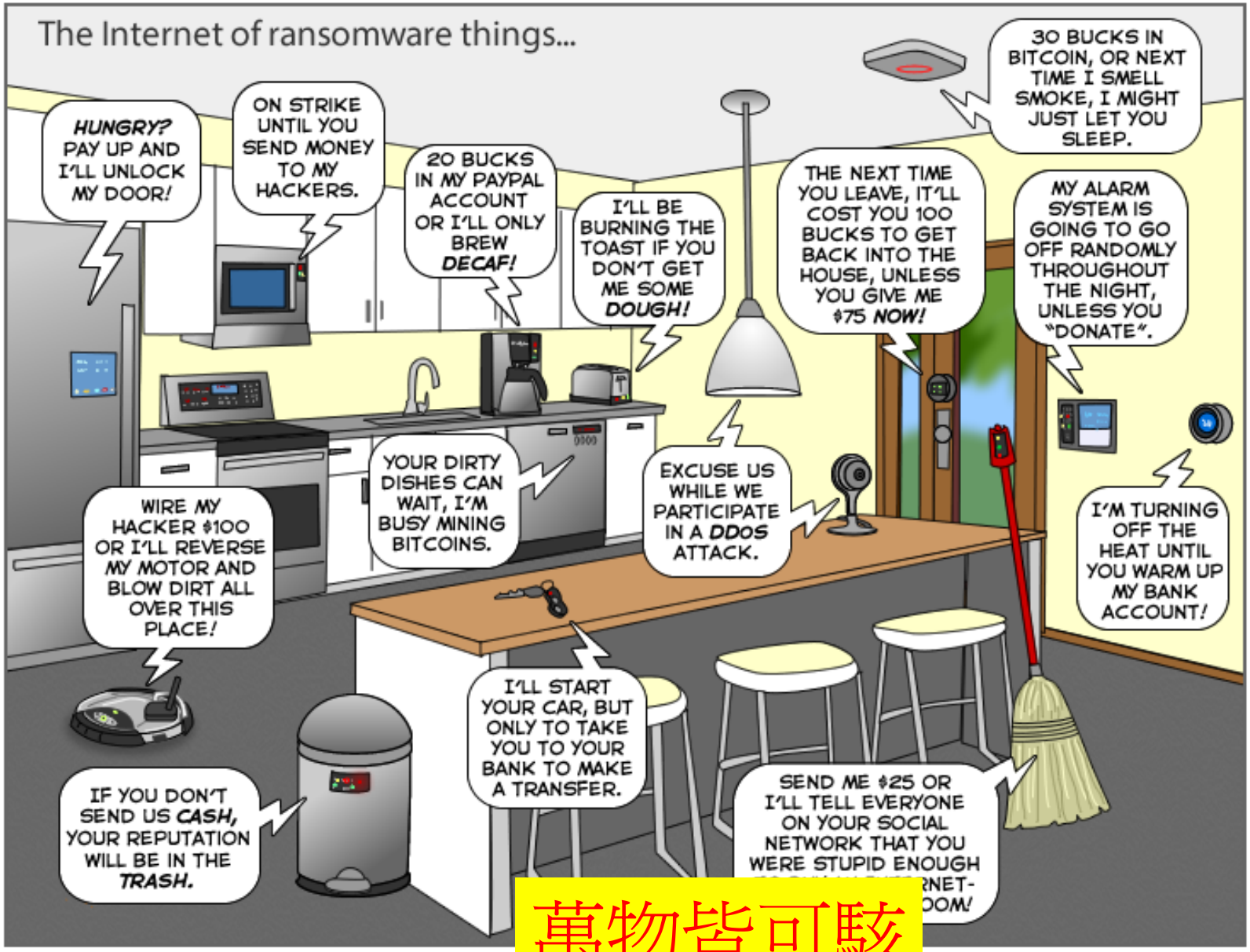
網際網路

美國大學遭到DDoS攻擊，「凶手」竟然是校內的自動販賣機、路燈

美國電信商Verizon揭露一所美國大學遭到DDoS攻擊，在追查下竟發現來自校內為數約5000台的物連網裝置，包含連網路燈、自動販賣機等，所幸駭客操控手法不夠高明，校方最後取回這些連網裝置的控制權。

文/ 陳文義 | 2017-02-14 發表

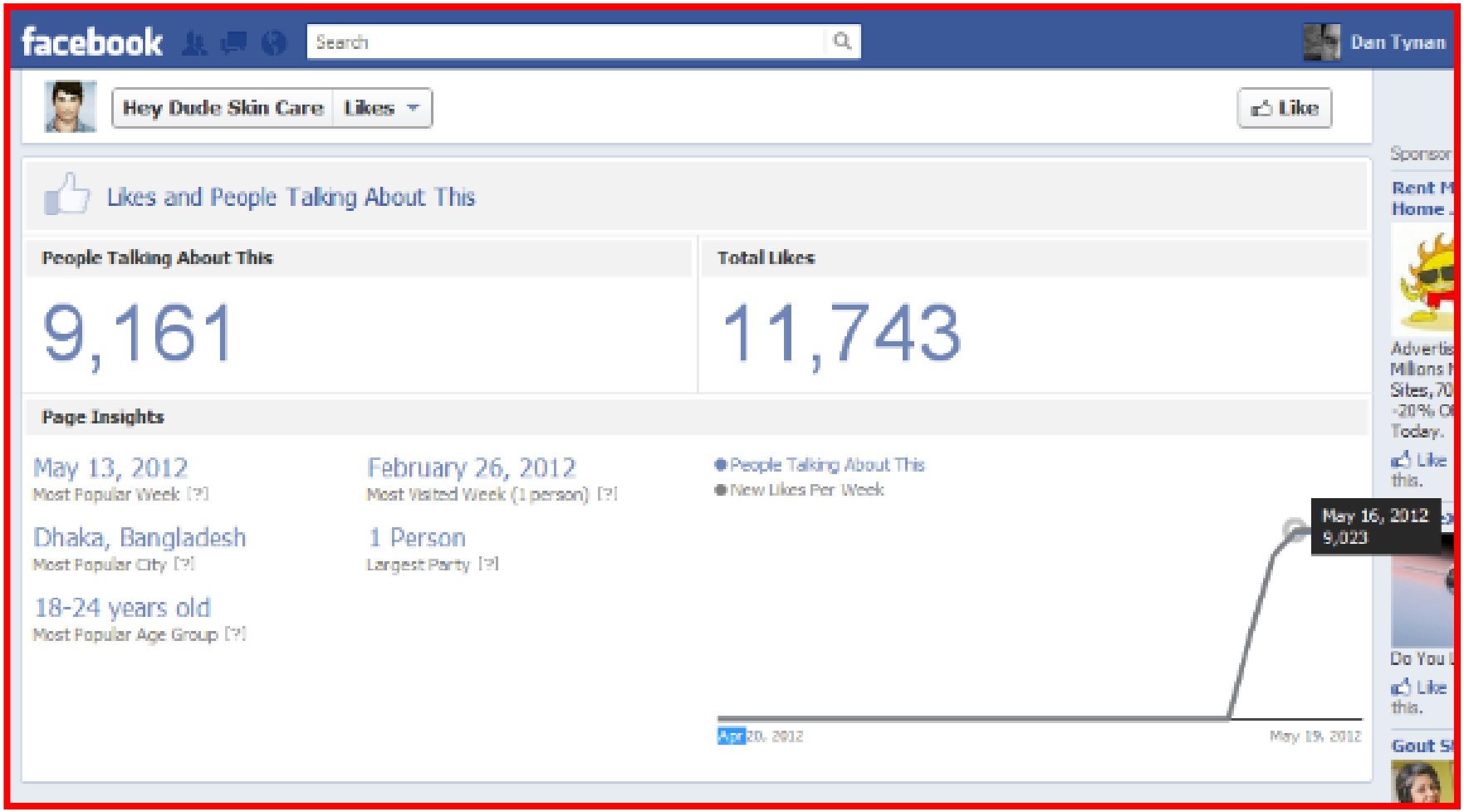
The Joy of Tech™ by Nitrozac & Snaggy

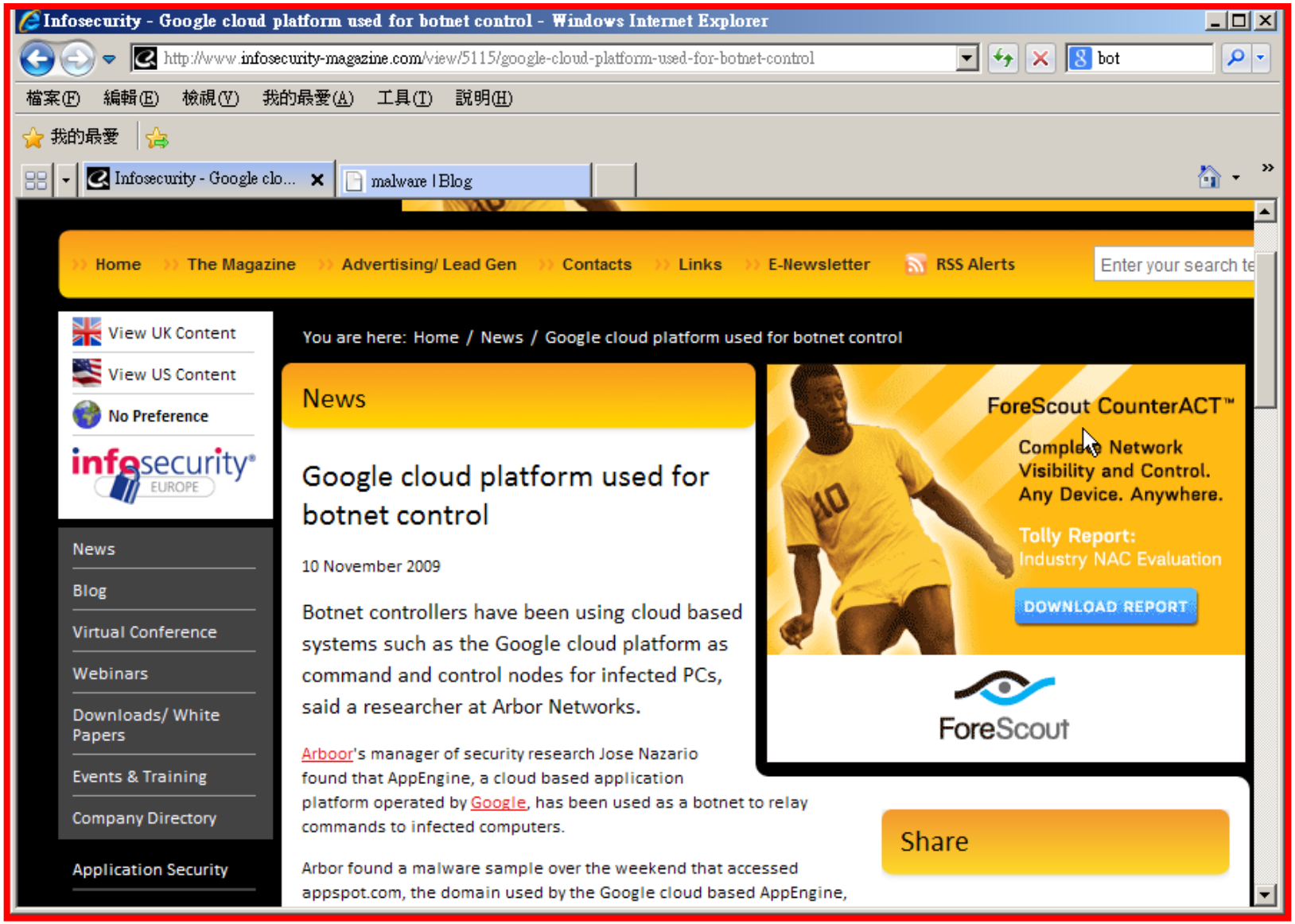


萬物皆可駭

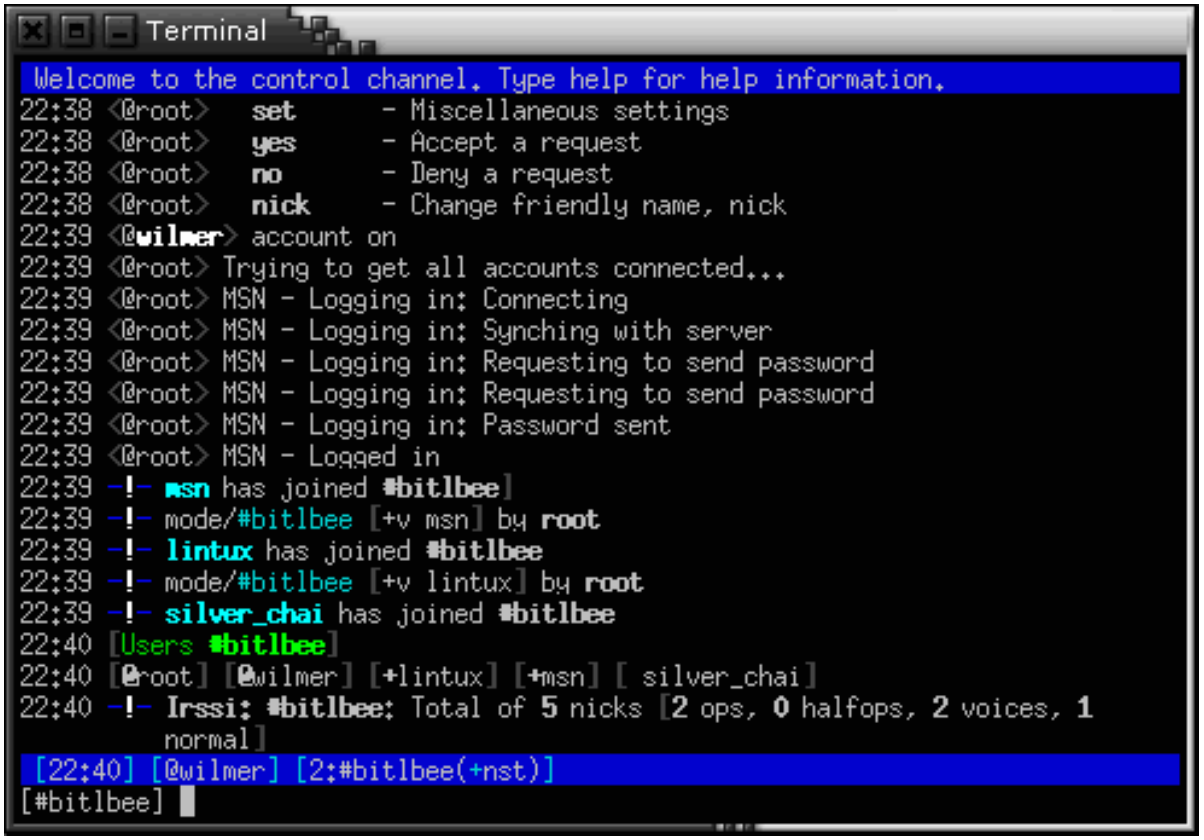
You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com


facebook
Search
Dan Tynan
Hey Dude Skin Care
Likes
Like
Likes and People Talking About This
People Talking About This
9,161
Total Likes
11,743
Page Insights
May 13, 2012
Most Popular Week [?]
February 26, 2012
Most Visited Week (1 person) [?]
Dhaka, Bangladesh
Most Popular City [?]
1 Person
Largest Party [?]
18-24 years old
Most Popular Age Group [?]
People Talking About This
New Likes Per Week
May 16, 2012
9,023
Apr 20, 2012
May 19, 2012
Sponsor
Rent M
Home
Adverti
Millions
Sites, 70
-20% O
Today.
Like
this.
Do You
Like
this.
Gout S


Infosecurity - Google cloud platform used for botnet control - Windows Internet Explorer
http://www.infosecurity-magazine.com/view/5115/google-cloud-platform-used-for-botnet-control
bot
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
Infosecurity - Google clo...
malware | Blog
Home
The Magazine
Advertising/ Lead Gen
Contacts
Links
E-Newsletter
RSS Alerts
Enter your search te
View UK Content
View US Content
No Preference
infosecurity EUROPE
News
Blog
Virtual Conference
Webinars
Downloads/ White Papers
Events & Training
Company Directory
Application Security
You are here: Home / News / Google cloud platform used for botnet control
News
Google cloud platform used for botnet control
10 November 2009
Botnet controllers have been using cloud based systems such as the Google cloud platform as command and control nodes for infected PCs, said a researcher at Arbor Networks.
Arboor's manager of security research Jose Nazario found that AppEngine, a cloud based application platform operated by Google, has been used as a botnet to relay commands to infected computers.
Arbor found a malware sample over the weekend that accessed appspot.com, the domain used by the Google cloud based AppEngine,
ForeScout CounterACT™
Complete Network Visibility and Control. Any Device. Anywhere.
Tolly Report: Industry NAC Evaluation
DOWNLOAD REPORT
ForeScout
Share

DDoS IRC/CLoud Based

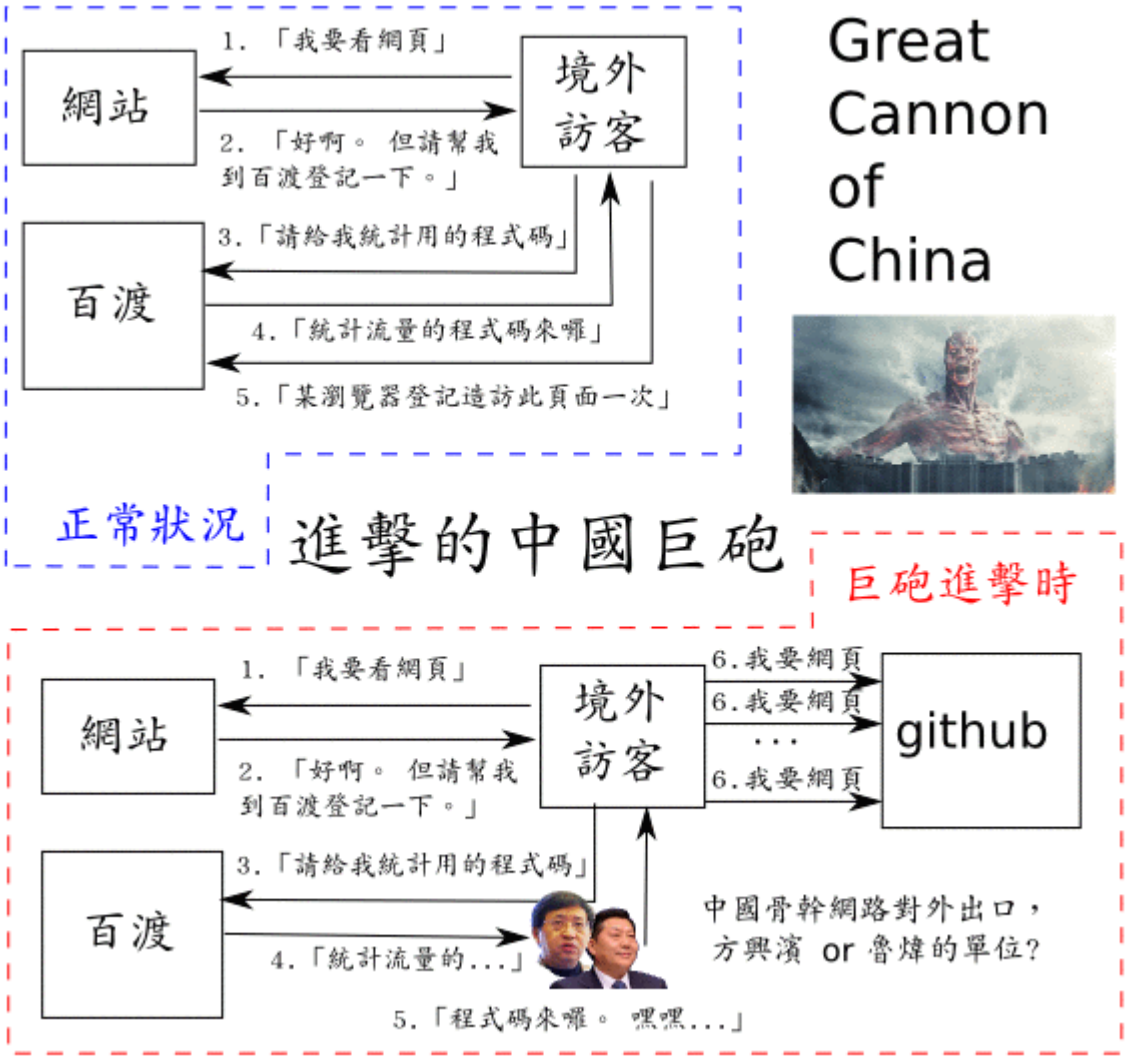


- 常用工具
  - Trinity
  - Knight
  - Kaiten

肉雞服務


是您殺人越貨持家理財生意興隆之必備良器 - PDA、PDA phone - HKFF 失敗論壇 - Powered by Discuz! - Windows Internet Explorer
http://www.failforum.net/forum/viewthread.php?tid=1313500
HKFF 失敗論壇 » PDA、PDA phone » 是您殺人越貨持家理財生意興隆之必備良器
Citibank「卡數結餘轉戶」，可借高達21倍月薪，立即申請！
分享到 facebook
回 復
新 帖
是您殺人越貨持家理財生意興隆之必備良器
打印
ddos1688
發表於 2010-12-15 01:48 AM 只看該作者
負積分會員
UID 1716990
帖子 7
精華 0
威望 -1
金幣 35
積分 0
註冊時間 2010-12-15
個人空間
發短消息
加為好友
是您殺人越貨持家理財生意興隆之必備良器
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

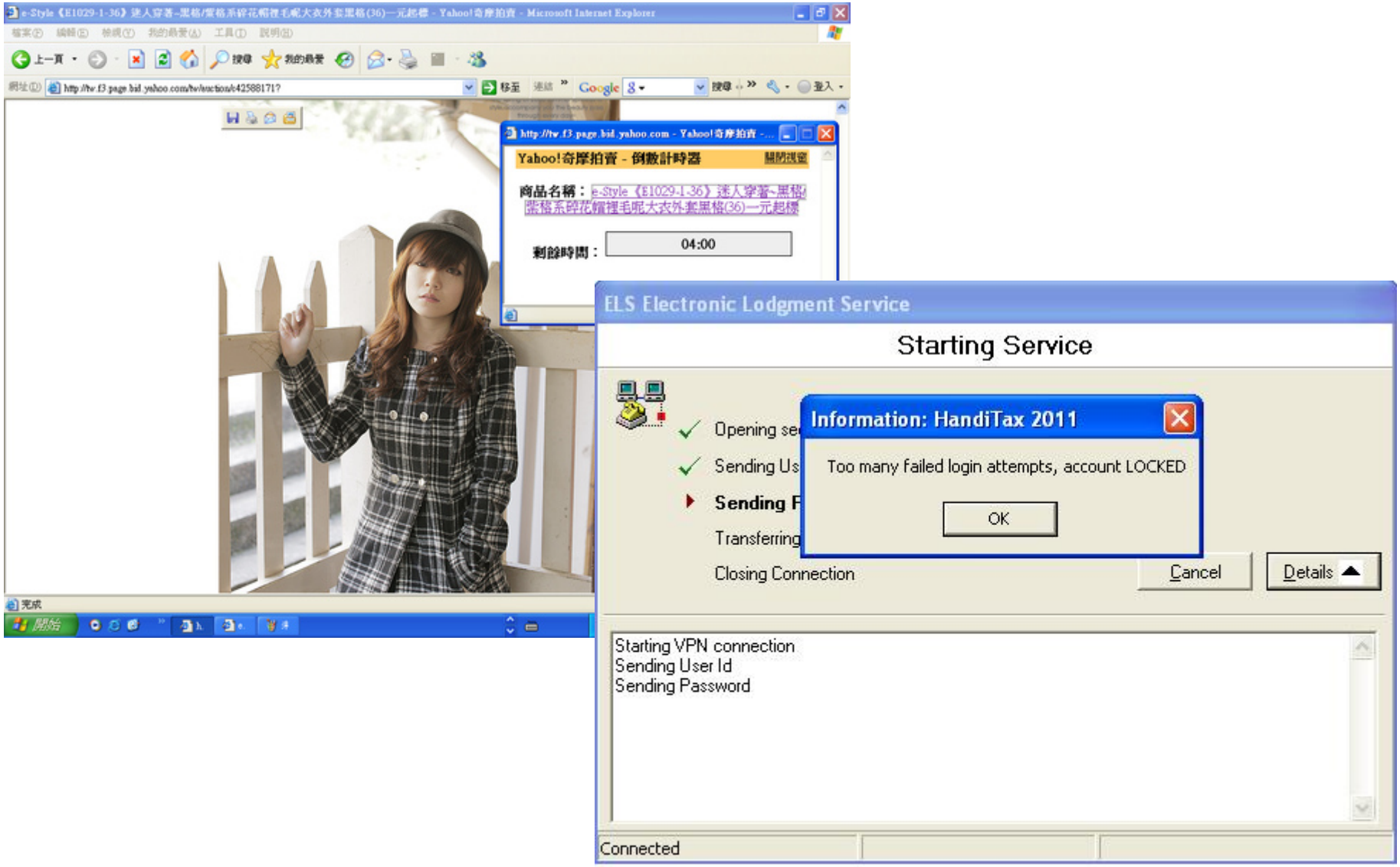
Great Cannon



DoS的攻擊目標

- 破壞目標實體設備
- 癱瘓目標服務網路
  - 頻寬消耗(Bandwidth Depletion)
  - 干擾連線 (Disrupt connection)
- 打擊目標主機或服務程式
  - 弱點攻擊(Exploitation)
  - 資源消耗(Resource Depletion)
- 阻礙個體使用者

帳號鎖定

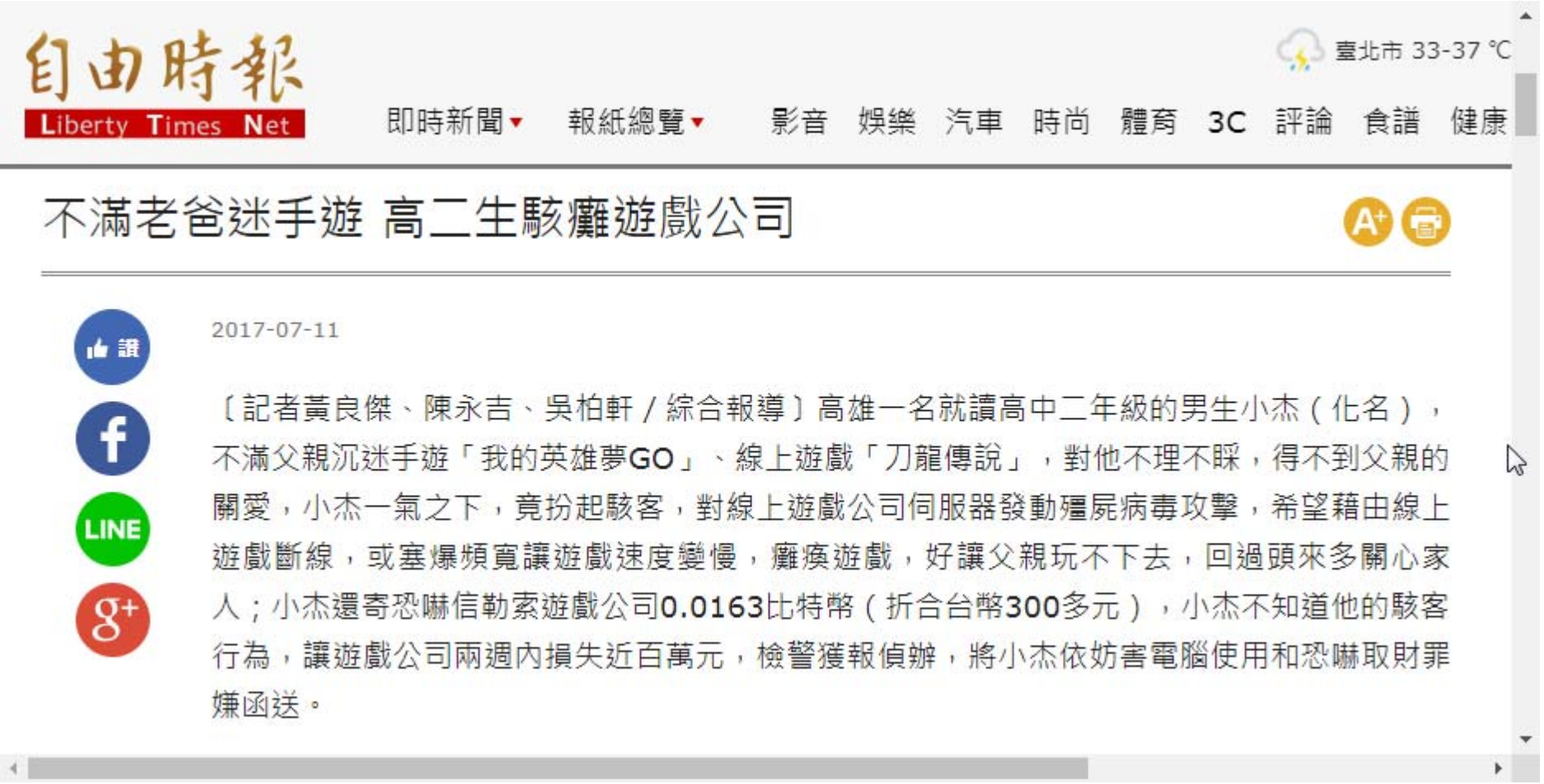

Yahoo!奇摩拍賣 - 倒數計時器
商品名稱：
剩餘時間：
04:00
ELS Electronic Lodgment Service
Starting Service
Information: HandiTax 2011
Too many failed login attempts, account LOCKED
OK
Transferring
Closing Connection
Cancel
Details
Starting VPN connection
Sending User Id
Sending Password
Connected

檢舉功能


檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
最美校花遭盜用 慕容生…
www.ettoday.net/news/20120927/108078
Yahoo 拍賣 倒數
最美校花遭盜用 慕容生氣：睜大眼睛看清楚
正文
網友評論
友善列印
點評：好衰喔！
偶像又被踢爆？快下載新聞雲app追蹤去
ETtoday分享雲
說這專頁讚
54 萬 按讚
記者蕭采薇／台北報導
「最美校花」慕蓉慘遭臉書「水桶」數天，直到27日才解禁。據悉是
檢舉她是「假慕蓉」。慕蓉也在臉書生氣的說：「睜大眼睛看清楚好嗎？真的憤怒唉。」看
來相當無奈。
很抱歉，你無法從這個帳號發表貼文到 Facebook。
為了安全起見，你的帳號會有幾天受到存取網站的限制。如有任何問題，
請前往我們的使用說明。
若你認為這是誤會，請請通知我們。
關閉

流量清洗擋不住權限清洗...

這全都是愛



自由時報 Liberty Times Net

臺北市 33-37 ℃

即時新聞 報紙總覽 影音 娛樂 汽車 時尚 體育 3C 評論 食譜 健康

不滿老爸迷手遊 高二生駭癱遊戲公司

讚

2017-07-11

〔記者黃良傑、陳永吉、吳柏軒／綜合報導〕高雄一名就讀高中二年級的男生小杰（化名），不滿父親沉迷手遊「我的英雄夢GO」、線上遊戲「刀龍傳說」，對他不理不睬，得不到父親的關愛，小杰一氣之下，竟扮起駭客，對線上遊戲公司伺服器發動殭屍病毒攻擊，希望藉由線上遊戲斷線，或塞爆頻寬讓遊戲速度變慢，癱瘓遊戲，好讓父親玩不下去，回過頭來多關心家人；小杰還寄恐嚇信勒索遊戲公司0.0163比特幣（折合台幣300多元），小杰不知道他的駭客行為，讓遊戲公司兩週內損失近百萬元，檢警獲報偵辦，將小杰依妨害電腦使用和恐嚇取財罪嫌函送。

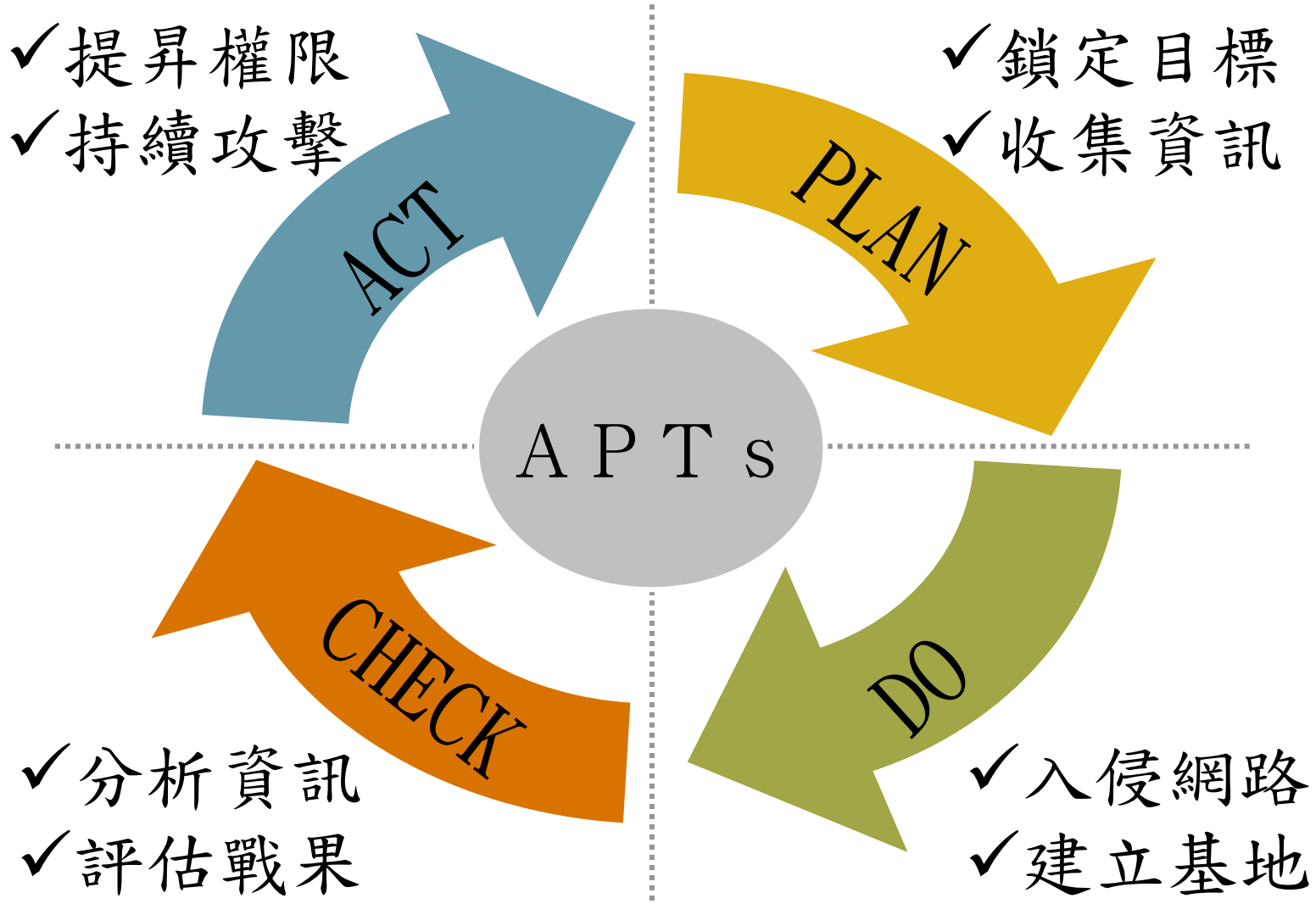
進階持續性威脅(APT)
概念與案例

APT攻擊現象

- APT, Advanced Persistent Threat – 針對特定目標，利用最新技術有規模地長期進行攻擊。採被動為主動，鎖定具有高價值目標的攻擊行為
- 駭客比目標組織還要了解組織
- 目標明確精準，範圍小樣本少，不易警覺，攻擊內容量身訂做，以假亂真
- 相關的子公司、合作廠商、下包商、物流業者都是可能被攻擊的對象
- 經常拌隨針對性的社交工程（原名魚叉式攻擊）
- 長期、低調、不易發現

資安界習慣發明新名詞，被害者聲稱被新名詞攻擊，聽起來感覺比較沒有責任:P

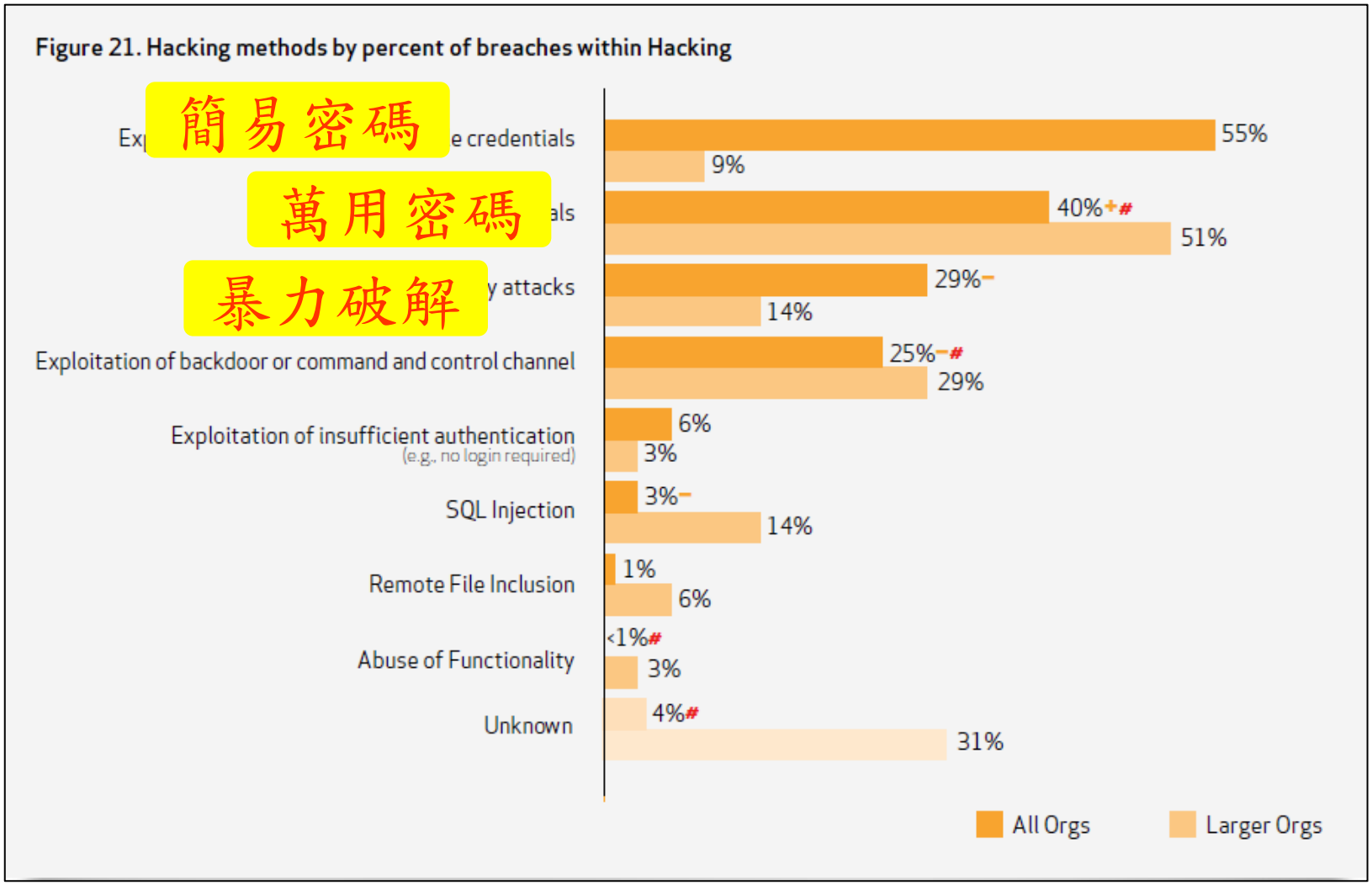
APT PDCA


✓提昇權限
✓持續攻撃
ACT
✓鎖定目標
✓収集資訊
PLAN
APTs
CHECK
✓分析資訊
✓評估戦果
DO
✓入侵網路
✓建立基地

被狠狠羞辱的資安大神

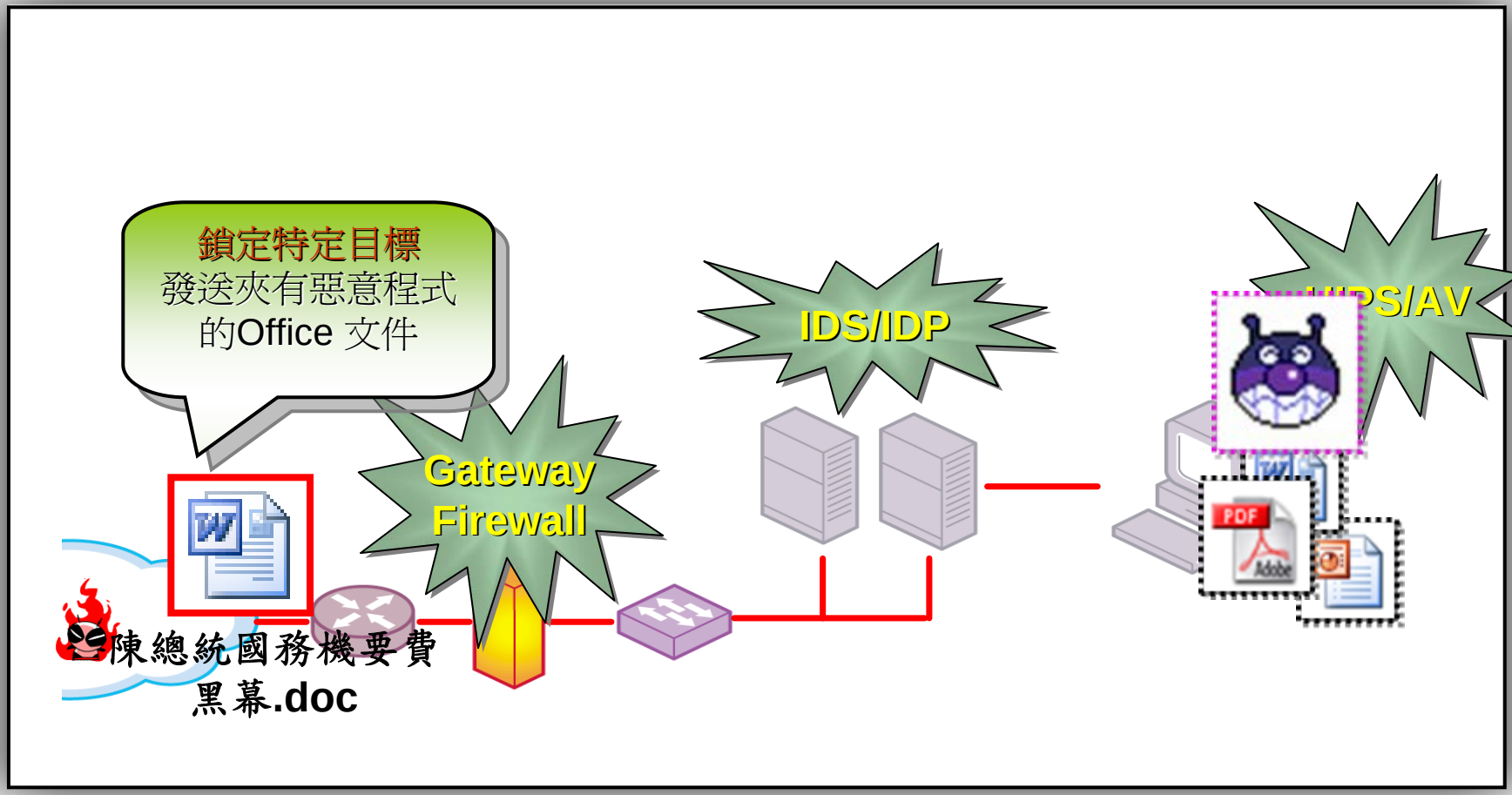

資安八卦鏡：被狠狠羞辱的資安大神 ,Information Security 資安人科技網 - Windows Internet Explorer
http://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=6072&pages=3
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
資安八卦鏡：被狠狠羞辱的資安大神 ,Information ...
▲ 社交工程偽冒信件內容，資料來源：http://krebsonsecurity.com
簡單摘要如下，駭客先冒充Greg Hoglund寄給他們公司的IT manager說：「我現在人在歐洲出差，我想連回進公司Server，情況很急，等一下就要用，可以幫我改一下Firewall的設定，以及把Root密碼改成changeme123嗎？」
IT Manager說：「OK!」
呃...之後，我就不用說了，反正是很歡樂… XD
有防火牆就不會資料外洩？
這些外洩的E-mail十分精彩，八卦內幕都有，包含HB Gary跟CIA、NSA、FBI、軍方、參議院還有各家資安公司往來信件都被公佈在網路上（據聞某朋友熬夜看了兩天，看到欲罷不能！）。原來HBGary也幫美國政府單位研究很多網軍的活動，據說也做了一些阿里不達的事情，而且對大陸駭客也著墨不少，由此可知各國對於資訊戰爭已經是提升到國防等級問題。反觀我們政府的資安態度，每次都是那句老話「本單位設置有XX道防火牆，沒有資料外洩情況發生」。
結論
這個故事告訴我們，花再多錢買了再多道防火牆、防水牆、防毒牆、防釣蝦牆、防釣魚牆都沒用，上了再多的教育訓練也沒用。
你看，一家國際級的資安公司三兩下就被幹掉，連大師也殞落了。
史記資安篇有記載，正所謂「樹大有枯枝，人多有白癡，雞排加辣最好吃」，駭客隨時都在虎
網際網路
115%

資料拼圖

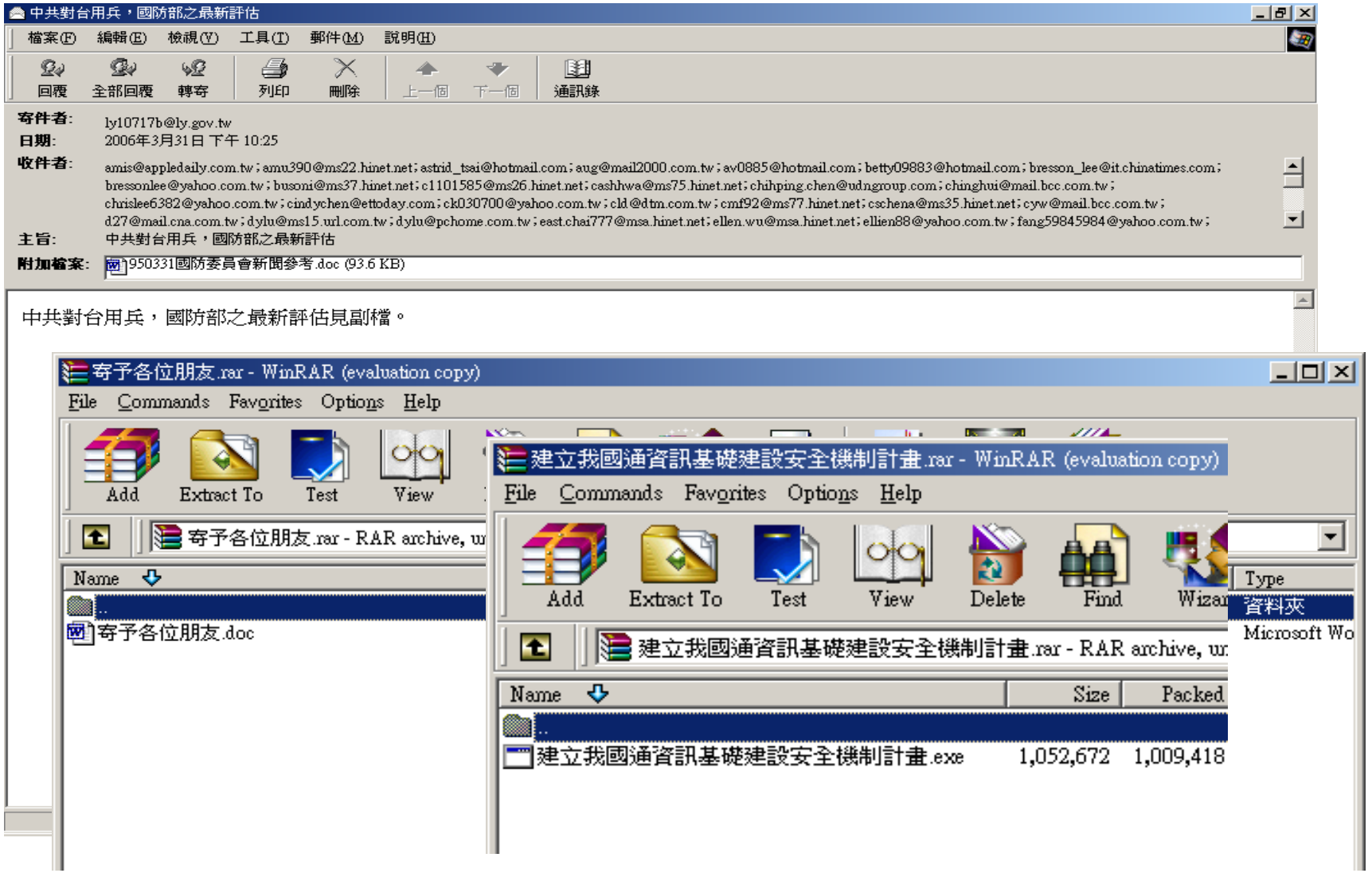


2012 Data BREACH Investigations Report - Verizon RISK Team

魚叉式路徑示意圖


鎖定特定目標
發送夾有惡意程式
的Office 文件
Gateway
Firewall
IDS/IDP
PS/AV
PDF
Adobe
陳總統國務機要費
黑幕.doc

網軍


中共對台用兵，國防部之最新評估
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄
寄件者: ly10717b@ly.gov.tw
日期: 2006年3月31日 下午 10:25
收件者: amis@appledaily.com.tw; amu390@ms22.hinet.net; astrid_tsai@hotmail.com; aug@mail2000.com.tw; av0885@hotmail.com; betty09883@hotmail.com; bresson_lee@it.chinatimes.com; bressonlee@yahoo.com.tw; busoni@ms37.hinet.net; c1101585@ms26.hinet.net; cashhwa@ms75.hinet.net; chihping.chen@udngroup.com; chinghui@mail.bcc.com.tw; chrislee6382@yahoo.com.tw; cindychen@ettoday.com; ck030700@yahoo.com.tw; cld@dtm.com.tw; cmf92@ms77.hinet.net; cschena@ms35.hinet.net; cyw@mail.bcc.com.tw; d27@mail.cna.com.tw; dylu@ms15.url.com.tw; dylu@pchome.com.tw; east.chai777@msa.hinet.net; ellen.wu@msa.hinet.net; ellien88@yahoo.com.tw; fang59845984@yahoo.com.tw;
主旨: 中共對台用兵，國防部之最新評估
附加檔案: 950331國防委員會新聞參考.doc (93.6 KB)
中共對台用兵，國防部之最新評估見副檔。
寄予各位朋友.rar - WinRAR (evaluation copy)
File Commands Favorites Options Help
Add Extract To Test View
寄予各位朋友.rar - RAR archive, u
Name
..
寄予各位朋友.doc
建立我國通資訊基礎建設安全機制計畫.rar - WinRAR (evaluation copy)
File Commands Favorites Options Help
Add Extract To Test View Delete Find
建立我國通資訊基礎建設安全機制計畫.rar - RAR archive, u
Name Size Packed
..
建立我國通資訊基礎建設安全機制計畫.exe 1,052,672 1,009,418
Type
資料夾
Microsoft Wo

水坑式攻擊（watering hole）

勒索病毒實例分析

勒索軟體成企業頭痛問題

File Edit View History Bookmarks Tools Help

RUN!PC | 即時新聞 | 資訊安...

www.runpc.com.tw/news.aspx?id=101

Search

即時新聞 - 資訊安全

分享到FaceBook 分享到Plurk

運用垃圾郵件入侵 勒索軟體成企業頭痛問題

【文／編輯部】2016/6/17 下午 02:14:59

Forcepoint日前公布一份最新Forcepoint 2016全球趨勢資安報告，該報告來源是從該公司廣佈在全世界155個國家當中的資安設備中，持續收集多達30億筆以上資料的分析結果。其中最值得注意之處，在經過長達6個月的觀察與分析發現，一個名為Jaku的全新僵屍網路活動，而2015年前五大受害國分別為南韓、日本、中國、美國、臺灣，顯見該攻擊標的主要以亞洲為主。

在該份研究報告中，還有幾項值得關注的資安趨勢，首先是在全球商業障礙快速消逝的趨勢下，帶動勒索軟體、反惡意軟體工具不斷問世，除導致網路專家、資安人員工作量大增外，也讓從事跨國貿易公司面臨更為嚴峻的營運挑戰。其次，全球各地仍然不斷爆發資料外洩事件，有不少事件源自於員工資安意識不足所致。根據統計結果顯示，2015年遭受入侵事件的企業中，有超過50%是因內部員工不慎誤用、或使用者出錯所致。

Forcepoint認為，勒索軟體目標是削弱國家經濟和工業競爭力，以及企圖在更短時間內獲得更高的經濟利益，才會導致2015年郵件攻擊事件比2014年多出250%。特別是現今雲服務供應商與企業資訊系統的安全規則迥異，導致資料保護方式極為複雜，也給予駭客組織更多可趁之機。

回首頁...

勒索軟體

- 一但中了病毒，所有本機檔案被加密，必需要付贖金給駭客，才能將檔案解密
- 注意
  - 會加密外接裝置內檔案，例如USB外接硬碟、NAS外接儲存系統
  - 會加密網路分享磁碟或雲端共享空間，例如Dropbox、企業內網芳主機
- 常見軟體：
  - TorLocker, TorrentLocker, CryptoLocker 、CTB-Locker、CryptoWall等等

2016年勒索軟體數量增加752%

趨勢科技：2016年勒索軟體數量增加752%

2015年新增勒索軟體只有29個，但2016年卻一口氣增加了247個，成長7倍之多。勒索軟體不斷精進，要求更多的贖金，鎖定的目標也不只是個人電腦，還有手機、伺服器，從個人到企業均受害。

文/ 陳曉莉 | 2017-05-29 發表

示意圖，與新聞事件無關。

早期勒索軟體


猜到密碼即可破解，密碼多半已公開
Endereço C:\System\Users\
Nome
TERMO DE JANELA
TREINAMENTO BOMBEIRO
UNIMED
USO RÁDIO
VALE TRANSPORTE E PASSES
VALE TRANSPORTE PROFESSORES
Pasta de arquivos
0% Extracting C:\System\Users\Do ... @gmail.com !).exe
Elapsed time:
Remaining time:
Files:
Compression ratio:
0 B
Enter password
Enter password:
Show password
OK
Cancel
Background
Pause
Cancel
prontuários.doc(!! to get password email id 1145256809 to brsech...
629 KB
Aplicativo
REDUÇÃO CARGA HORÁRIA.docx(!! to get password email id 114...
124 KB
Aplicativo

CryptoLocker

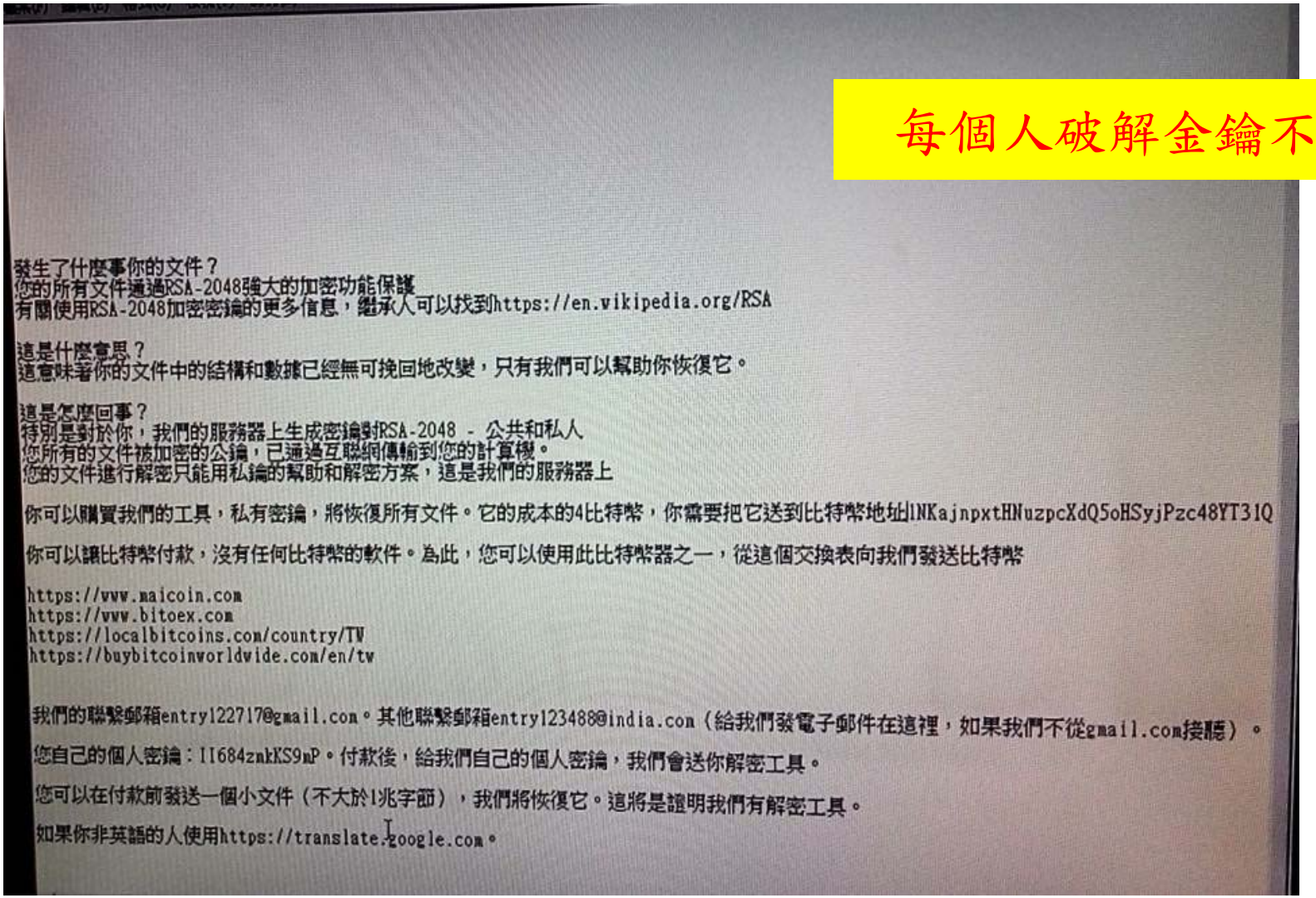
CryptoLocker

Cerber - 限時優惠

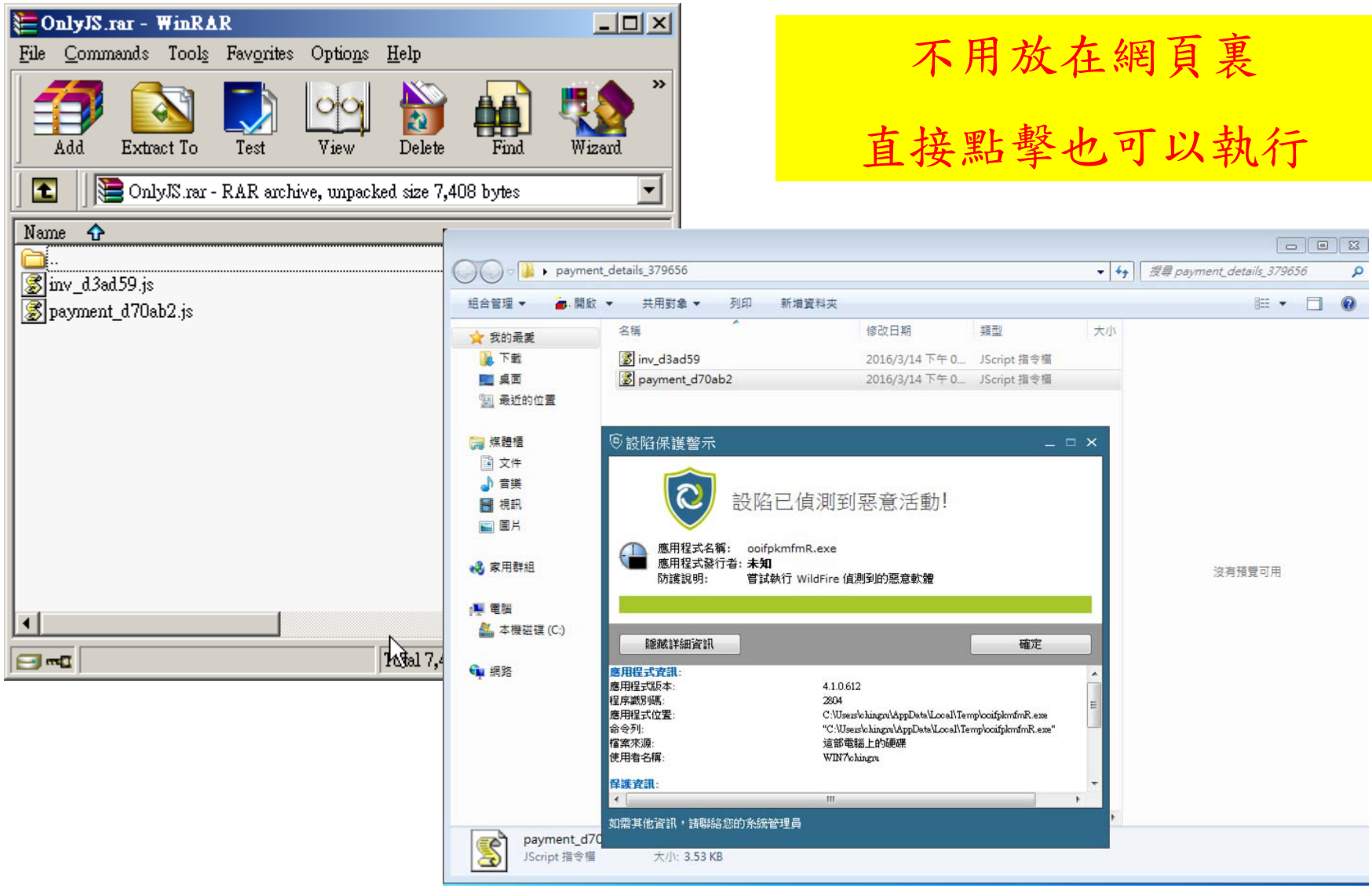

CERBER DECRYPTOR
主页
常问问题
服务支持
免费破译一份文件
重新加载此页面
您的文档、照片、数据库和其他重要文件将被加密！
若要解密您的文件，您需要购买特殊的软件 – «Cerber Decryptor»。
所有的交易仅通过 bitcoin 网络完成。
在 5 天内您可以按照特惠价格 Ƀ1.000 (≈ $681) 购买该产品。
5 天后该产品价格将提高到 Ƀ2.000 (≈ $1363)。
特惠价有效
04 . 20:36:29
如何购买«Cerber Decryptor»?
1. 创建比特币钱包 (我们推荐 Blockchain.info)

勒索

每個人破解金鑰不一樣



Javascript版病毒



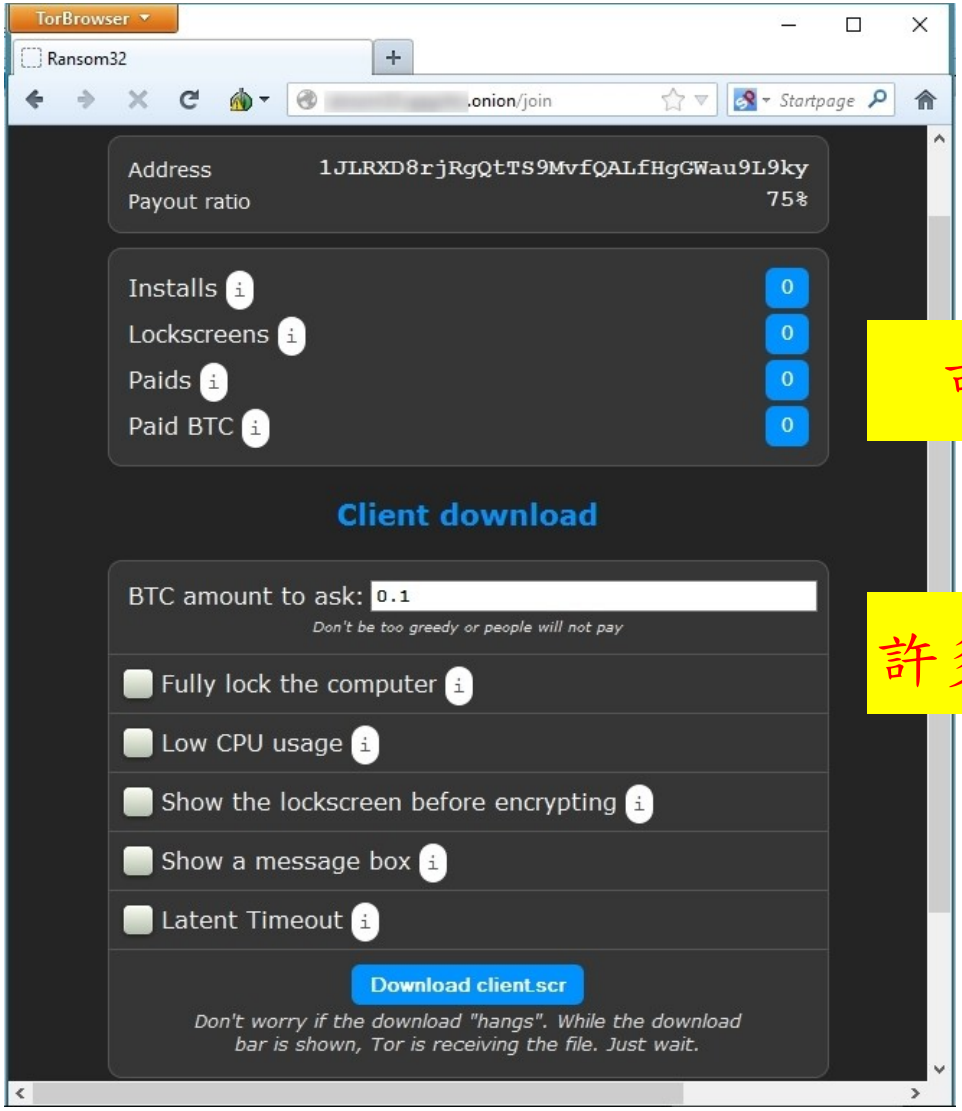
不用放在網頁裏

直接點擊也可以執行

人性的考驗


勒索軟體人性大考驗，受
www.ithome.com.tw/news/110148
iThome
新聞
勒索軟體人性大考驗，受害者只要感染另兩人就能免費解密
安全研究人員發現一個正在開發中的新勒索軟體Popcorn Time，當使用者不慎感染後，螢幕上會顯示兩種解密方式，一是選擇支付1個比特幣作爲贖金獲得解密，另一個是將連結傳給其他人，如果有2人受到感染且支付贖金，第一位受害者就能獲得免費解密。
文/ 陳曉莉 | 2016-12-12 發表
按讚加入iThome粉絲團
G+1 2
圖片來源: 維基共享資源；作者：Jericho
連線中…

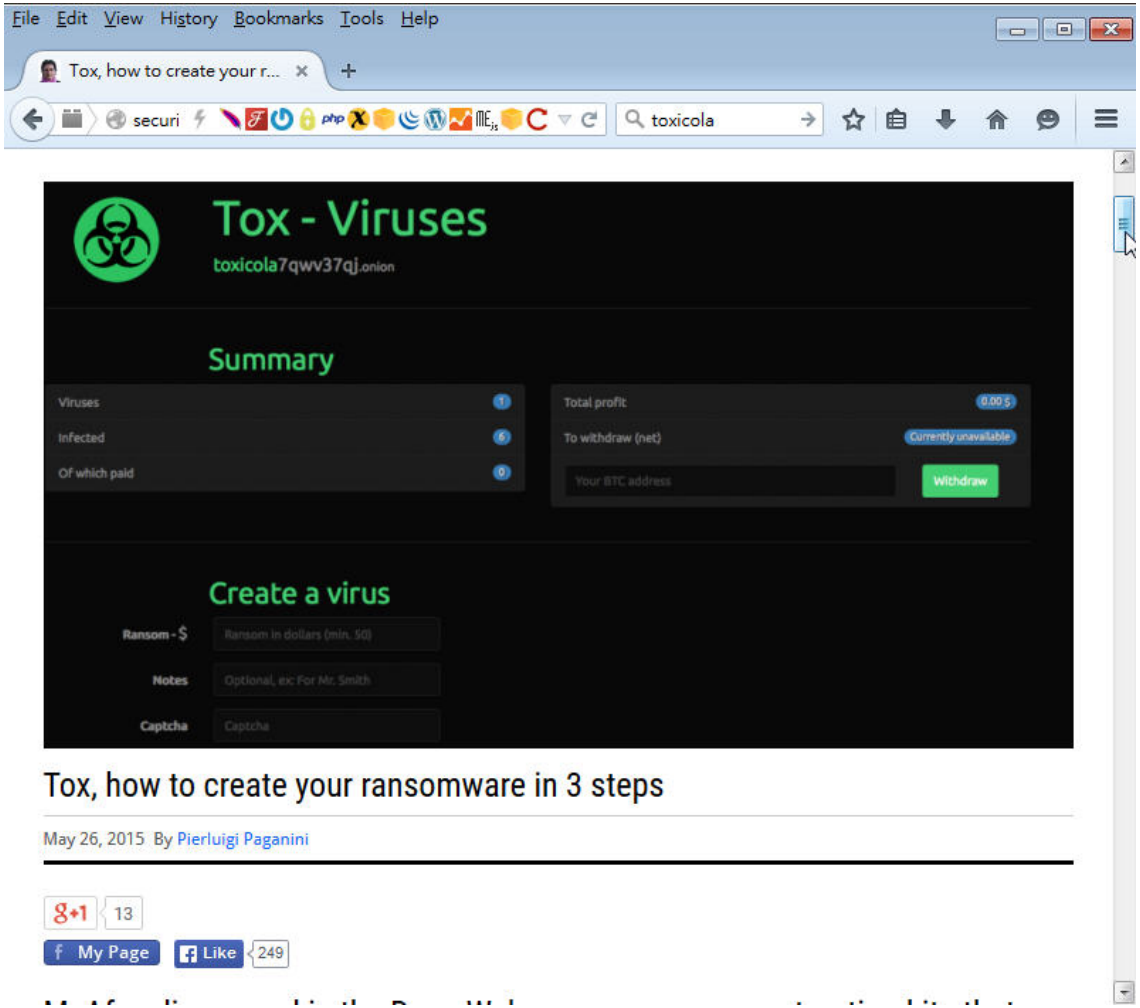
製作工具— Ransom32



可以快速製作不同病毒

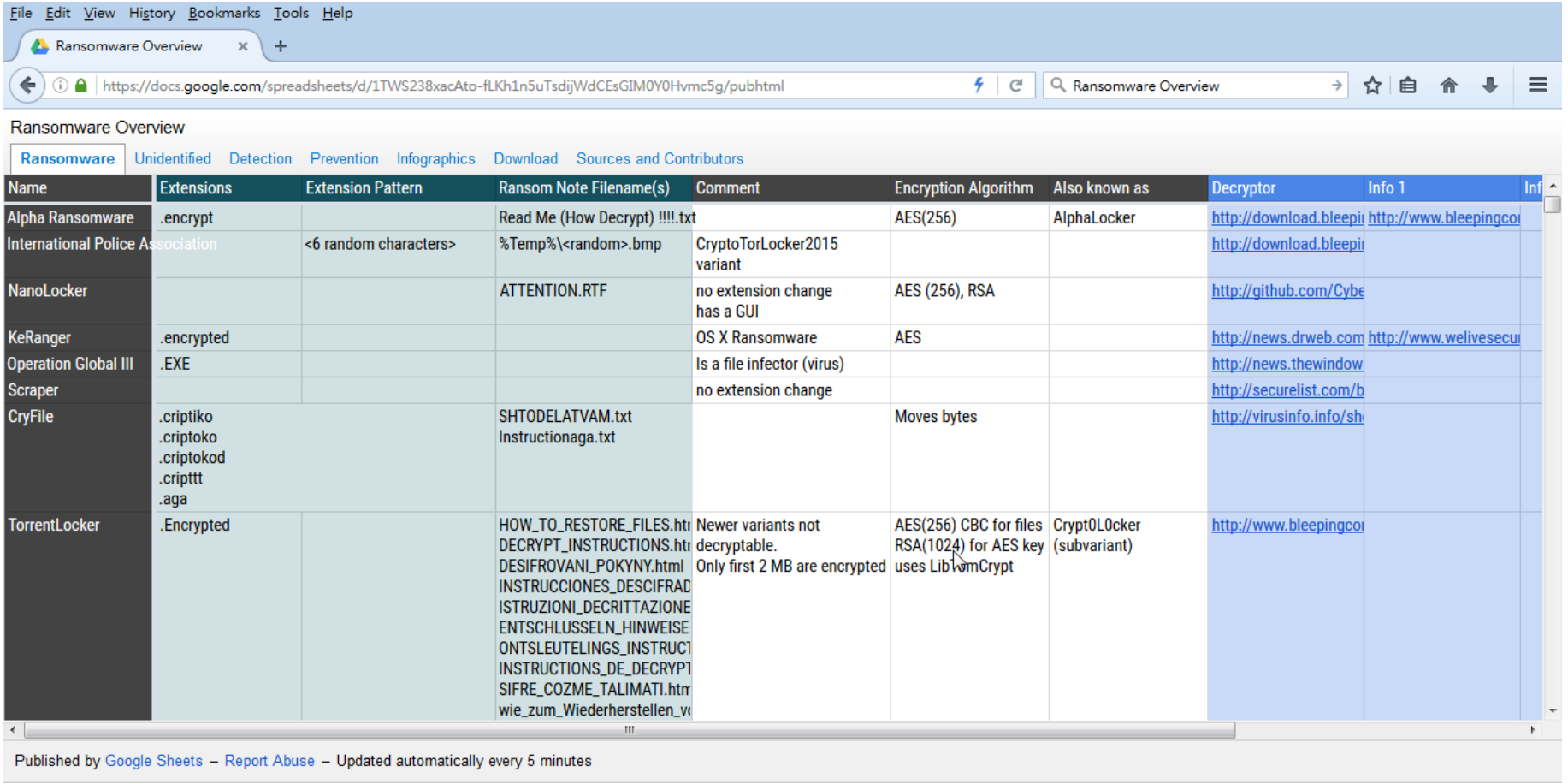
許多掃毒軟體會跳過Js檔案

網路版製作工具— Tox


File Edit View History Bookmarks Tools Help
Tox, how to create your r...
toxicola
Tox - Viruses
toxicola7qwv37qj.onion
Summary
Viruses
Infected
Of which paid
Total profit
To withdraw (net)
Currently unavailable
Your BTC address
Withdraw
Create a virus
Ransom - $
Notes
Captcha
Tox, how to create your ransomware in 3 steps
May 26, 2015 By Pierluigi Paganini
13
My Page
Like
249

勒索大全

- https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml



File Edit View History Bookmarks Tools Help

Ransomware Overview

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml

Ransomware Overview

Ransomware Overview

Ransomware | Unidentified | Detection | Prevention | Infographics | Download | Sources and Contributors

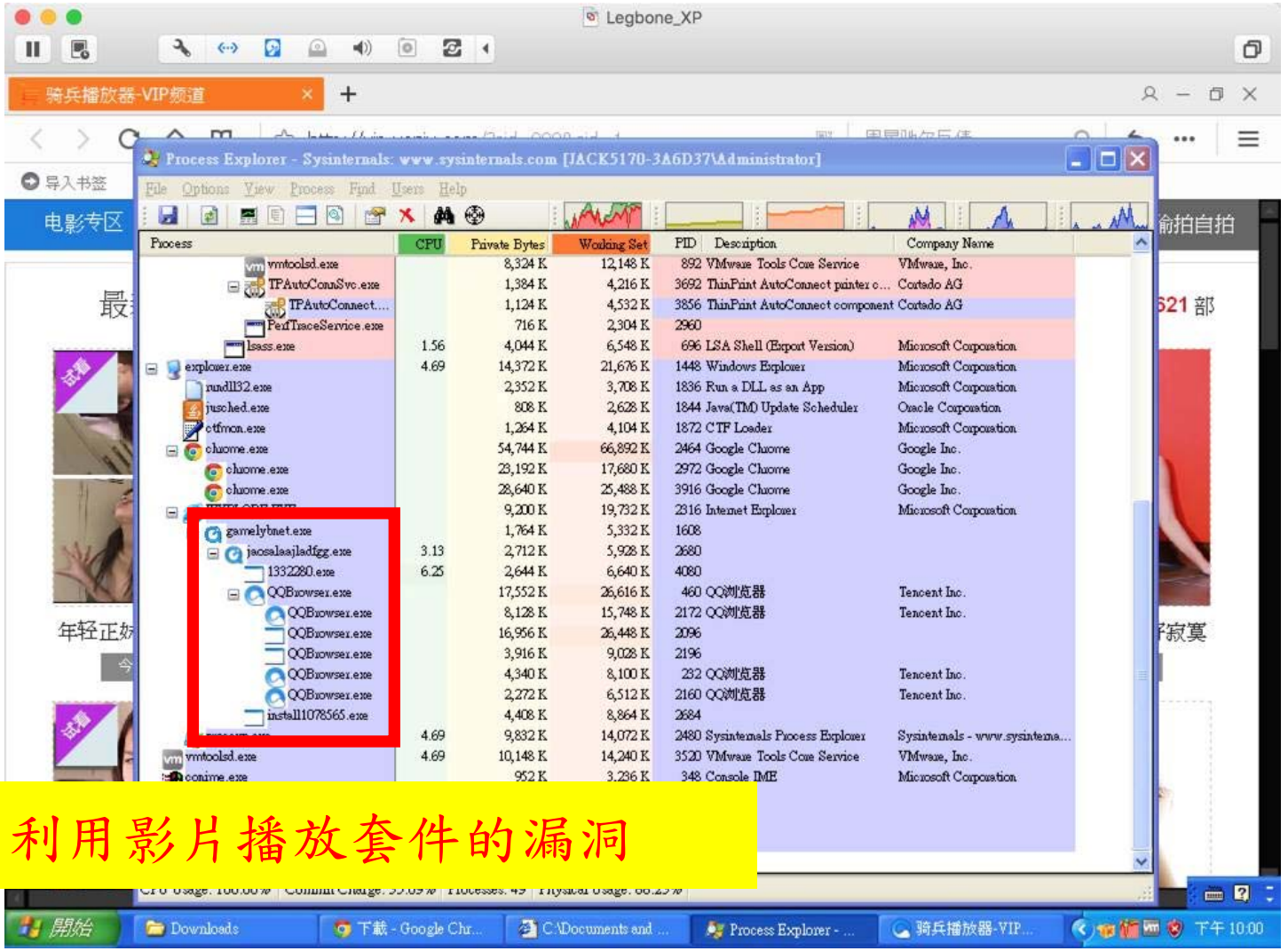
Name	Extensions	Extension Pattern	Ransom Note Filename(s)	Comment	Encryption Algorithm	Also known as	Decryptor	Info 1	Inf
Alpha Ransomware	.encrypt		Read Me (How Decrypt) !!!!.txt		AES(256)	AlphaLocker	http://download.bleepi	http://www.bleepingco	
International Police Association		<6 random characters>	%Temp%\<random>.bmp	CryptoTorLocker2015 variant			http://download.bleepi		
NanoLocker			ATTENTION.RTF	no extension change has a GUI	AES (256), RSA		http://github.com/Cybe		
KeRanger	.encrypted			OS X Ransomware	AES		http://news.drweb.com	http://www.welivesecu	
Operation Global III	.EXE			Is a file infector (virus)			http://news.thewindow		
Scraper				no extension change			http://securelist.com/b		
CryFile	.criptiko .criptoko .criptokod .cripttt .aga		SHTODELATVAM.txt Instructionaga.txt		Moves bytes		http://virusinfo.info/sh		
TorrentLocker	.Encrypted		HOW_TO_RESTORE_FILES.htr DECRYPT_INSTRUCTIONS.htr DESIFROVANI_POKYNY.html INSTRUCCIONES_DESCIFRAD ISTRUZIONI_DECRITTAZIONE ENTSCHLUSSELN_HINWEISE ONTSLEUTELINGS_INSTRUCT INSTRUCTIONS_DE_DECRYPT SIFRE_COZME_TALIMATI.htm wie_zum_Wiederherstellen_v	Newer variants not decryptable. Only first 2 MB are encrypted	AES(256) CBC for files RSA(1024) for AES key uses LibTomCrypt	Crypt0L0cker (subvariant)	http://www.bleepingco		

Published by Google Sheets – Report Abuse – Updated automatically every 5 minutes

駭客入侵，植入網站

會選擇用戶，只把病毒派給IE

駭客入侵，植入網站



利用影片播放套件的漏洞

大喇喇租廣告

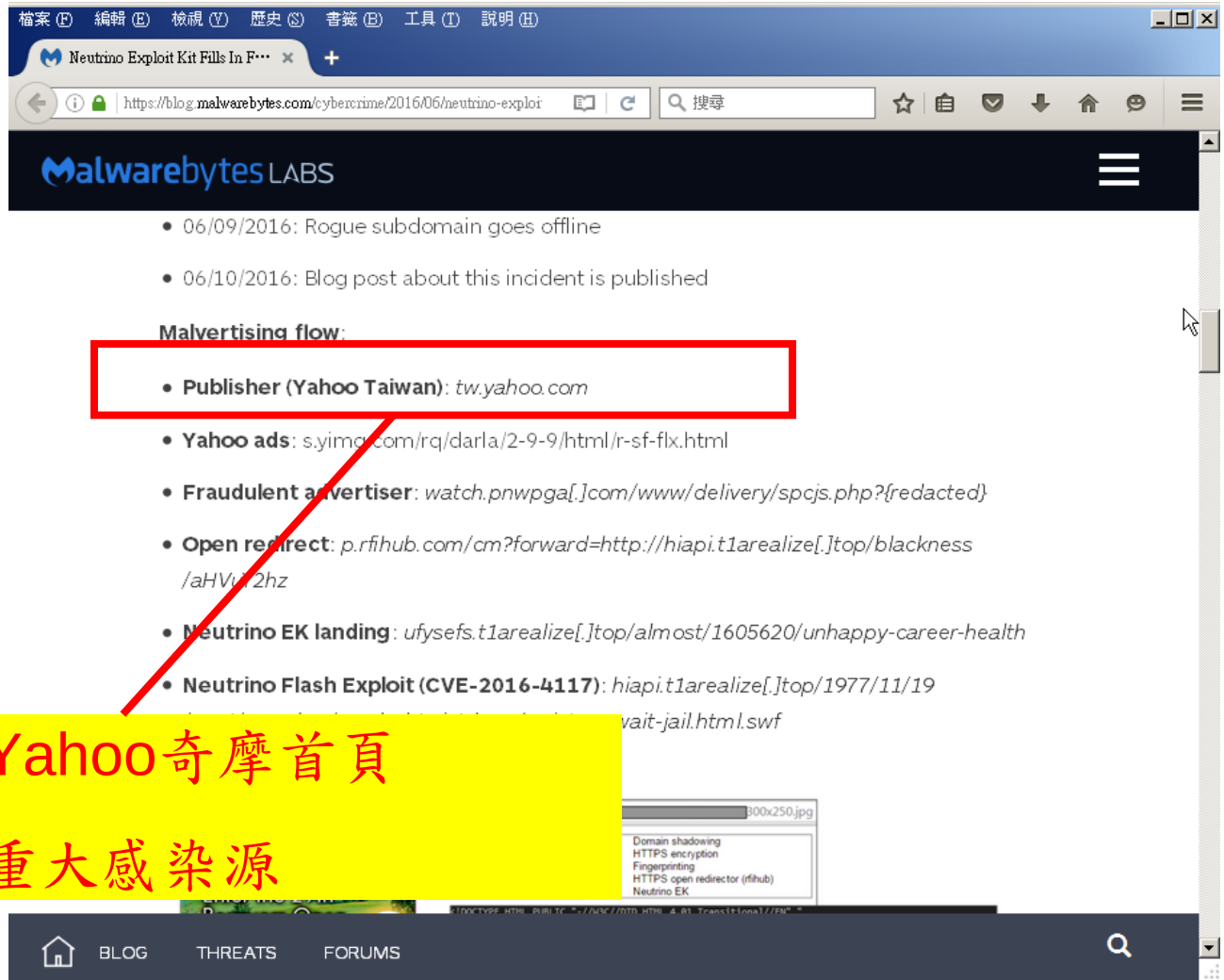
Angler病毒

直接跟紐約時報、BBC、MSN、AOL

等入口網頁租廣告頁

大喇喇租廣告

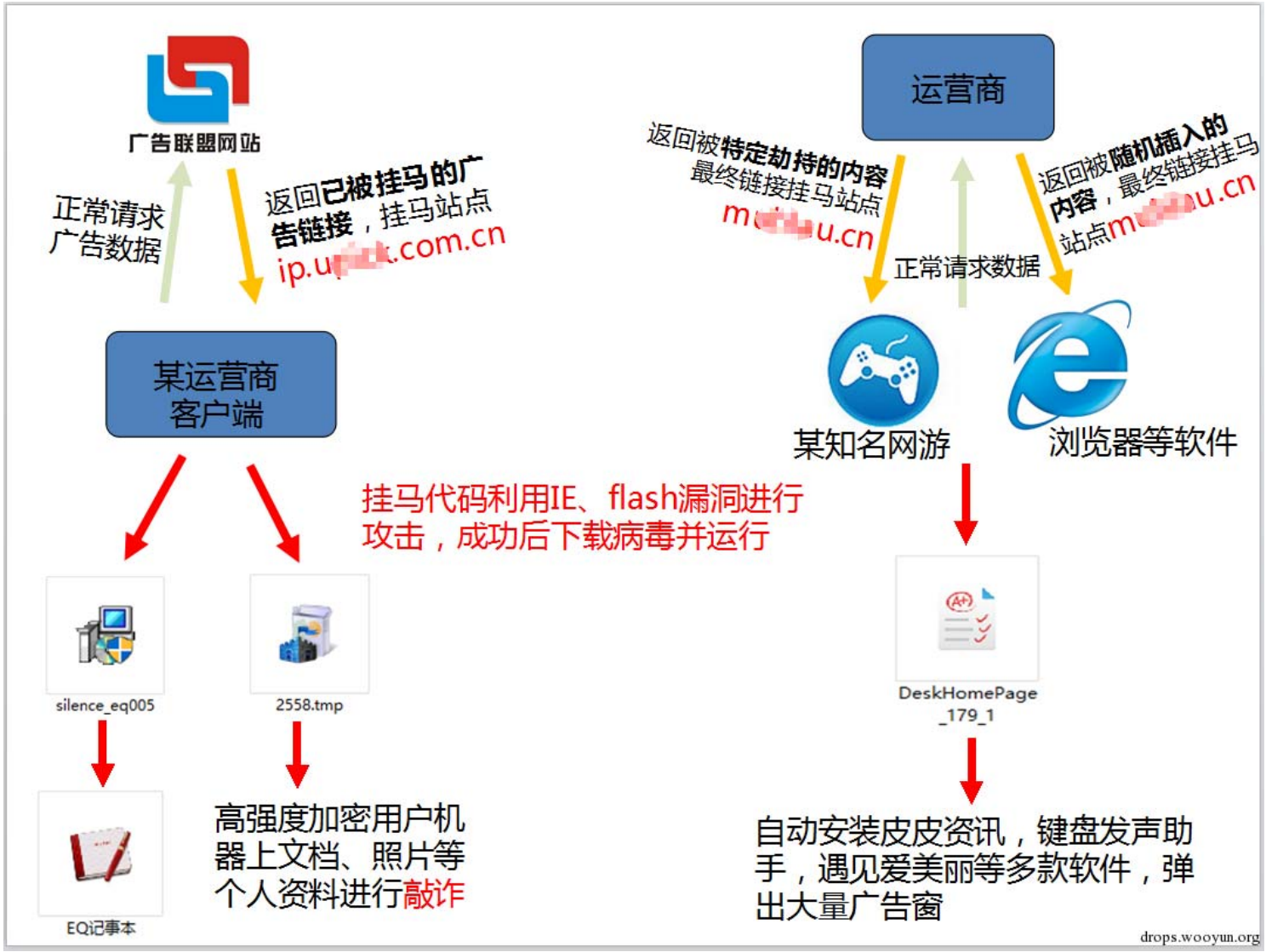
https://blog.malwarebytes.com/cybercrime/2016/06/neutrino-exploit-kit-fills-in-for-angler-ek-in-recent-malvertising-campaigns/



臺灣Yahoo奇摩首頁

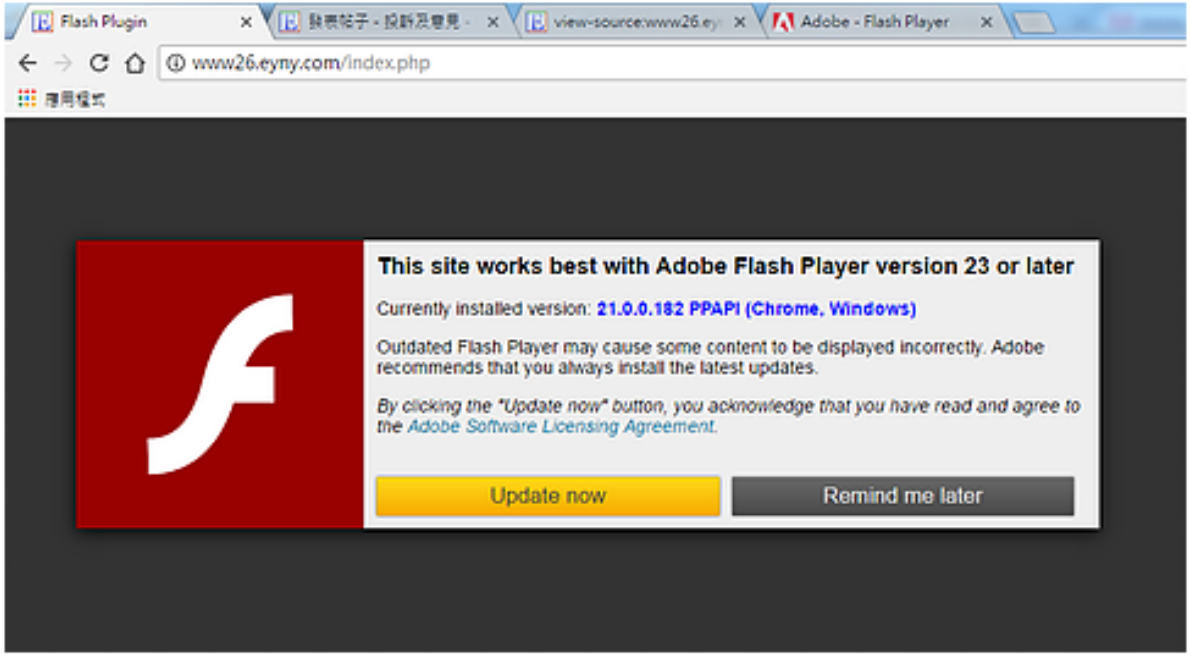
重大感染源

大喇喇租廣告


广告联盟网站
正常请求
广告数据
返回已被挂马的广
告链接，挂马站点
ip.u
.com.cn
某运营商
客户端
运营商
返回被特定劫持的内容
最终链接挂马站点
m
u.cn
正常请求数据
返回被随机插入的
内容，最终链接挂马
站点m
u.cn
某知名网游
浏览器等软件
挂马代码利用IE、flash漏洞进行
攻击，成功后下载病毒并运行
silence_eq005
2558.tmp
DeskHomePage
_179_1
EQ记事本
高强度加密用户机
器上文档、照片等
个人资料进行敲诈
自动安装皮皮资讯，键盘发声助
手，遇见爱美丽等多款软件，弹
出大量广告窗
drops.wooyun.org

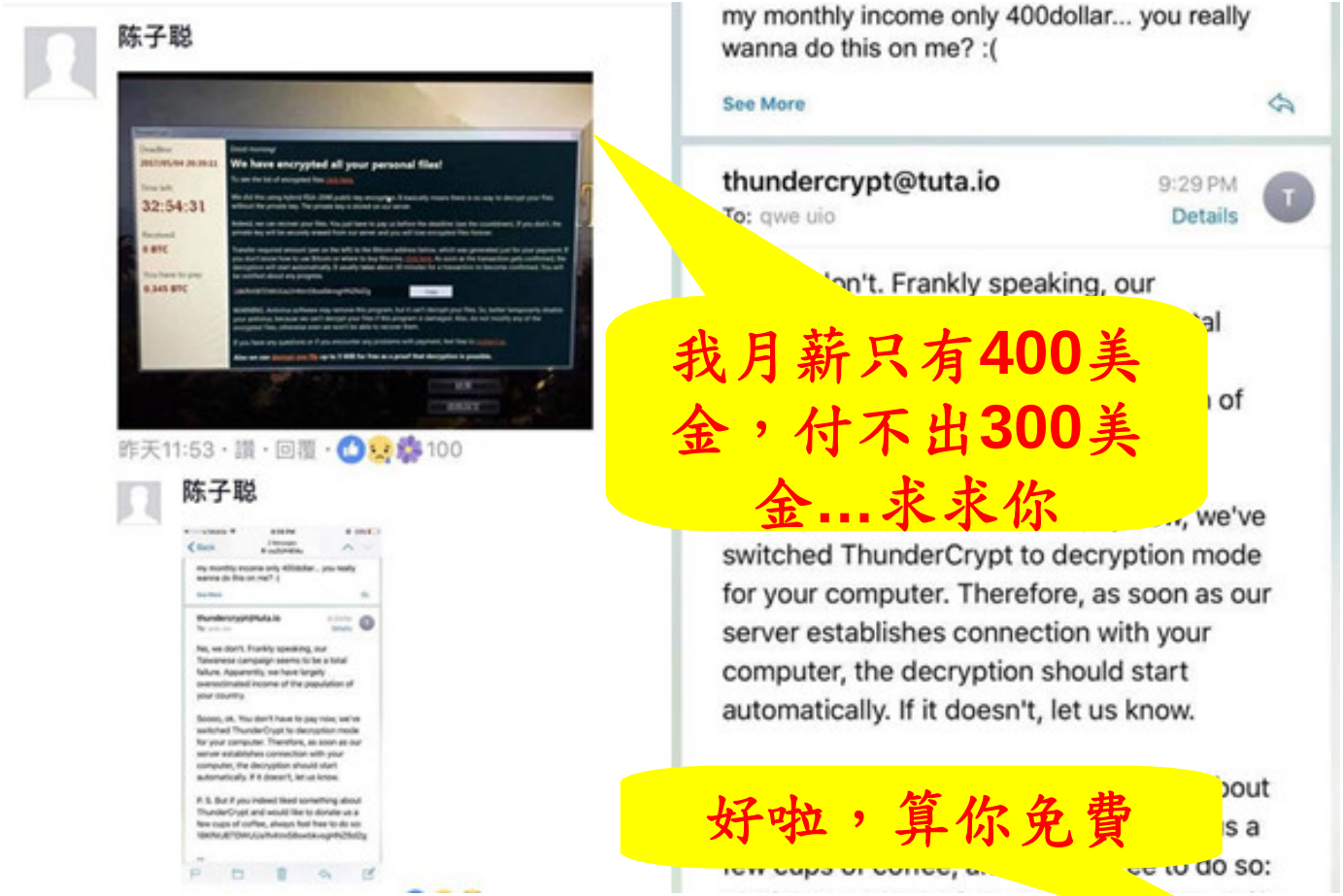
ThunderCrypt – 伊莉論壇

"目前所安裝的版本：21.0.0.182 PPAPI（Chrome，Windows），過期的Flash Player可能會導致某些內容不正確顯示， Adobe建議您始終安裝最新的更新。點擊"立即更新"按鈕，即表示您已閱讀並同意Adobe軟體許可協議。"



ThunderCrypt – 伊莉論壇

ThunderCrypt 客服信箱



ThunderCrypt 客服信箱

Yes, the screenshot with our message is genuine. It was all just a big accident. On the third day since the beginning of the campaign, we had a lot of encrypted computers, but no one paid us. And all that we got in our inbox were just a few messages asking for a lower price.

是的，這張截圖是真的。這其實是一個巨大的意外。在我們開始活動的第三天，我們成功加密了許多人的電腦檔案，但卻沒有人付錢給我們。僅有寥寥幾封信請求降低索取金額。

We thought that people in Taiwan must have set up some backups for their data or something like that. So, we decrypted files for free for those poor souls, who wrote the messages, and decided to give up the campaign. But soon we discovered a bug in our software, because of which our ransom note could not be displayed on most computers even though encryption stage was over.

我們以為台灣人有各種備份或其他相關的方案。所以我們替這幾個寄信來的可憐傢伙免費解鎖，並決定放棄這次的活動。但很快地我們發現了程式錯誤，造成我們的勒索訊息就算已經完成了加密，也沒有顯示在多數客戶的電腦上。

ThunderCrypt 客服信箱

Shortly after we became aware of this, we developed a patch that was deployed quite quickly thanks to our auto-upgrade system. That radically changed the state of affairs.

一發現這個問題，我們馬上做了更新，並藉由我們的自動更新系統，迅速地部署至多數客戶的電腦上。這從根本上改變了整個情況。

病毒的寫作流程、更新速度和客戶服務

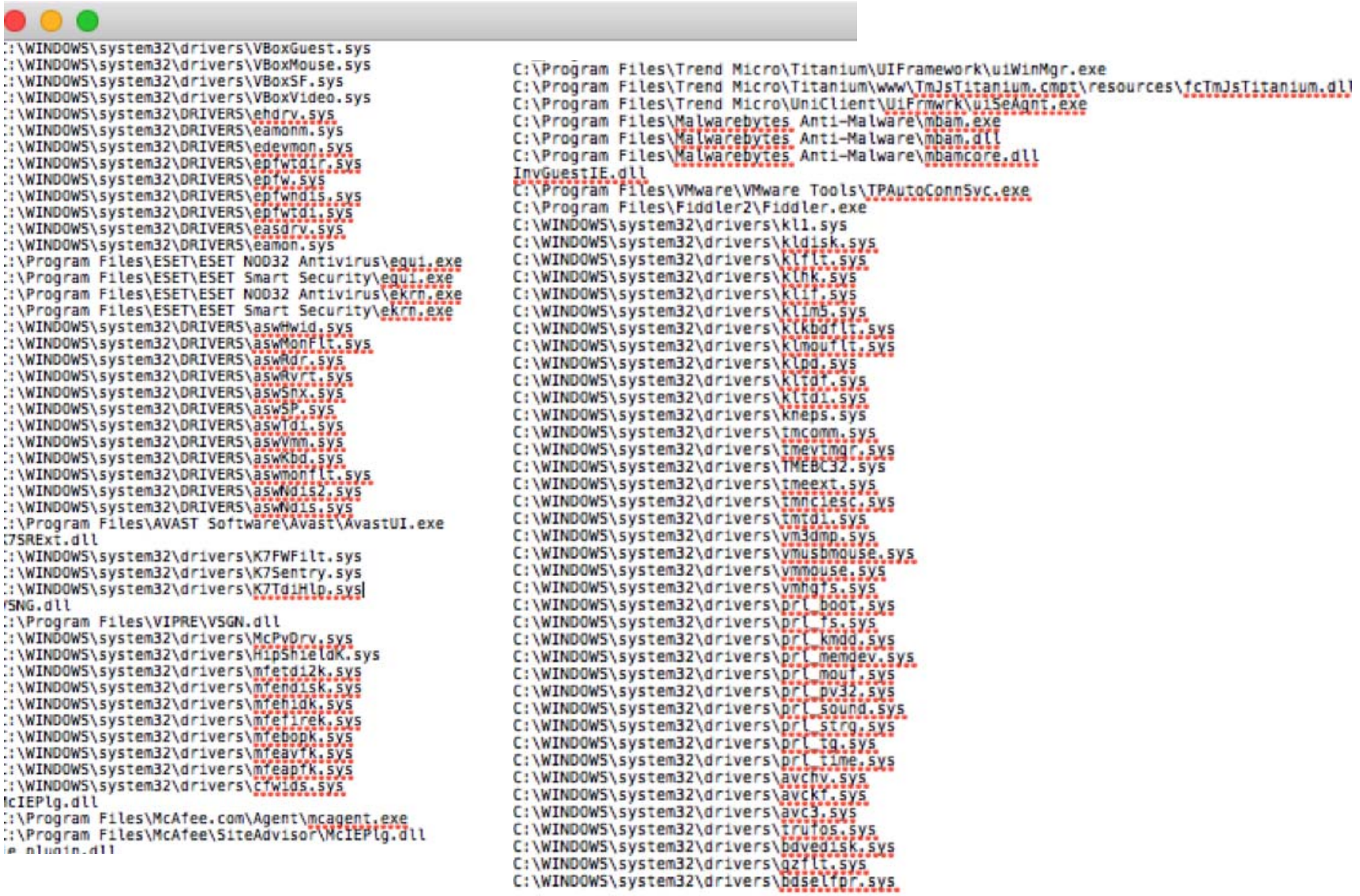
比正版軟體還好！

ThunderCrypt 客服信箱

ThunderCrypt 客服信箱

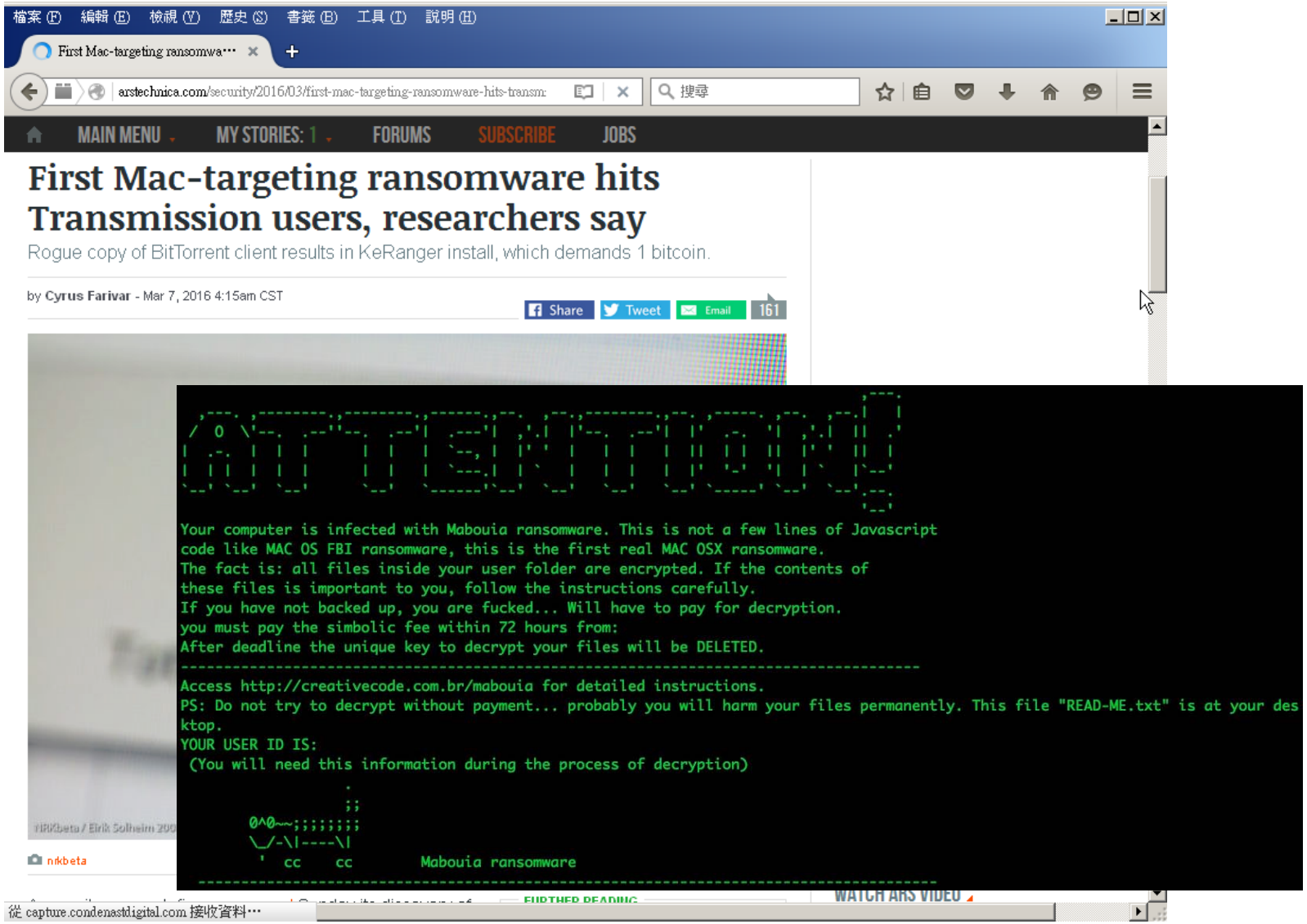
付款完成後，網友去信表示希望不要再攻擊他的電腦了，駭客回信說：「我們有一些保護機制確保已經中毒過的電腦不會再受到我們的攻擊，儘管如此，還是建議時常備份資料，網路上很危險的。」由於駭客的誠信取決於是否能夠取得贖金，因此大多數勒索病毒確實是會交還檔案，且不會重複攻擊（但誰知道他們會不會換個名字再來一次呢？）

先檢查受害者裝哪一種防毒？



```
:\WINDOWS\system32\drivers\VBoxGuest.sys
:\WINDOWS\system32\drivers\VBoxMouse.sys
:\WINDOWS\system32\drivers\VBoxSF.sys
:\WINDOWS\system32\drivers\VBoxVideo.sys
:\WINDOWS\system32\DRIVERS\ehdrv.sys
:\WINDOWS\system32\DRIVERS\eamonm.sys
:\WINDOWS\system32\DRIVERS\edevmon.sys
:\WINDOWS\system32\DRIVERS\eftwtdir.sys
:\WINDOWS\system32\DRIVERS\eftw.sys
:\WINDOWS\system32\DRIVERS\eftwmdis.sys
:\WINDOWS\system32\DRIVERS\eftwtdi.sys
:\WINDOWS\system32\DRIVERS\easdrv.sys
:\WINDOWS\system32\DRIVERS\eamon.sys
:\Program Files\ESET\ESET NOD32 Antivirus\egui.exe
:\Program Files\ESET\ESET Smart Security\egui.exe
:\Program Files\ESET\ESET NOD32 Antivirus\ekrn.exe
:\Program Files\ESET\ESET Smart Security\ekrn.exe
:\WINDOWS\system32\DRIVERS\aswHwid.sys
:\WINDOWS\system32\DRIVERS\aswMonFlt.sys
:\WINDOWS\system32\DRIVERS\aswMdr.sys
:\WINDOWS\system32\DRIVERS\aswRvrt.sys
:\WINDOWS\system32\DRIVERS\aswSnx.sys
:\WINDOWS\system32\DRIVERS\aswSP.sys
:\WINDOWS\system32\DRIVERS\aswTdi.sys
:\WINDOWS\system32\DRIVERS\aswVmm.sys
:\WINDOWS\system32\DRIVERS\aswKbd.sys
:\WINDOWS\system32\DRIVERS\aswmonflt.sys
:\WINDOWS\system32\DRIVERS\aswNdis2.sys
:\WINDOWS\system32\DRIVERS\aswNdis.sys
:\Program Files\AVAST Software\Avast\AvastUI.exe
7SRExt.dll
:\WINDOWS\system32\drivers\K7FWFilt.sys
:\WINDOWS\system32\drivers\K7Sentry.sys
:\WINDOWS\system32\drivers\K7TdiHlp.sys
VSNG.dll
:\Program Files\VIPRE\VSGN.dll
:\WINDOWS\system32\drivers\McPvDrv.sys
:\WINDOWS\system32\drivers\HipShieldK.sys
:\WINDOWS\system32\drivers\mfetdi2k.sys
:\WINDOWS\system32\drivers\mfendisk.sys
:\WINDOWS\system32\drivers\mfehidk.sys
:\WINDOWS\system32\drivers\mfetirek.sys
:\WINDOWS\system32\drivers\mfebopk.sys
:\WINDOWS\system32\drivers\mfeavfk.sys
:\WINDOWS\system32\drivers\mfeapfk.sys
:\WINDOWS\system32\drivers\cfwids.sys
McIEPlg.dll
:\Program Files\McAfee.com\Agent\mcagent.exe
:\Program Files\McAfee\SiteAdvisor\McIEPlg.dll
e_plugin.dll

C:\Program Files\Trend Micro\Titanium\UIFramework\uiWinMgr.exe
C:\Program Files\Trend Micro\Titanium\www\TmJsTitanium.cmpt\resources\fcTmJsTitanium.dll
C:\Program Files\Trend Micro\UniClient\UiFrmwrk\uiSeAgnt.exe
C:\Program Files\Malwarebytes Anti-Malware\mbam.exe
C:\Program Files\Malwarebytes Anti-Malware\mbam.dll
C:\Program Files\Malwarebytes Anti-Malware\mbamcore.dll
InvGuestIE.dll
C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
C:\Program Files\Fiddler2\Fiddler.exe
C:\WINDOWS\system32\drivers\kl1.sys
C:\WINDOWS\system32\drivers\kldisk.sys
C:\WINDOWS\system32\drivers\klflt.sys
C:\WINDOWS\system32\drivers\klhk.sys
C:\WINDOWS\system32\drivers\klif.sys
C:\WINDOWS\system32\drivers\klim5.sys
C:\WINDOWS\system32\drivers\klkbdflt.sys
C:\WINDOWS\system32\drivers\klmouflt.sys
C:\WINDOWS\system32\drivers\klpd.sys
C:\WINDOWS\system32\drivers\kltdf.sys
C:\WINDOWS\system32\drivers\kltdi.sys
C:\WINDOWS\system32\drivers\kneps.sys
C:\WINDOWS\system32\drivers\tmcomm.sys
C:\WINDOWS\system32\drivers\tmevtmgr.sys
C:\WINDOWS\system32\drivers\TMEBC32.sys
C:\WINDOWS\system32\drivers\tmeext.sys
C:\WINDOWS\system32\drivers\tmnciesc.sys
C:\WINDOWS\system32\drivers\tmtdi.sys
C:\WINDOWS\system32\drivers\vm3dmp.sys
C:\WINDOWS\system32\drivers\vmusbmouse.sys
C:\WINDOWS\system32\drivers\vmmouse.sys
C:\WINDOWS\system32\drivers\vmhgfs.sys
C:\WINDOWS\system32\drivers\prl_boot.sys
C:\WINDOWS\system32\drivers\prl_fs.sys
C:\WINDOWS\system32\drivers\prl_kmdd.sys
C:\WINDOWS\system32\drivers\prl_memdev.sys
C:\WINDOWS\system32\drivers\prl_mouf.sys
C:\WINDOWS\system32\drivers\prl_pv32.sys
C:\WINDOWS\system32\drivers\prl_sound.sys
C:\WINDOWS\system32\drivers\prl_strg.sys
C:\WINDOWS\system32\drivers\prl_tg.sys
C:\WINDOWS\system32\drivers\prl_time.sys
C:\WINDOWS\system32\drivers\avchv.sys
C:\WINDOWS\system32\drivers\avckf.sys
C:\WINDOWS\system32\drivers\avc3.sys
C:\WINDOWS\system32\drivers\trufos.sys
C:\WINDOWS\system32\drivers\bdvedisk.sys
C:\WINDOWS\system32\drivers\gzflt.sys
C:\WINDOWS\system32\drivers\bdselfpr.sys
```

MAC病毒


檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
First Mac-targeting ransomwa…
arstechnica.com/security/2016/03/first-mac-targeting-ransomware-hits-transm
搜尋
MAIN MENU
MY STORIES: 1
FORUMS
SUBSCRIBE
JOBS
First Mac-targeting ransomware hits Transmission users, researchers say
Rogue copy of BitTorrent client results in KeRanger install, which demands 1 bitcoin.
by Cyrus Farivar - Mar 7, 2016 4:15am CST
Share
Tweet
Email
161
Your computer is infected with Mabouia ransomware. This is not a few lines of Javascript
code like MAC OS FBI ransomware, this is the first real MAC OSX ransomware.
The fact is: all files inside your user folder are encrypted. If the contents of
these files is important to you, follow the instructions carefully.
If you have not backed up, you are fucked... Will have to pay for decryption.
you must pay the simbolic fee within 72 hours from:
After deadline the unique key to decrypt your files will be DELETED.
Access http://creativecode.com.br/mabouia for detailed instructions.
PS: Do not try to decrypt without payment... probably you will harm your files permanently. This file "READ-ME.txt" is at your des
ktop.
YOUR USER ID IS:
(You will need this information during the process of decryption)
Mabouia ransomware
nrkbeta
從 capture.condenastdigital.com 接收資料…

專打NAS

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

勒索軟體有新變種，鎖定…

www.ithome.com.tw/news/89871

搜尋

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群 - 搜尋

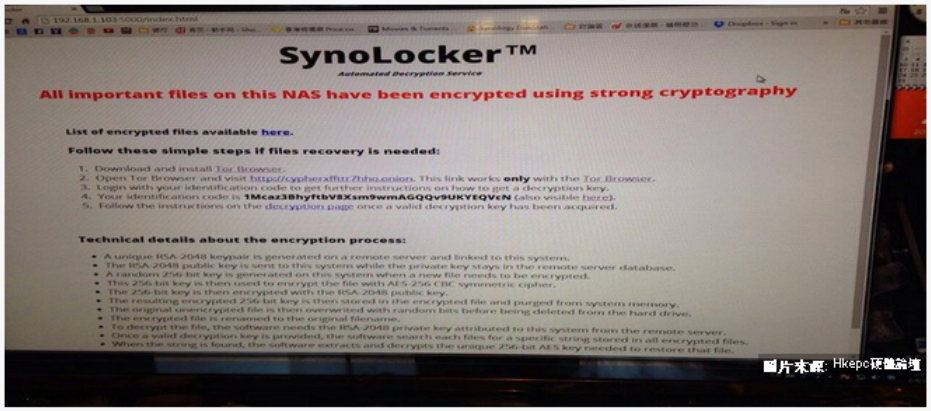
新聞

勒索軟體有新變種，鎖定群暉NAS綁架網路硬碟資料

近日，勒索軟體又出現新變種的SynoLocker，改鎖定以網路儲存硬碟NAS爲勒索對象，臺灣群暉科技（Synology）旗下的NAS硬碟也深受其害，接連在國外出現多起贖金勒索案例，造成Synology NAS用戶硬碟重要檔案文件加密無法開啓。群暉官方也表示，昨日已接獲使用者通報，目前正在清查是否有產品漏洞，最快今日會有結果公布。

文/ 余至浩 | 2014-08-04 發表

按讚加入iThome粉絲團 2.3萬 分享 2,550 G+1 63



圖片來源：Hkepc硬體論壇

群暉科技官方最新公告發布應急方案請參考《臺灣出現NAS勒索軟體災情，群暉證實舊版DSM漏洞釀災》

去年底一款勒索軟體CryptoLocker大舉入侵企業及個人電腦，悄悄地將受害者電腦裏的檔案加密，讓使用者無法開啟檔案，也沒辦法破解加

利用系統未更新的漏洞

MS17-010 (2017/03月釋出)

Microsoft 資訊安全公告 MS17-010 - 重大

Microsoft Windows SMB 伺服器的安全性更新 (4013389)

發行日期：2017 年 3 月 14 日

版本：1.0

本頁內容

提要

此安全性更新可解決 Microsoft Windows 中的弱點。如果攻擊者傳送蓄意製作的訊息到 Windows SMBv1 伺服器，最嚴重的弱點可能會允許遠端執行程式碼。

對於所有受支援版本的 Microsoft Windows，此安全性更新的等級為「重大」。如需詳細資訊，請參閱 < 受影響的軟體和弱點嚴重性等級 > 一節。

此安全性更新會更正 SMBv1 處理蓄意製作之要求的方式，藉此解決弱點。

如需有關弱點的詳細資訊，請參閱 < 弱點資訊 > 一節。

如需有關此更新的詳細資訊，請參閱 Microsoft 知識庫文章 4013389。

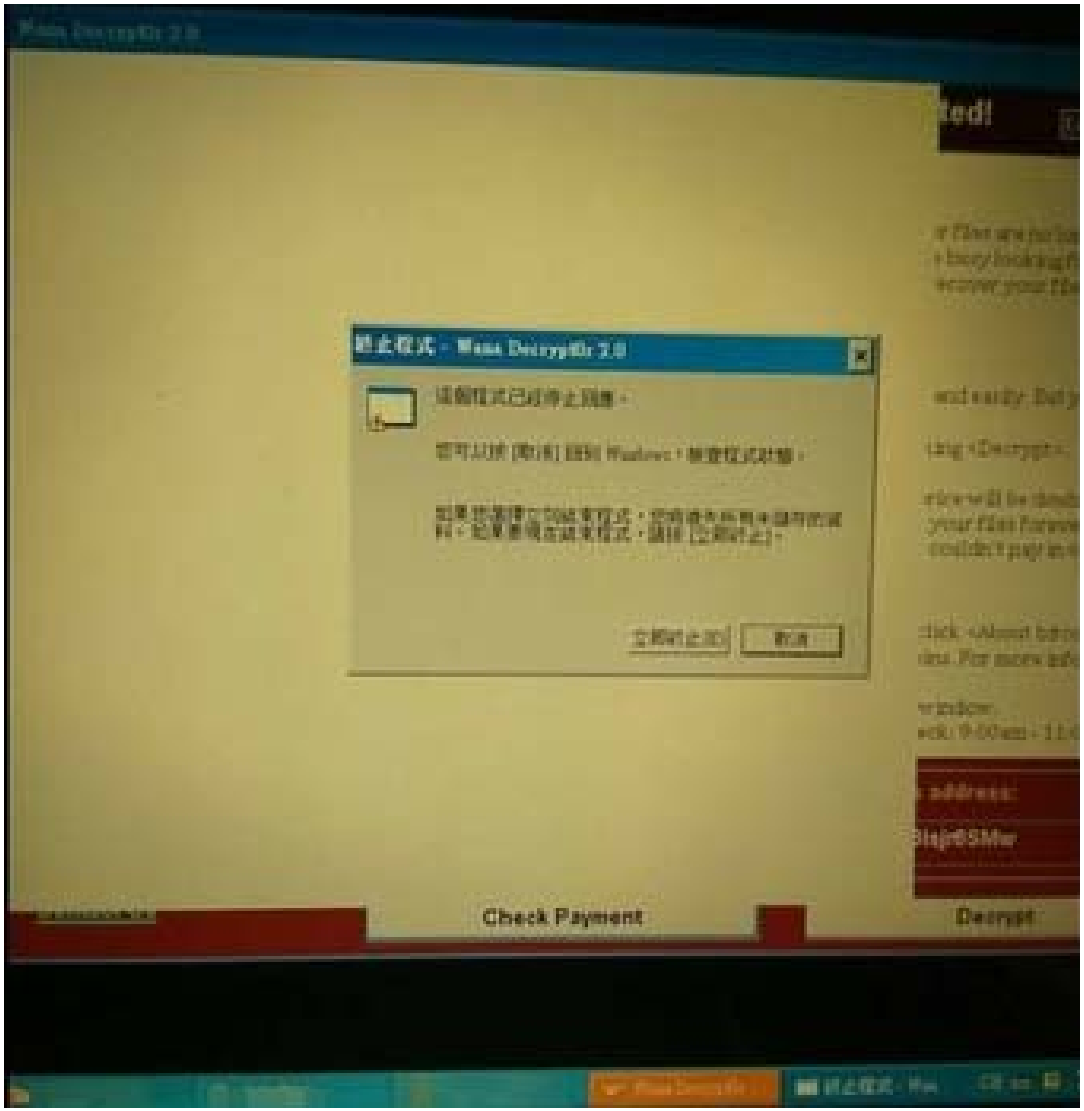
WannaCrypt 2.0

WannaCrypt 2.0

WannaCrypt 2.0

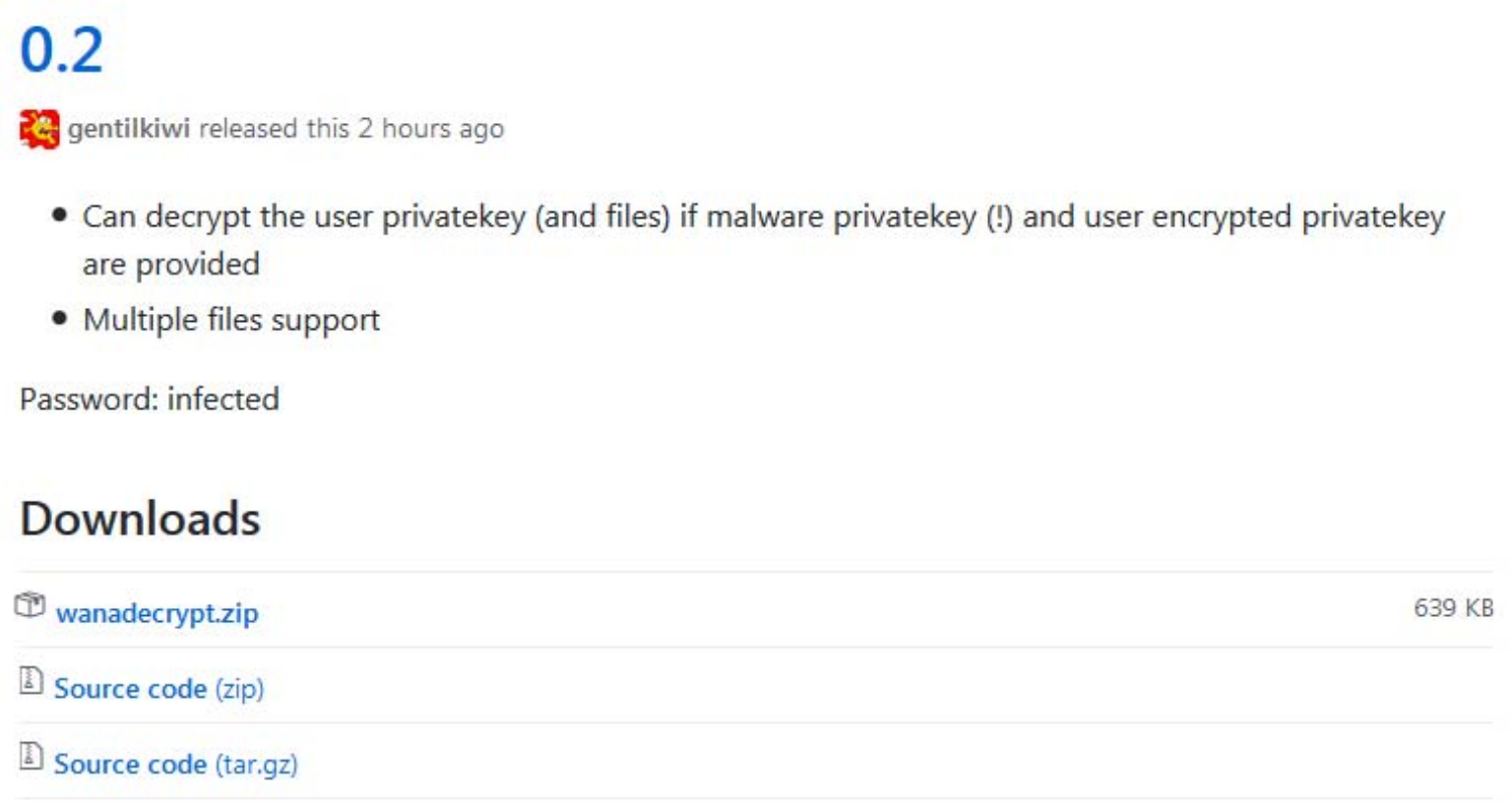
注意
這支病毒沒良心，
根本沒有作解密機制

逃過一劫的 Windows XP



WannaCrypt 解密工具（部分）

- https://github.com/gentilkiwi/wanadecrypt/releases



綁架網站

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

Hackers holding websites to r··· | Atelier Wini: [資安通知] 預···

www.theguardian.com/technology/2015/ ransom website

Hackers holding websites to ransom by switching their encryption keys

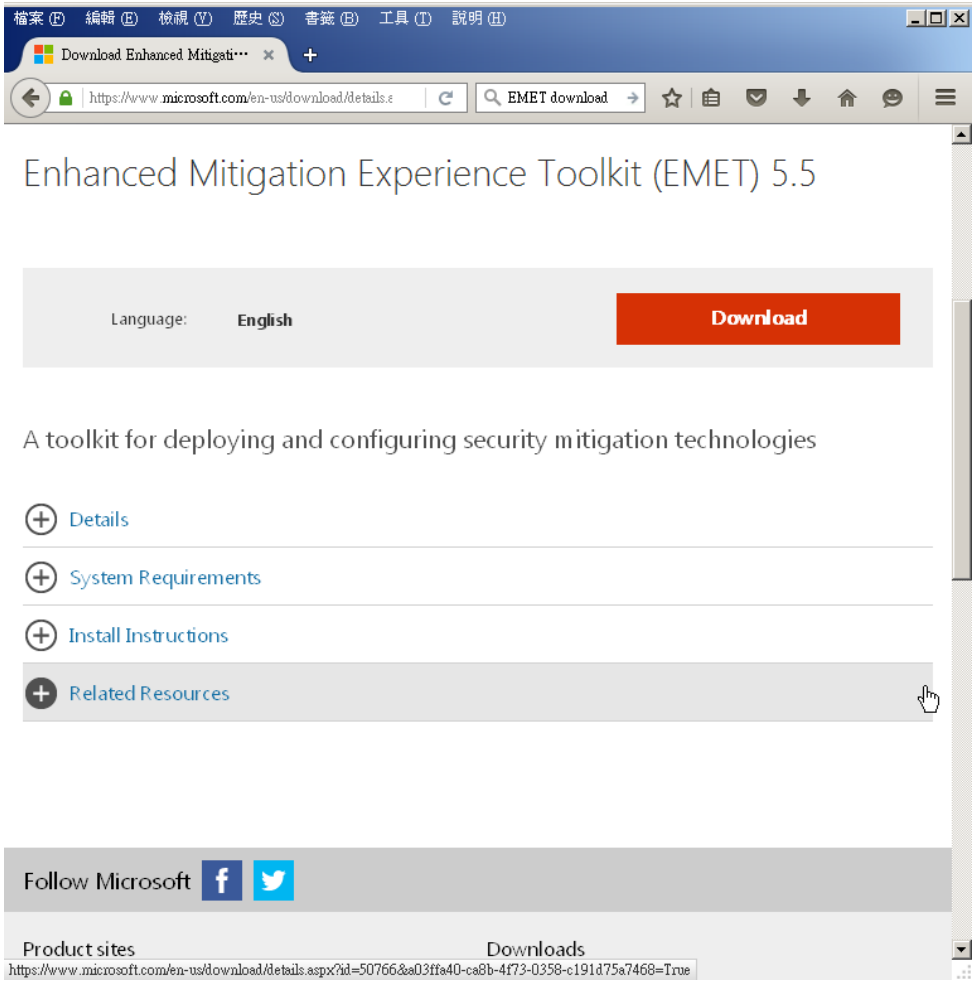
Websites taken offline in new attack, which sees hackers change codes to permanently lock owners out unless they pay a ransom

Ransomware has moved to the web targeting businesses with encyption attacks. Photograph: LJSphotography / Alamy/Alamy

Samuel Gibbs

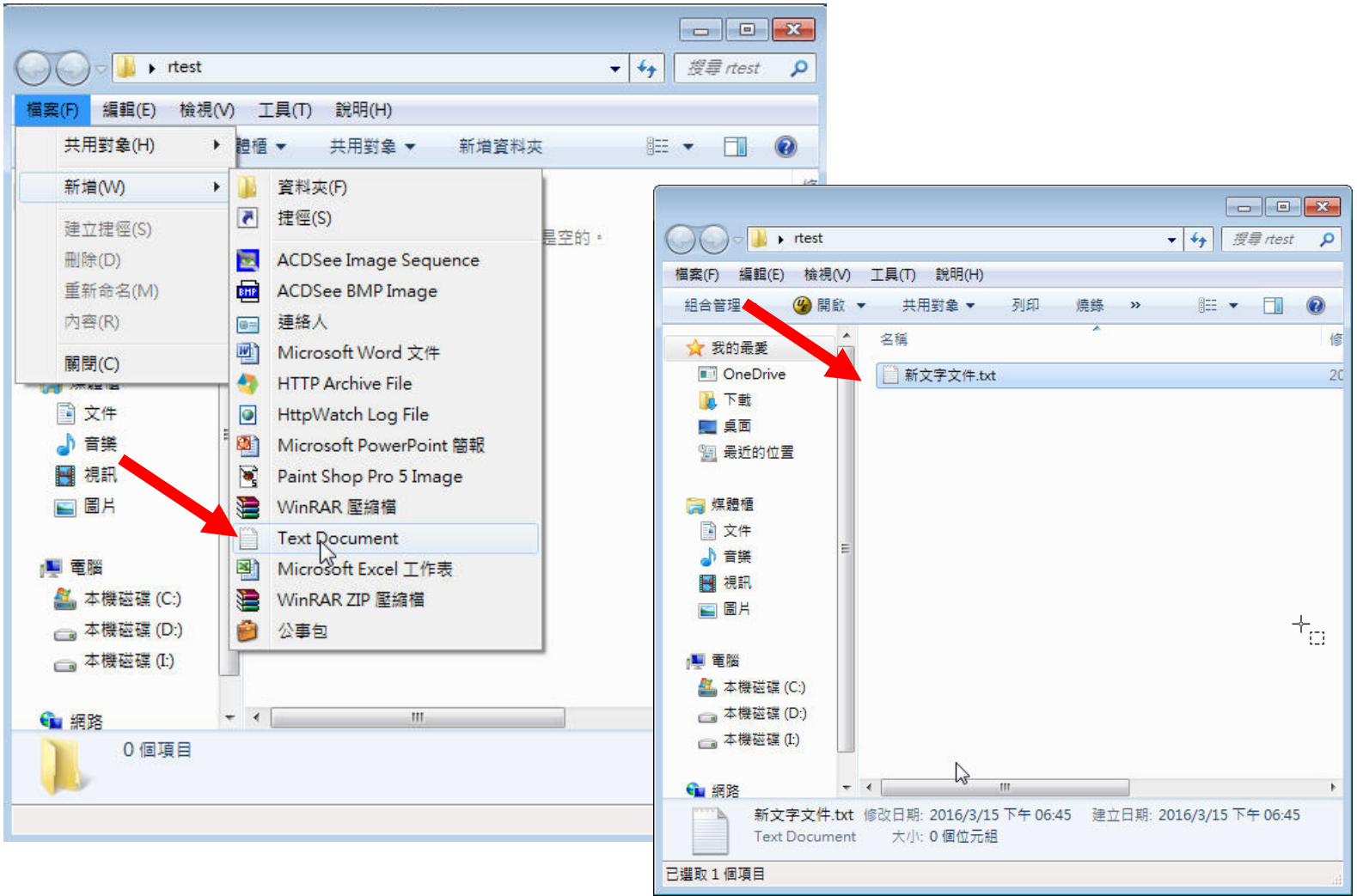
勒索防護—Windows防護

- Microsoft EMET

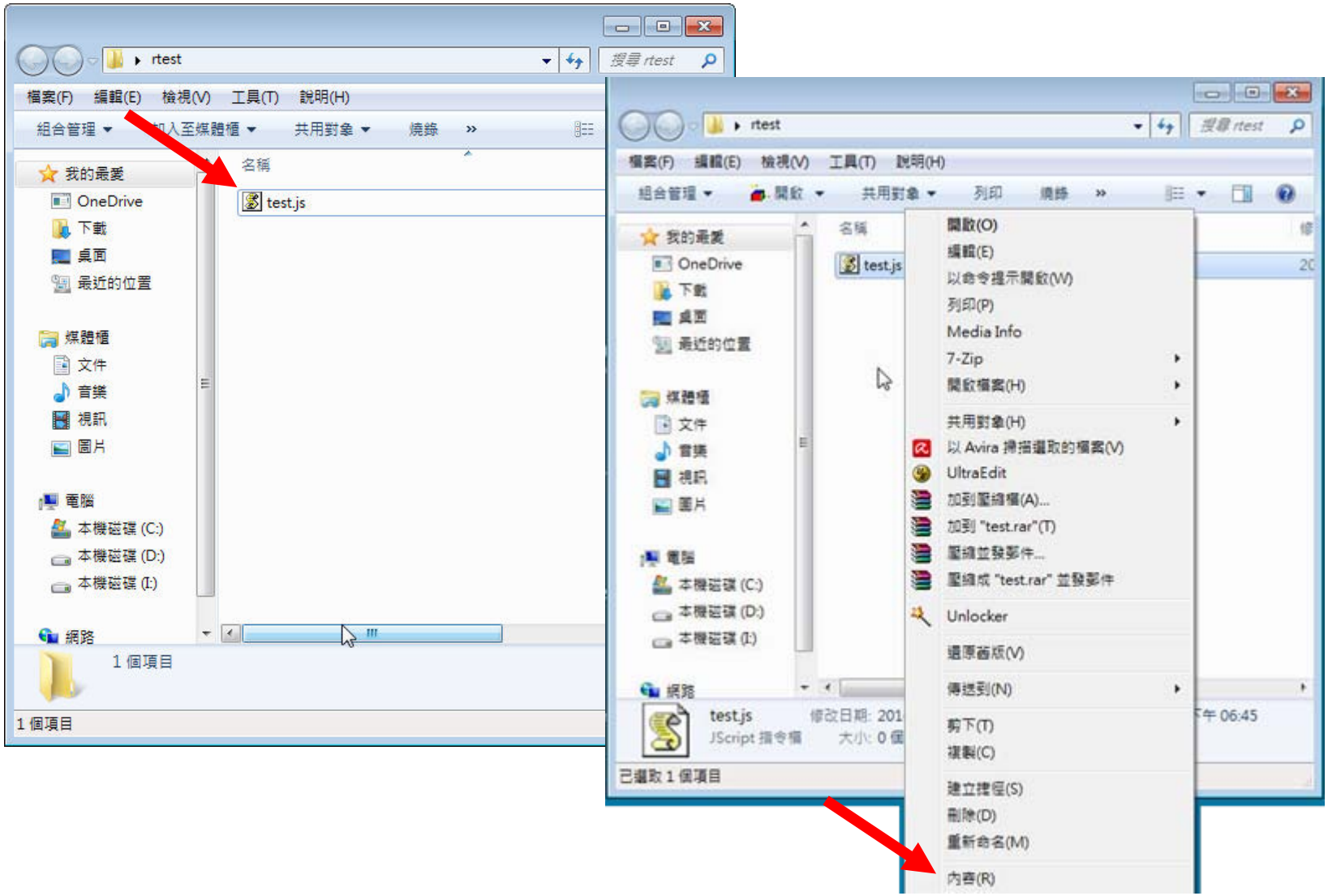


勒索防護—Windows防護

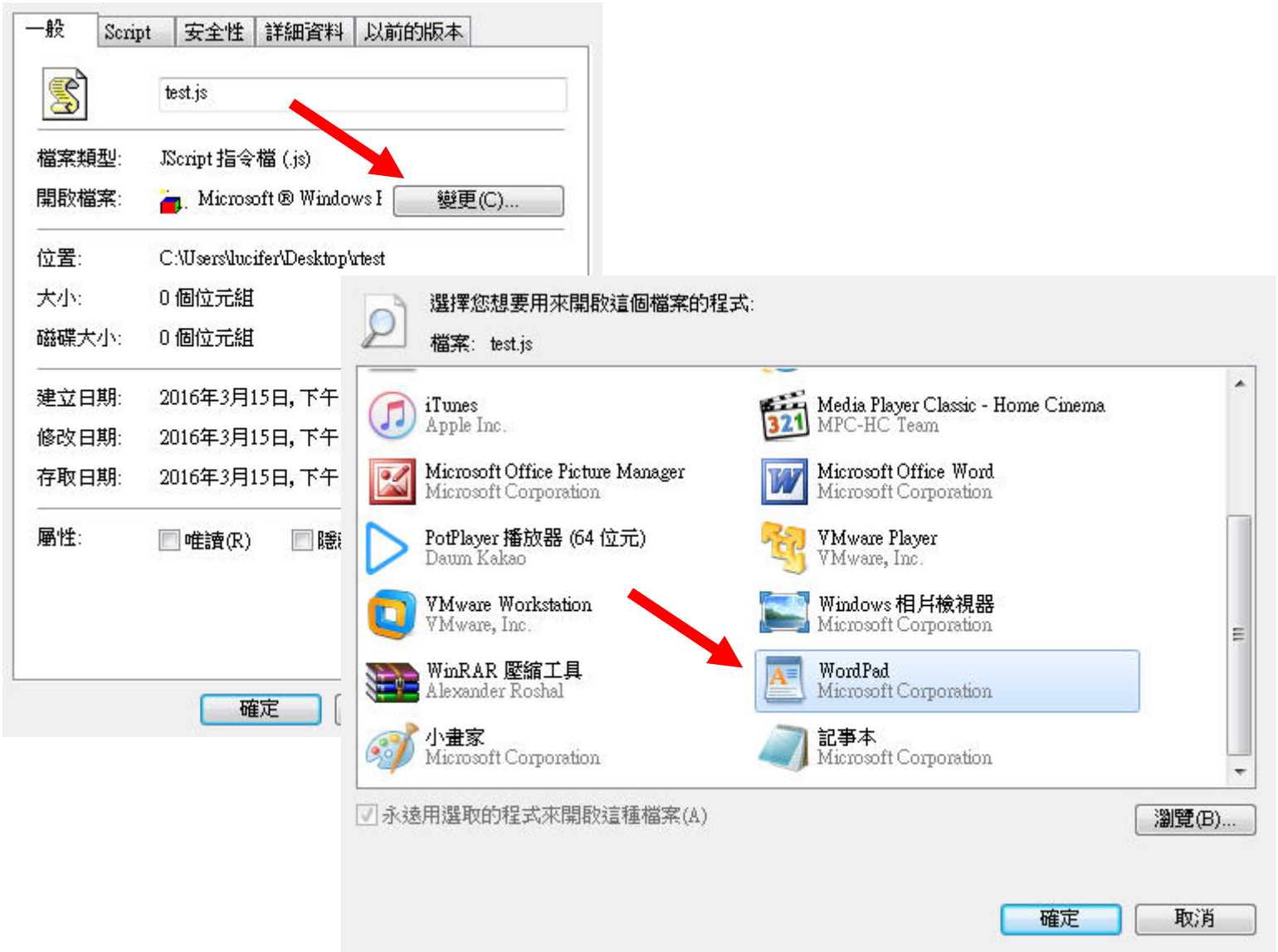
- 不直接開啟js/jse



勒索防護—Windows防護

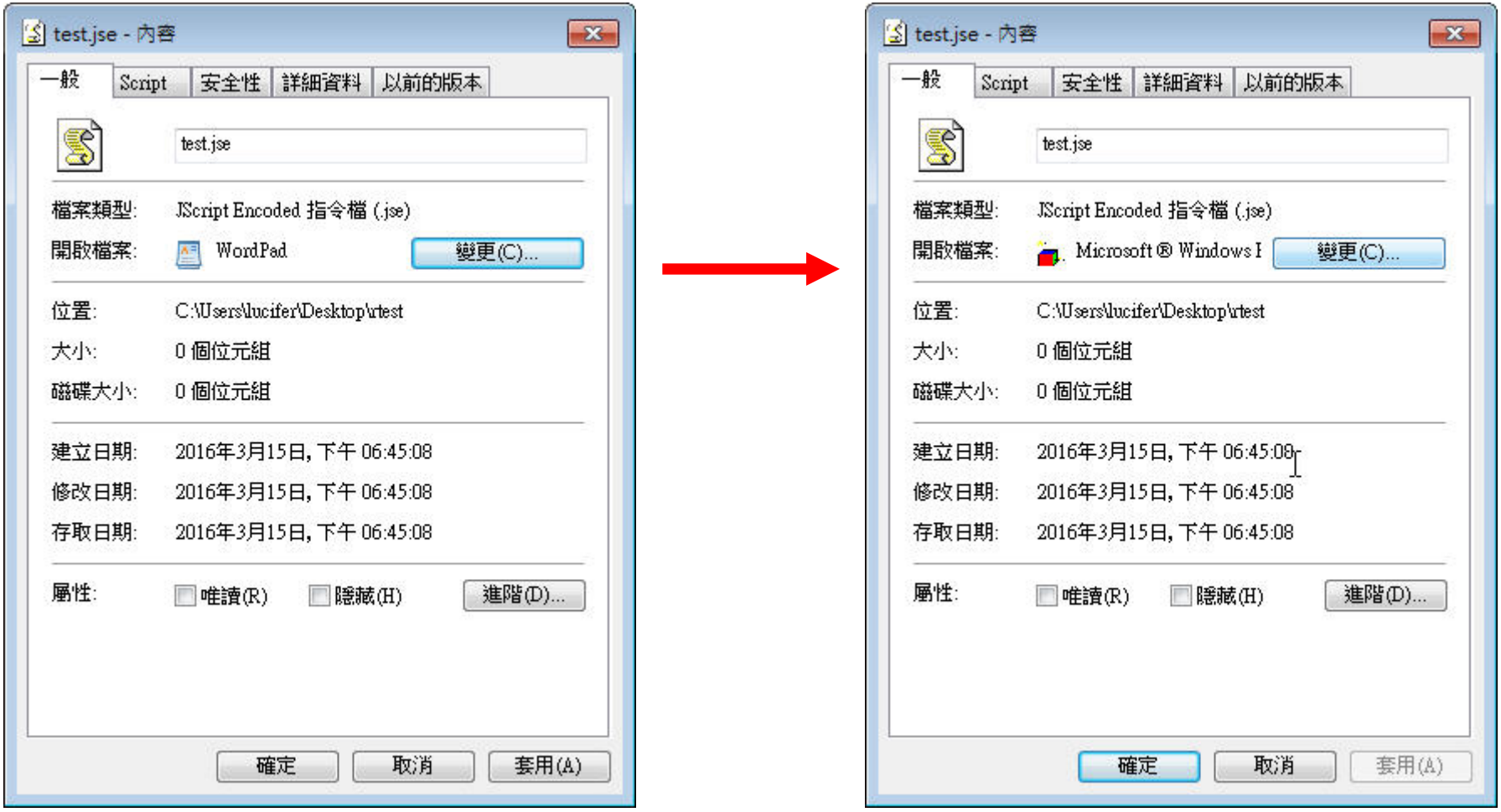


勒索防護—Windows防護



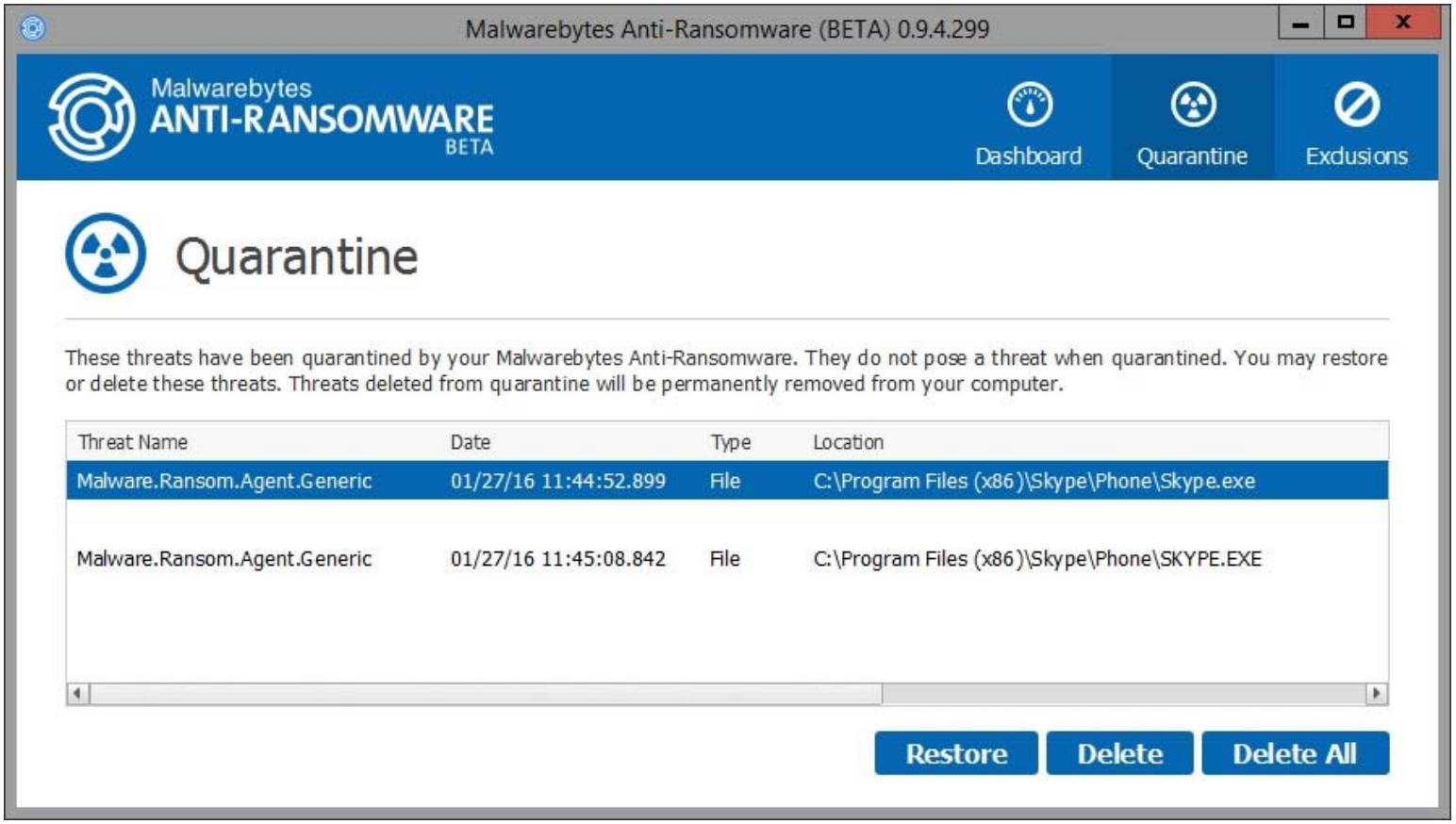
勒索防護—Windows防護

勒索防護—Windows防護



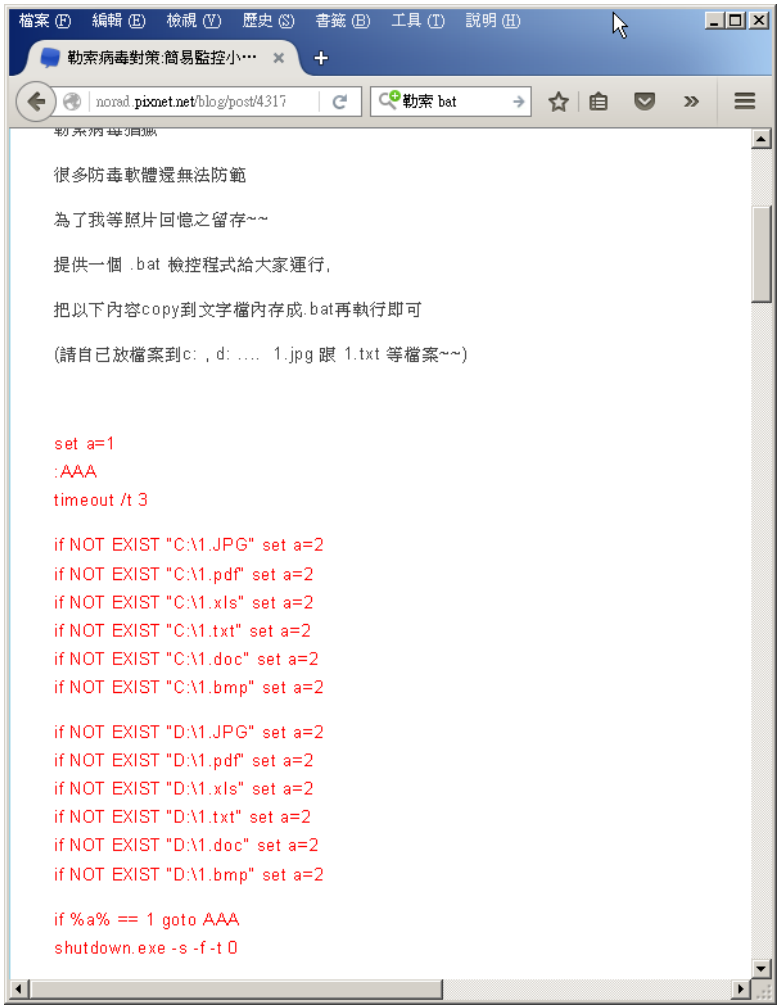
勒索防護—偵測加密

- Malwarebytes Anti-Ransomware



勒索防護—偵測加密

- 勒索病毒對策:簡易監控小腳本



已經中了怎麼辦？

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

中了勒索軟體該怎麼辦？F…

www.ithome.com.tw/news/99586

CIS 嘲勒索

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群 搜尋

新聞

中了勒索軟體該怎麼辦？FBI回答：解密資料的最快方法就是花錢消災！

美國FBI探員Joseph Bonavolonta近日在波士頓舉行的網路安全高峰會上表示，雖然鼓勵受害者向FBI報案，但FBI無法替受害者取回加密的資料，最簡單的方式就是支付贖金。還說勒索軟體賺很多錢的原因就是絕大多數的人都選擇了支付贖金，而且可能因爲這樣，駭客也不會要求太高的贖金，同時也會履行承諾幫受害者解密。

文/ 陳曉莉 | 2015-10-28 發表

按讚加入iThome粉絲團 2.3萬 分享 1,249 G+1 19

根據Security Ledger的報導，美國聯邦調查局（FBI）探員Joseph Bonavolonta近日在波士頓舉行的網路安全高峰會上表示，當他們遇到有人投訴遭到勒索軟體的攻擊時，經常建議受害者支付贖金以取回被駭客加密的檔案，此語一出即惹來了爭議。

已經中了怎麼辦？—破解特定病毒

- 趨勢科技勒索病毒檔案解密工具
  - http://esupport.trendmicro.com/solution/zh-TW/1114221.aspx

勒索病毒種類	被加密後的檔案名稱及副檔名格式
CryptXXX V1, V2, V3*	{原始檔案名稱}.crypt
TeslaCrypt V1**	{原始檔案名稱}.ECC
TeslaCrypt V2**	{原始檔案名稱}.VVV 或 CCC 或 ZZZ 或 AAA 或 ABC 或 XYZ
TeslaCrypt V3	{原始檔案名稱}.XXX 或 TTT 或 MP3 或 MICRO
TeslaCrypt V4	檔名及副檔名均未被變更
SNSLocker	{原始檔案名稱}.RSNSLocked
AutoLocky	{原始檔案名稱}.locky

已經中了怎麼辦？—破解特定病毒

- https://noransom.kaspersky.com/

豬隊友的故事

公司要倒了嗎…
因為會計部的堅持erp伺服器在他們單位
(他們認為他們是完全獨立單位)
也有會計部資訊組
會資組今天上午erp當掉打來資訊部詢

他用伺服器update 順便 check mail
運氣很好，免費中獎 iphone 6S
點了以後沒有反應
重開機發現資料都被加密了……
中了cryptolocker
問我們怎麼辦？！拜托就解

這位同事可以打包了吧？
我也可以找新公司了吧？
別問我為什麼沒有防毒

他們家不歸我們家管
就讓你獨立吧!
豬隊友

ERP死亡的第二天：
昏迷指數3大概能用植物人來形容這台伺服器。今天廠商來了速手無徹。

各位關心的"備份資料"有辦法吧！

來！我說給你聽豬隊友怎麼處理的
當時：

1.他買了一顆硬碟裝在伺服器上
(不是一組所以沒有RAID)
2.建立了新資料夾
3.新增網路磁碟指向資料夾
4.成功騙過ERP防護裝置
有備份資料！
購置系統時的全新光碟！

資訊、會計一邊一國。
你的麻煩別來找我們。
公司今天一整天吃飽沒事做。
喔、你知道嗎、倉儲無法下班了
因為盤點資料也全沒了!
恐怕要點到死
提辭呈換新工作比較快。

會計部主任說：這套ERP太爛我們要跟你們解約、早知道當年就買SAP一定沒問題。

豬隊友的故事

ERP 死亡第三天
【豬隊友☆ERP☆Iphone6s☆cryptolocker】
今天資訊部門為了加班費、拯救世界願意回去上班再補休一天
ERP買了很多模組、所以現在打卡機也無法打卡、公司呈現植物人狀態。

小弟聽會計師說年底要結帳、月底也要結帳、我不會會計不過聽起來蠻嚴重的。

會計部會了讓員工安心
公告：由於本部升級、ERP、等系統暫停使用。週一起請同仁在原單位簽到及簽退。會計部OOO主任敬上。(掩蓋完畢)

大多員工還稿不清楚發生了什麼事情(只有各主任知道)、週一總經理、董事長要開會瞭解當機情況、評估緊急採購新設備來升級。

今天拉了兩台普通PC架了臨時系統、供補資料大戰、我下班！

ERP Day 4 Part 1
【豬會計部、會計資訊組、掩蓋、資訊部的正義】

在10點開會以前、資訊部開了個小會
主任說大家最近很有空、因為有人出包了。
我朋友這邊有些缺額有興趣的自己跟我說。
要推薦函的也跟我說一定寫正面的！
大家要有心裡準備、我也可能位置不保了。
（超感動 要落淚了）

(節錄重點)
會主：報告、各位長官這次我們ERP系統資料被加密所以系統產生當機
總經理：很好阿！加密才安全、是加密所以電腦跑不動嗎，需要多少預算？
會主：因為廠商建議我們加密、結果因為設備老舊所以意外的失敗了！
(ME: WHAT THE FUCK?!)

豬隊友的故事

ERP DAY 4 Part 2
總經理：你們沒通知資訊部嗎？
資主：有、我們當下協助處理但
[redacted]
你們資訊組打來說中毒尋求協助。檔案遭惡意加密、因為O姓員工….付了贖金也不一定能解密、只能全部格式化。

會主：資訊組、你當初不是這樣跟我會報的！

人資：打卡紀錄怎麼辦？加班時數怎麼算？薪水怎麼發？

業務：顧客都打來問我們現在要怎麼報價？

倉儲：無日無夜的重新盤點了、你麼這是在怎樣阿！

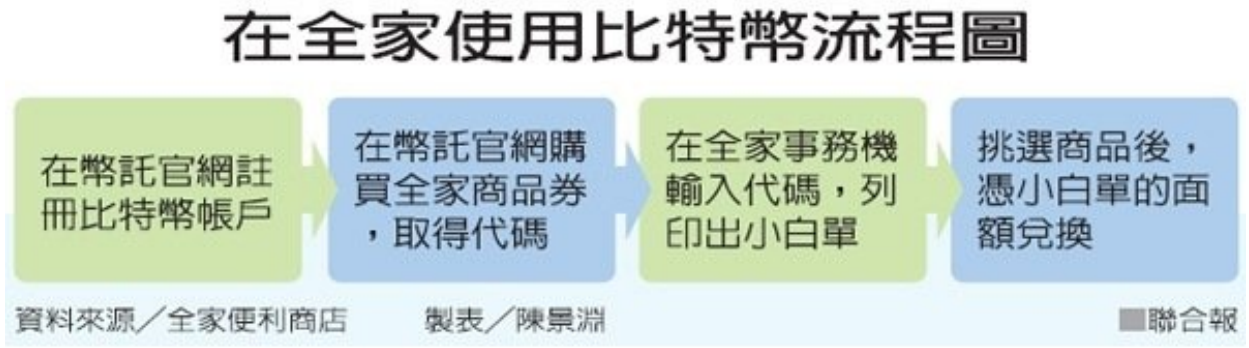
資主：我們現在提供兩台電腦作為資料補登、而且會計主任你都知情、有監視器畫面證明你在現場、我可以親自作證。

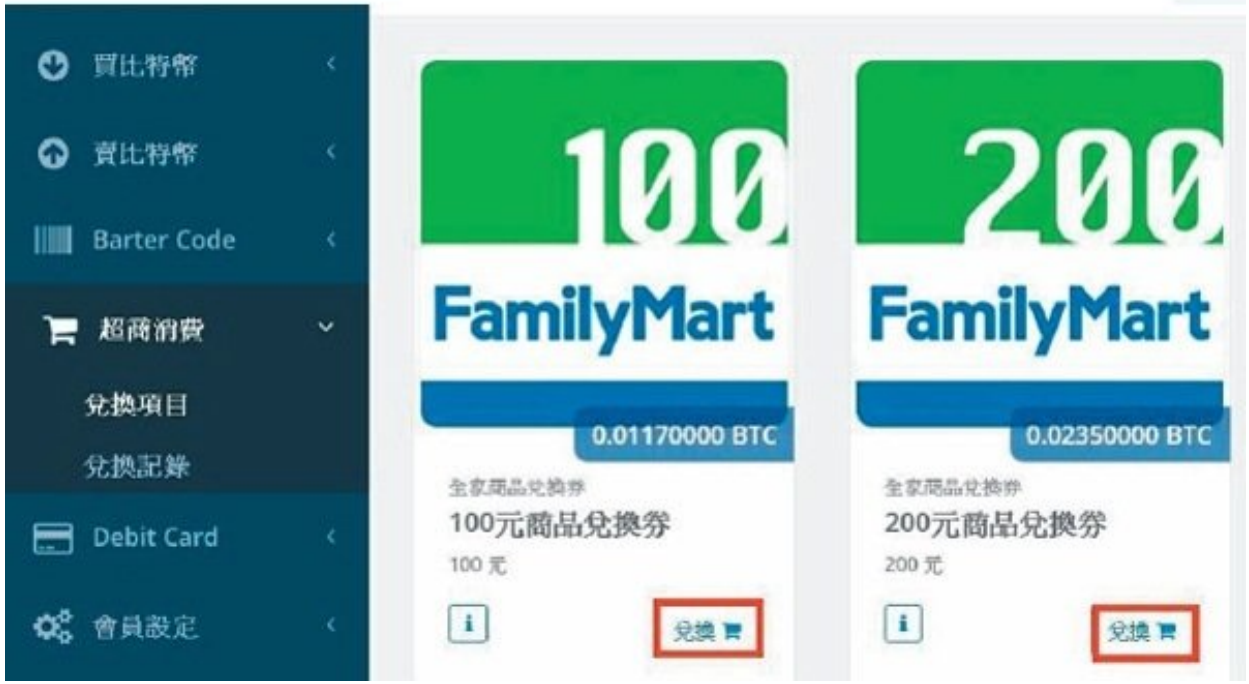
(繼續吵架)

ERP Day 4 Part3
董事長
1.會計部主任調離主管現職、副主任代理
2.會計資訊組組長、x調離現職、整組重編
3.你們三個自己應該心裡有數、我會請律師處理
3.下個月薪水照發、這個月誰有加班自己去人資部簽名
4.月底公佈在一樓誰亂簽、被自己單位同事揭發沒有信用的人我們不需要
5.伺服器搬回資訊部機房、由資訊部統一管理

接下來就是恢復期也沒什麼好收看了？
公司有列印習慣與邊冊、所以資料只差一週
設定全要重來真的是哇靠
討論後決定格式化、全新重來也不錯
只補2015資料其他的再找時間補打、會計年底結帳最重要
資訊主任怕揭發遇不測
以上為屬事實位於台北市
資安教育不能等
END

購買比特幣


在全家使用比特幣流程圖
在幣託官網註冊比特幣帳戶
在幣託官網購買全家商品券，取得代碼
在全家事務機輸入代碼，列印出小白單
挑選商品後，憑小白單的面額兌換
資料來源／全家便利商店
製表／陳景淵
聯合報


買比特幣
賣比特幣
Barter Code
超商消費
兌換項目
兌換記錄
Debit Card
會員設定
100
FamilyMart
0.01170000 BTC
全家商品兌換券
100元商品兌換券
100 元
兌換
200
FamilyMart
0.02350000 BTC
全家商品兌換券
200元商品兌換券
200 元
兌換

問題與討論