南投縣教育網路中心

資安防護種子教師培訓研習課程

雲端應用與安全

麟瑞科技

蔡和燁

Solutions

系統整合、資訊服務的第一選擇

Services

Agenda

1. 關於雲端服務
2. 生活中的雲端科技
3. 駭客漫步在雲端
4. 雲端使用安全

SANS CEO:走資安要學中文

Advice to Security Pros: Learn Chinese
Career Insights from Stephen Northcutt, CEO of SANS
Upasana Gupta, Contributing Editor
September 14, 2010

Stephen Northcutt, CEO of SANS Technology Institute, has a piece of advice for up and coming security professionals. "Learn Chinese; you are going to need it."

Further, Northcutt advises, "Learn and live by the security axiom: protection is ideal, but detection is a must."

Source: bankinfosecurity, 2010

駭客的定義

「駭客」（hacker）一詞一般有以下意義：
一個對（某領域內的）程式語言有足夠了解，可以不經長時間思考就能創造出有用的軟體的人。
喜愛編程(Coding)並享受在其中變得更擅長於編程的人。
喜愛自由(Freedom)，不易受約束，但覺得假如是為了喜愛的事物，可以被受適當的約束。

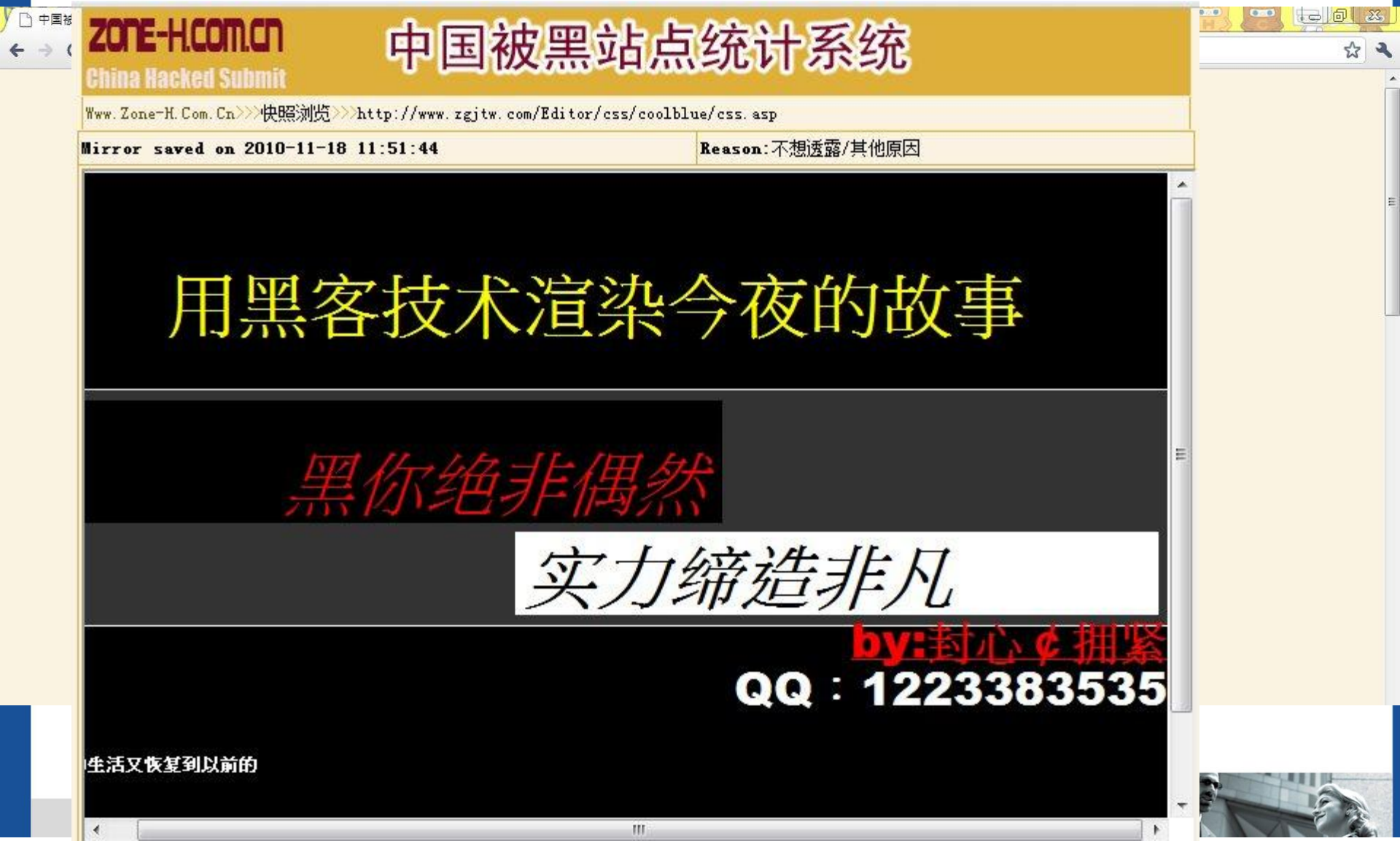
「黑客、怪客、垮客和劊客」（cracker）一詞一般有以下意義：
一個惡意（一般是非法地）試圖破解或破壞某個程式、系統及網路安全的人。

「**hacker**」們建設，而「**cracker**」們破壞。

- From Wiki

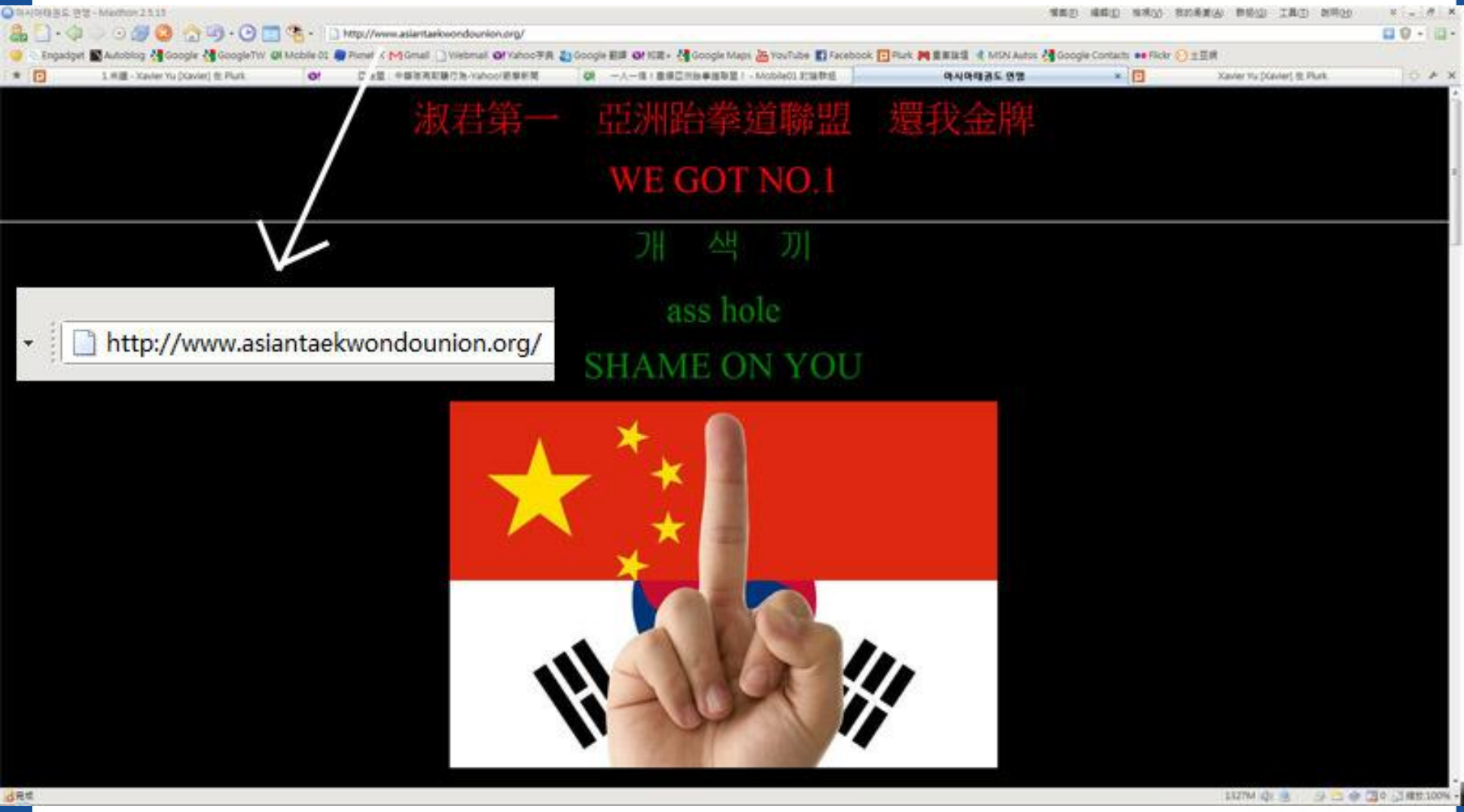
駭客的目的

為名

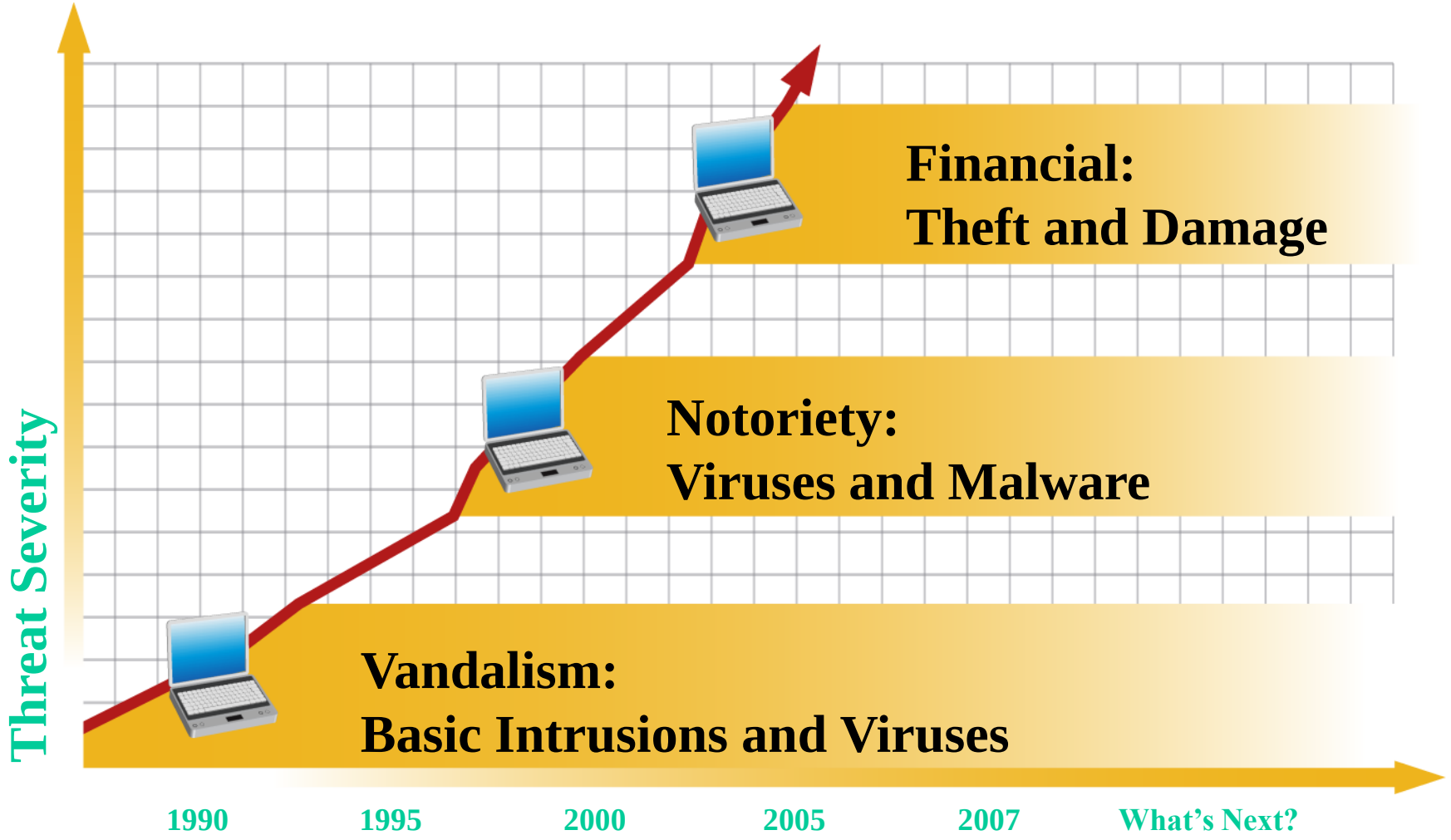

ZONE-H.COM.CN
China Hacked Submit
中国被黑站点统计系统
Www.Zone-H.Com.Cn>>>快照浏览>>>http://www.zgjtw.com/Editor/css/coolblue/css.asp
Mirror saved on 2010-11-18 11:51:44
Reason:不想透露/其他原因
用黑客技术渲染今夜的故事
黑你绝非偶然
实力缔造非凡
by:封心¢捆紧
QQ：1223383535
生活又恢复到以前的

不同的駭客

為名　　為利　　為一口氣



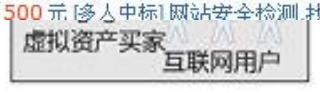
黑客想的是什麼?


Threat Severity
Financial:
Theft and Damage
Notoriety:
Viruses and Malware
Vandalism:
Basic Intrusions and Viruses
1990
1995
2000
2005
2007
What's Next?

黑客產業鏈

Sellers , Buyers

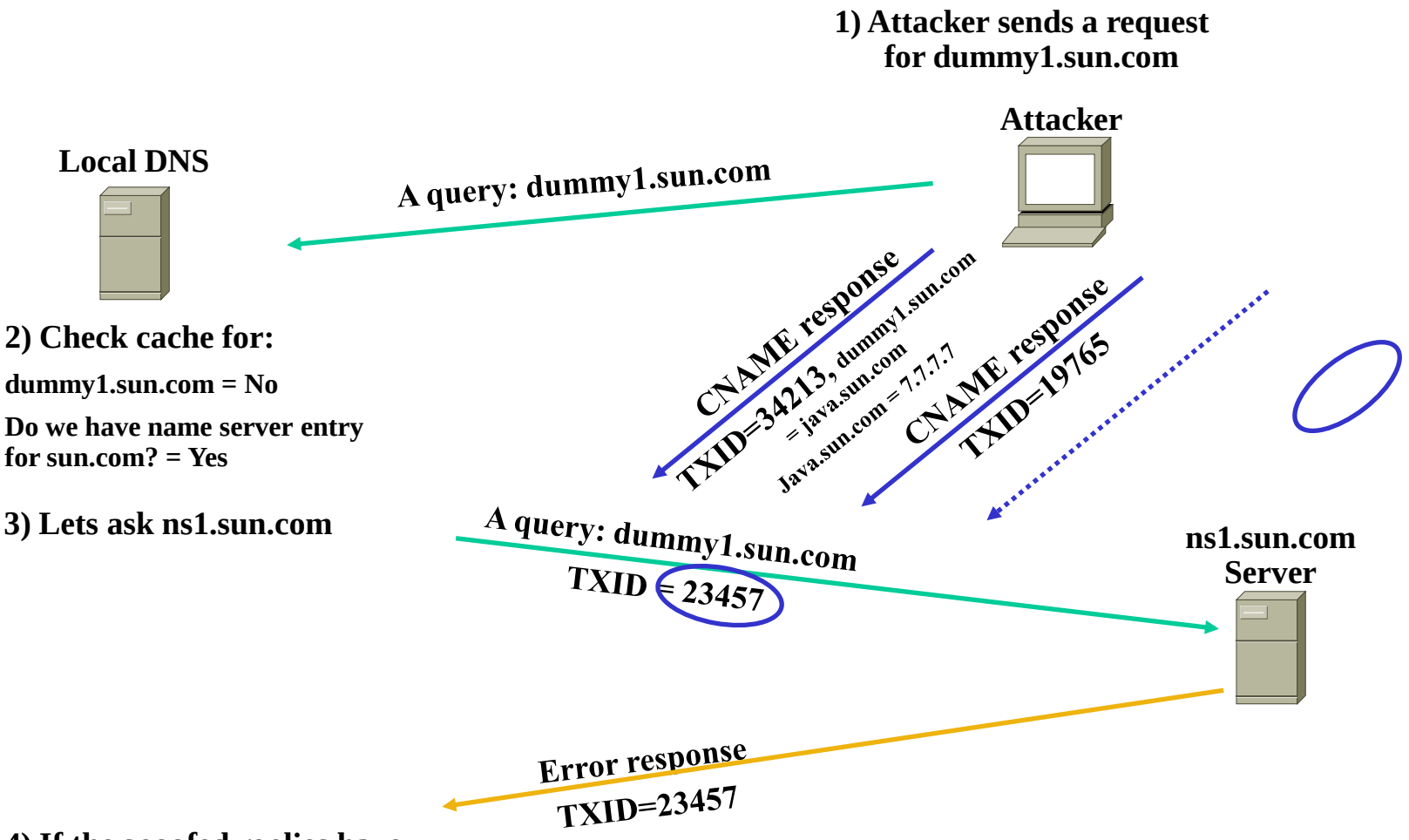
User ID	Name	Act	Payment type	Personal rates CC(raw$,unique$)	Money made	Money paid	Money made today	Money to pay	Status	Act	
					51688.844	51123.216	2.96	565.628			
0smsmsms	0smsmsms	edit	sale	80%	1210.8	980	2.4	230.8	!	pay	
lama	lama	edit	raw	US(**0.002**$/0.003$)	37640.802	37315	0.44	325.802	!!	pay	
12345	555	edit	unique	RU(0$/**0.00003**$)	150.102	140.946	0.02	9.156		pay	
archi11	Sergey	edit	unique		0	0	0	0		pay	
blabla	Test	edit	unique		0	0	0	0		pay	
flycove	Namee	edit	unique		0	0	0	0		pay	
goss	Gossudar	edit	unique		0.01	0	0	0.01		pay	
jack	Jack	edit	raw	RU(**0.01**$/0.03$) US(**0.01**$/0.05$) EU(**0.01**$/0.04$)	0.06	0	0	0.06		pay	
kaban	Zzz	edit	unique	*(0$/**0.01**$)	12674.06	12662.77	0.1	11.29		pay	
mike	Mike	edit	raw		1.5	1.5	0	0		pay	
mufi	Muf Mufich	edit	unique	BY(0.01$/**0.04**$) EN(0.01$/**0.04**$) FR(0.01$/**0.05**$) GB(0.01$/**0.05**$) US(0.01$/**0.04**$) AU(0.01$/**0.05**$)	0.05	0	0	0.05		pay	
peterspb	Peter Ost	edit	unique		11.36	13	0	-1.64		pay	



DNS – 網域名稱伺服器

Router – 路由器

DNS Cache 攻擊

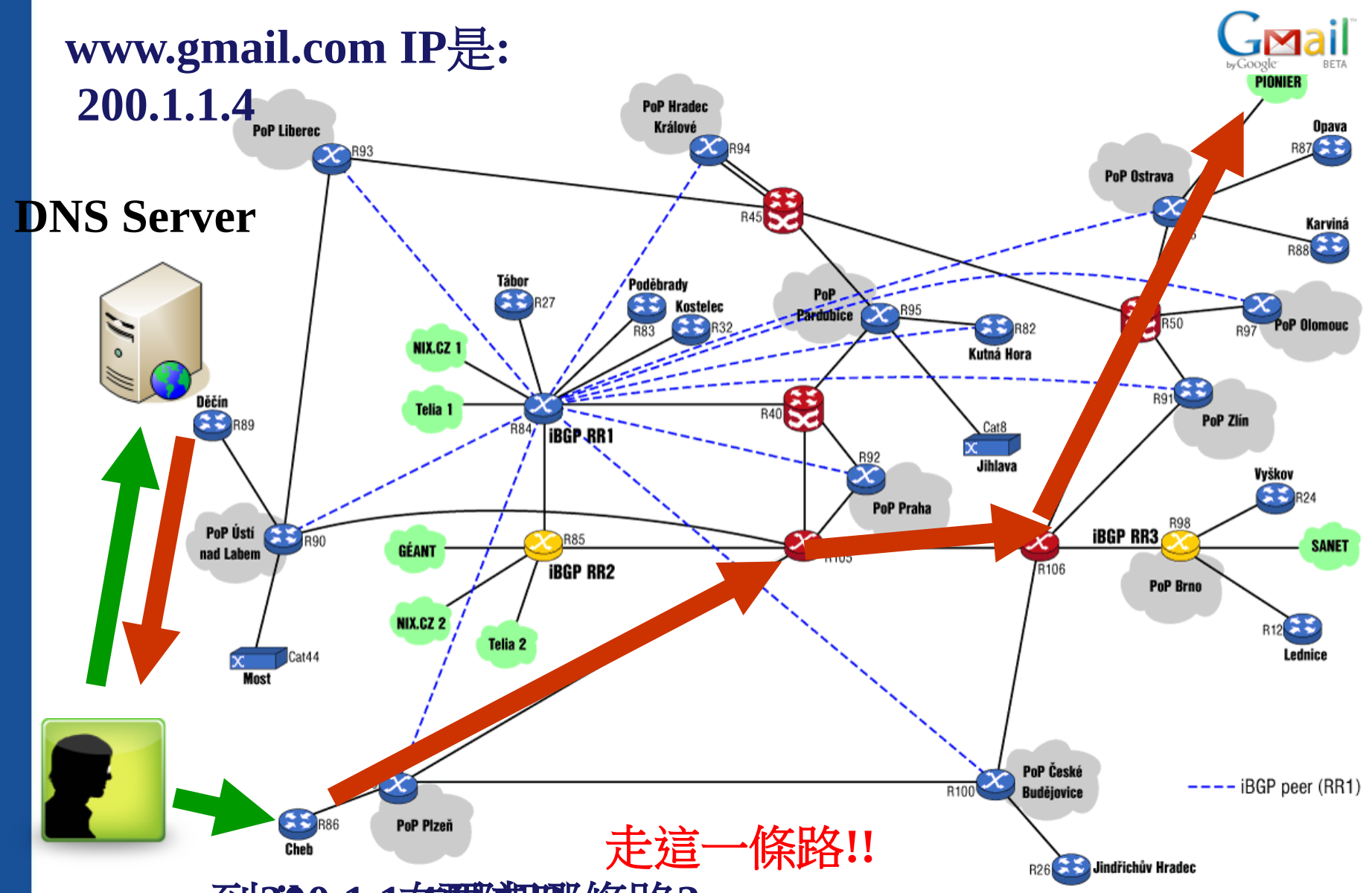

1) Attacker sends a request for dummy1.sun.com
Attacker
Local DNS
A query: dummy1.sun.com
CNAME response TXID=34213, dummy1.sun.com = java.sun.com Java.sun.com = 7.7.7.7
CNAME response TXID=19765
2) Check cache for:
dummy1.sun.com = No
Do we have name server entry for sun.com? = Yes
3) Lets ask ns1.sun.com
A query: dummy1.sun.com
TXID = 23457
ns1.sun.com Server
Error response
TXID=23457
4) If the spoofed replies have right TXID, update cache with:
• dummy1.sun.com = java.sun.com
• java.sun.com = 7.7.7.7

DNS Cache 攻擊

Router

www.gmail.com IP是:
200.1.1.4

DNS Server



走這一條路!!

www.gmail.com在哪裡? 到200.1.1.4要經哪條路?

DNS 被黑??

新　聞
新　聞　專　題
即　時　新　聞
新　聞　簡　訊
技　術
產　品　報　導
技　術　專　題
IT　書　訊
IT管理
CIO
IT　人　物
專　欄
新聞總覽
業界動態

微軟MSN首頁遭轉址　疑上層DNS被入侵

文/蘇文彬 (記者) 2009-03-06

由於並非所有使用者登入皆發生問題，專家指出問題點應是首頁上層DNS遭入侵，導致網站首頁發生被轉址問題。

台灣微軟MSN及CNET等網站首頁本週發生遭轉址事件，對此資安業者表示，應是上層DNS遭入侵所致。

根據網友在網路上的反映，本週部份連入MSN或CNET首頁的網友，被連結至某一特定中國網址（http://www.dachengkeji.com/artical/index.htm），由於並非所有網友皆發生此問題，部份網友壞疑自己電腦中毒，甚至引發網路上的討論。

對此，台灣微軟線上服務事業群行銷經理鍾婉珍表示，微軟並未接獲使用者的回報，而是從媒體報導後得知此訊息。而據微軟自己的瞭解，MSN系統正常並無被入侵的問題，不過微軟還交由內部安全部門調查，具體的原因並不清楚。

實驗新型態的攻擊手法。

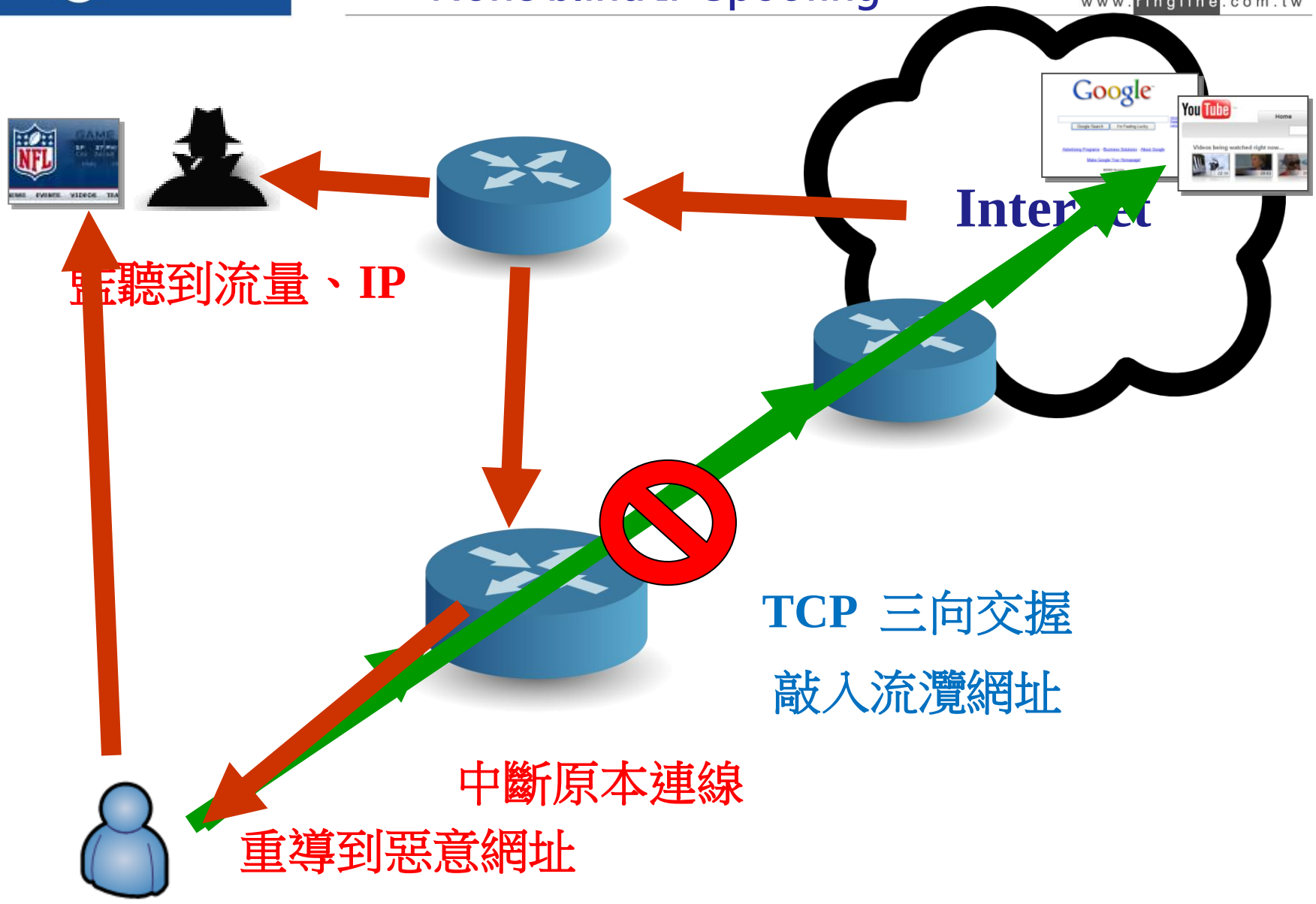
None-blind IP spoofing

是指攻擊者**可以監聽到TCP/IP流量**
，並發出TCP s/n對的假封包，並成功讓受害者以為是真封包。

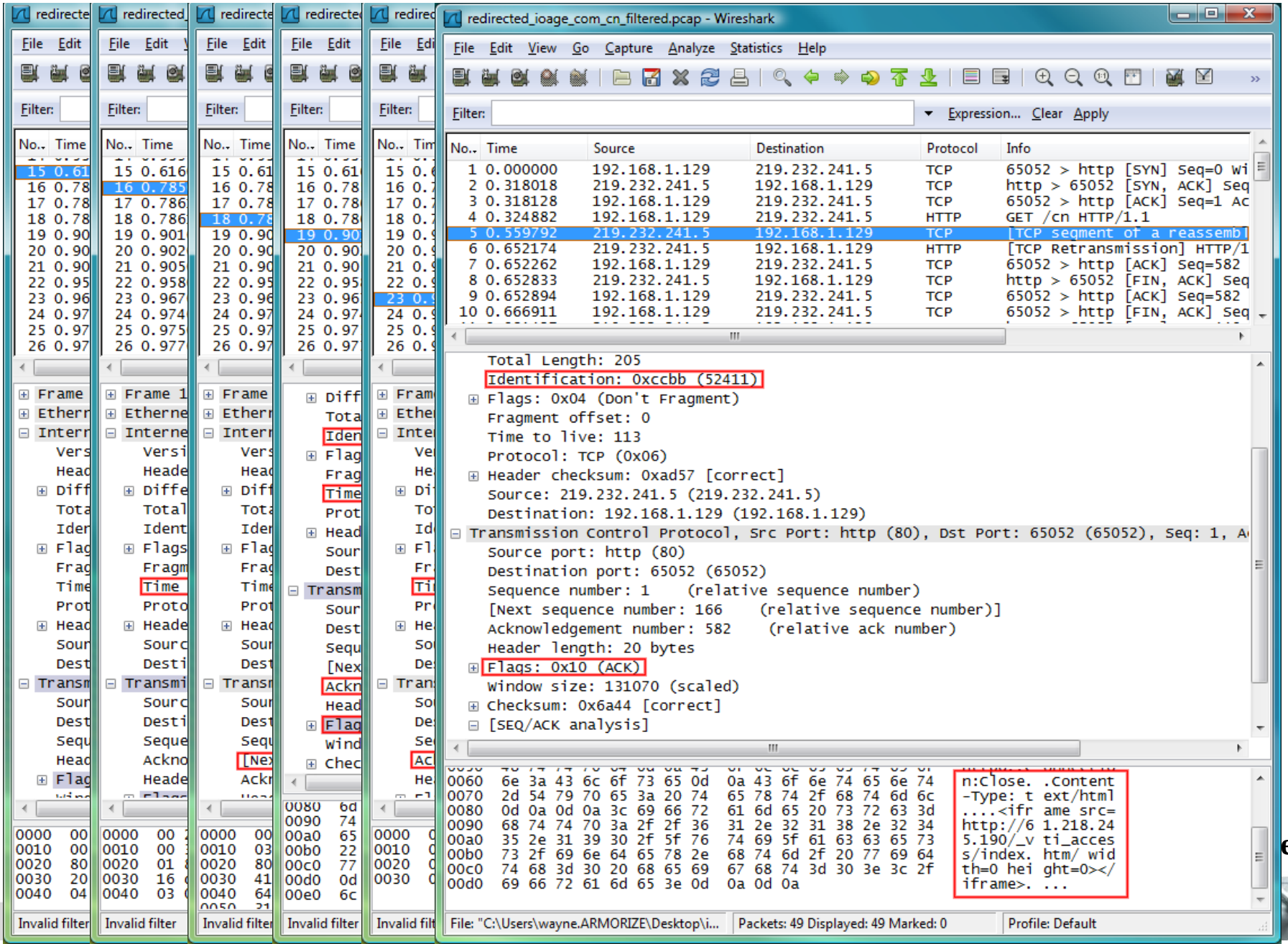
不同於因為監聽不到流量而必須發出大量封包的blind IP spoofing
，none-blind IP spoofing通常可以很準確的發幾個甚至一個封包，
就能達到效果--這是攻擊者喜愛它的重要原因之一。

來源: 阿碼科技 Wayne

None blind IP Spoofing



Non-Blind IP Spoofing



凡走過必留下痕跡


```
3/28/2009 8:38:38 test Default Group show configuration <cr>
3/28/2009 8:38:59 test Default Group show interfaces <cr>
3/28/2009 8:39:48 test Default Group configure terminal <cr>
3/28/2009 8:39:50 test Default Group interface Tunnel 128 <cr>
3/28/2009 8:39:57 test Default Group show interfaces <cr>
3/28/2009 8:41:48 test Default Group configure terminal <cr>
3/28/2009 8:41:49 test Default Group access-list 20 permit 192.168.2.2 <cr>
3/28/2009 8:41:50 test Default Group ip nat pool new [removed] netmask 255.255.255.252 <cr>
3/28/2009 8:41:51 test Default Group ip nat inside source list 20 pool new overload <cr>
3/28/2009 8:41:52 test Default Group ip nat inside source static tcp 192.168.2.2 113 [removed] 113 extendable
3/28/2009 8:41:52 test Default Group interface Serial 1/0 <cr>
3/28/2009 8:41:53 test Default Group ip nat outside <cr>
3/28/2009 8:41:53 test Default Group interface Tunnel 128 <cr>
3/28/2009 8:41:53 test Default Group ip nat inside <cr>
3/28/2009 8:41:54 test Default Group ip address 192.168.2.1 255.255.255.0 <cr>
3/28/2009 8:41:54 test Default Group ip tcp adjust-mss 1400 <cr>
3/28/2009 8:41:55 test Default Group tunnel source Serial 1/0 <cr>
3/28/2009 8:41:55 test Default Group tunnel destination [removed] <cr>
```

建立Tunnel

設定Tunnel

加入ACL

設定新的NAT

Whoa! The bad guy is not wasting any time. Barely five minutes after connecting, and he has configured a network tunnel back to his home base.

```
3/28/2009 8:47:23 test Default Group configure terminal <cr>
3/28/2009 8:47:26 test Default Group line console 0 <cr>
3/28/2009 8:47:32 test Default Group password *****
3/28/2009 8:47:45 test Default Group who <cr>
3/28/2009 8:47:55 test Default Group configure terminal <cr>
3/28/2009 8:48:01 test Default Group line vty 0 1052 <cr>
3/28/2009 8:48:06 test Default Group password *****
3/28/2009 8:49:12 test Default Group no transport input <cr>
3/28/2009 8:49:26 test Default Group transport input ssh <cr>
```

修改Router 密碼

DNS –

在使用者不知的情況下被導向惡意的IP。

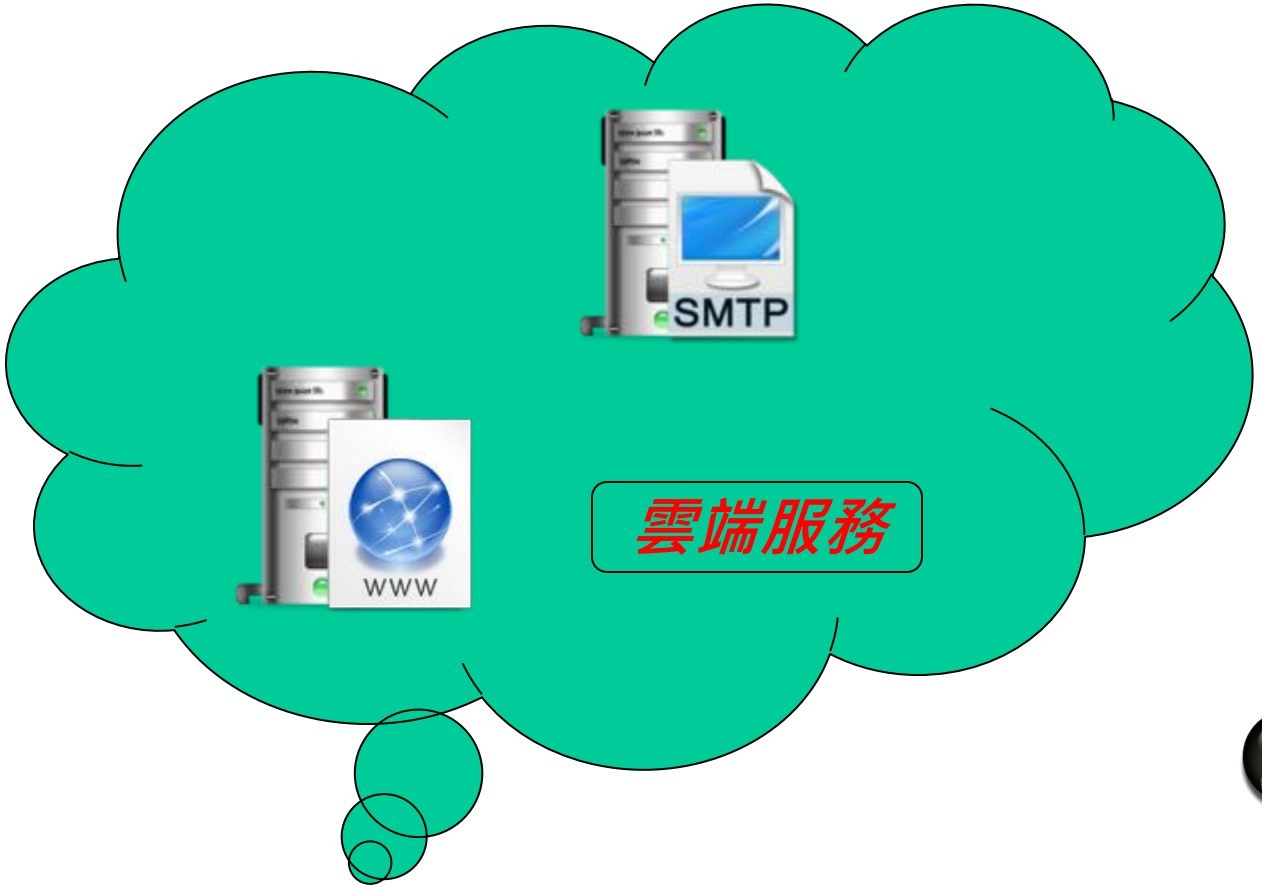
Router –

在使用者不知的情況下被導向惡意的IP。

目的在騙取你的帳密，使用者不自覺被掛馬...。

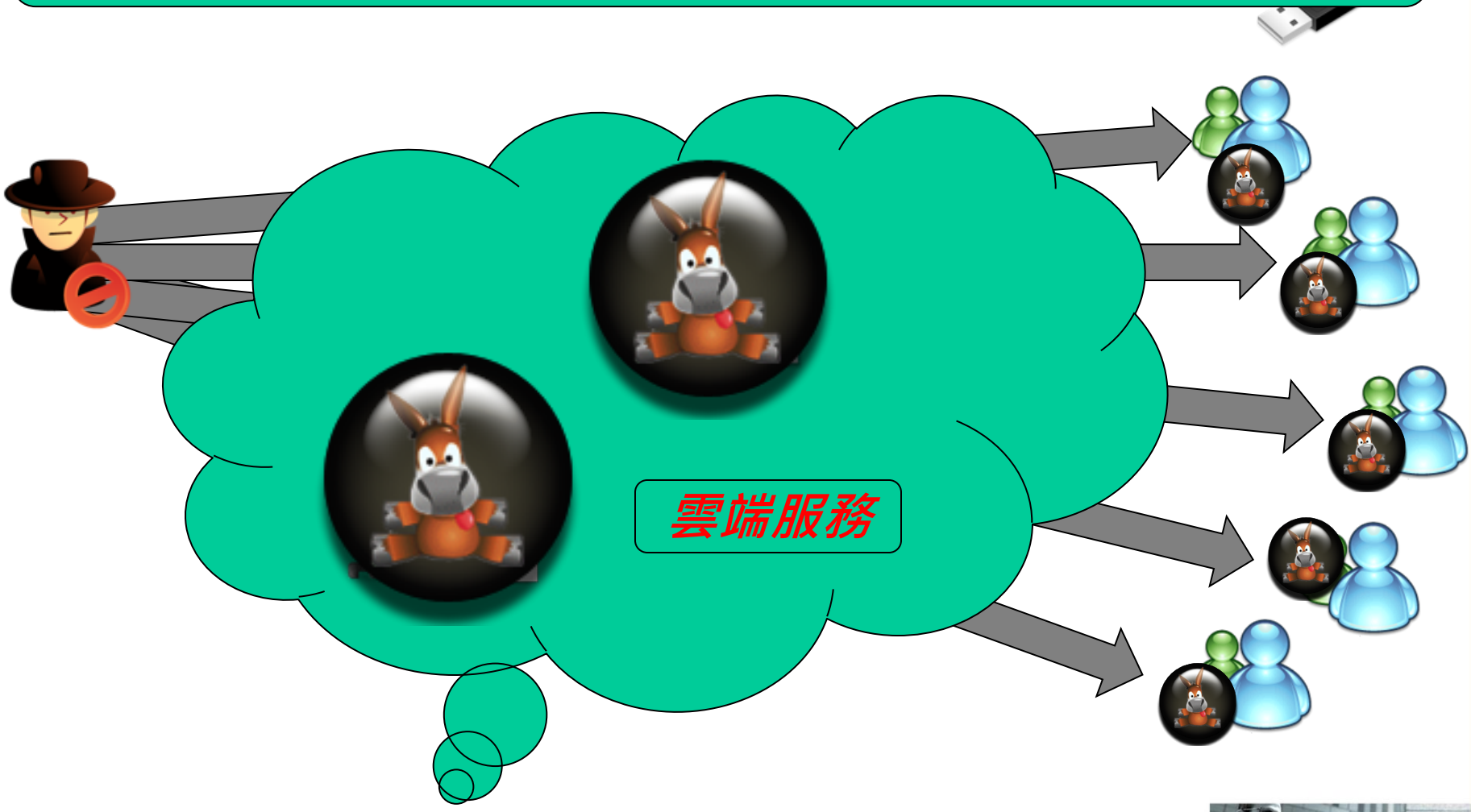
在沒有PaaS之前

黑客透過Mail,Web,USB...方式快速傳遞木馬



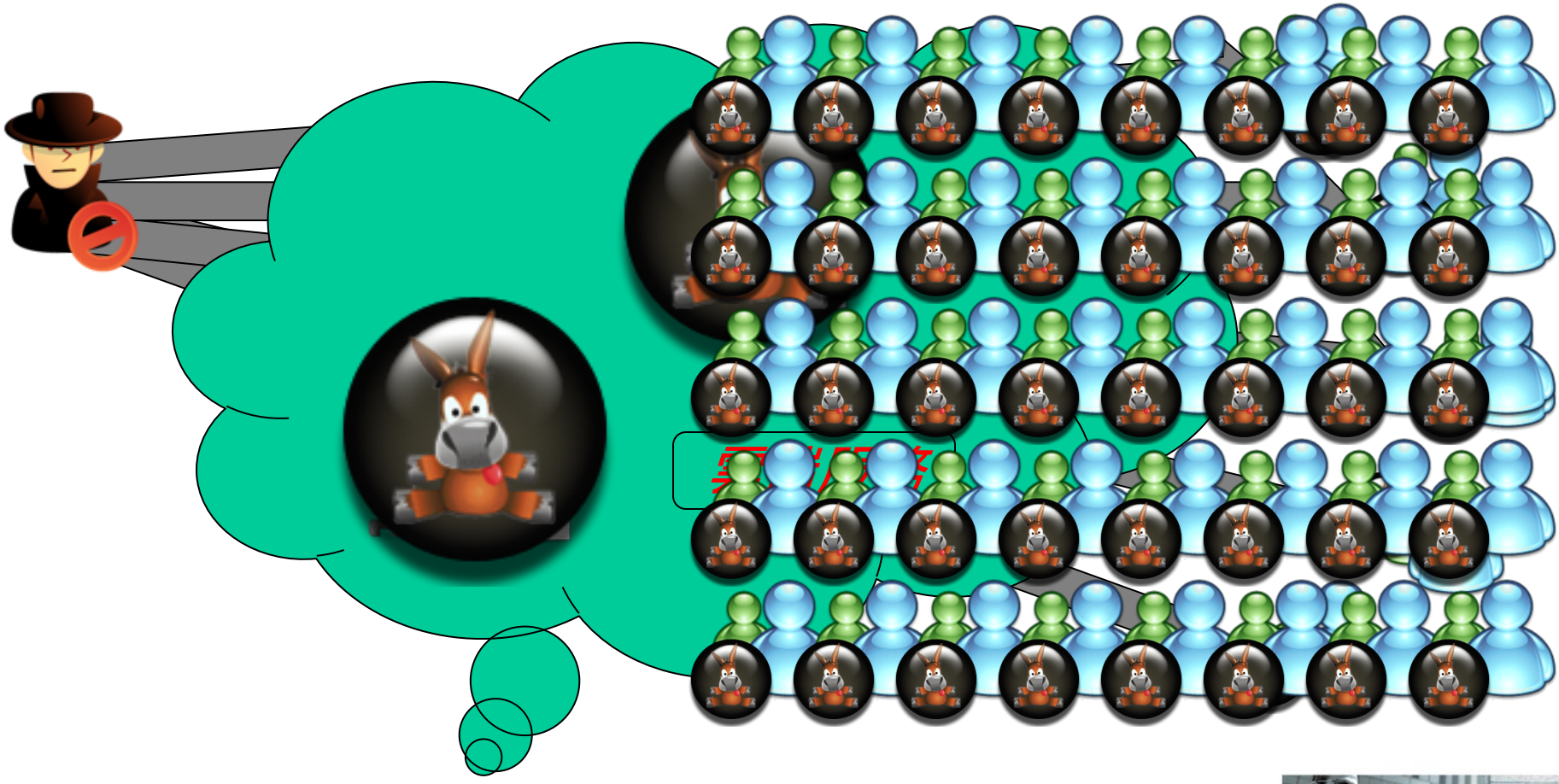
在沒有PaaS之前

此時黑客可以任何的操控您的電腦　佔領新目標 或...

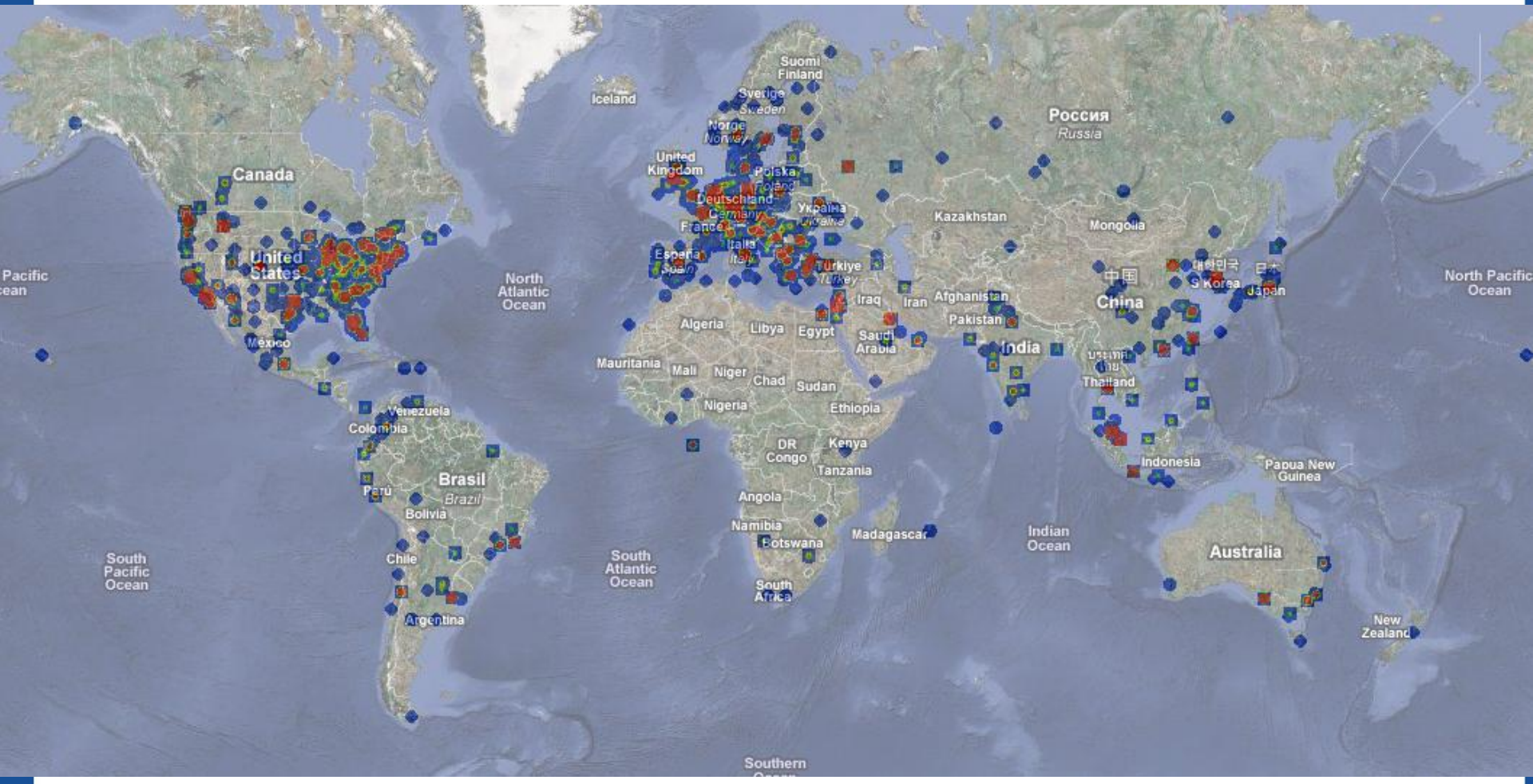


在沒有PaaS之前

成為黑客的　網路大軍

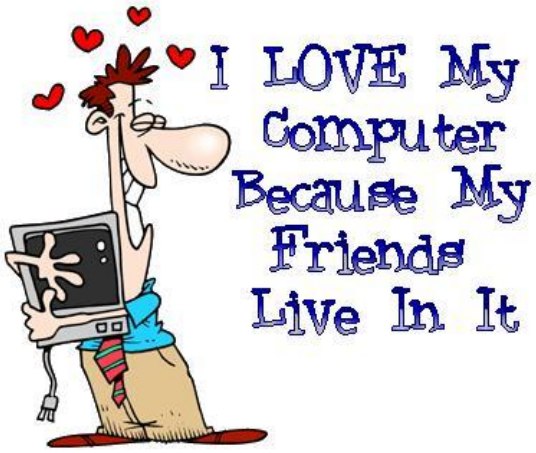


2010 Botnet分佈



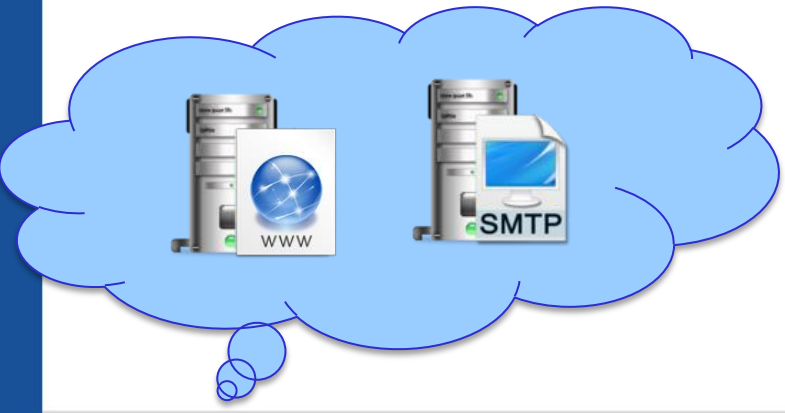
http://www.shadowserver.org

當黑客漫步 PaaS

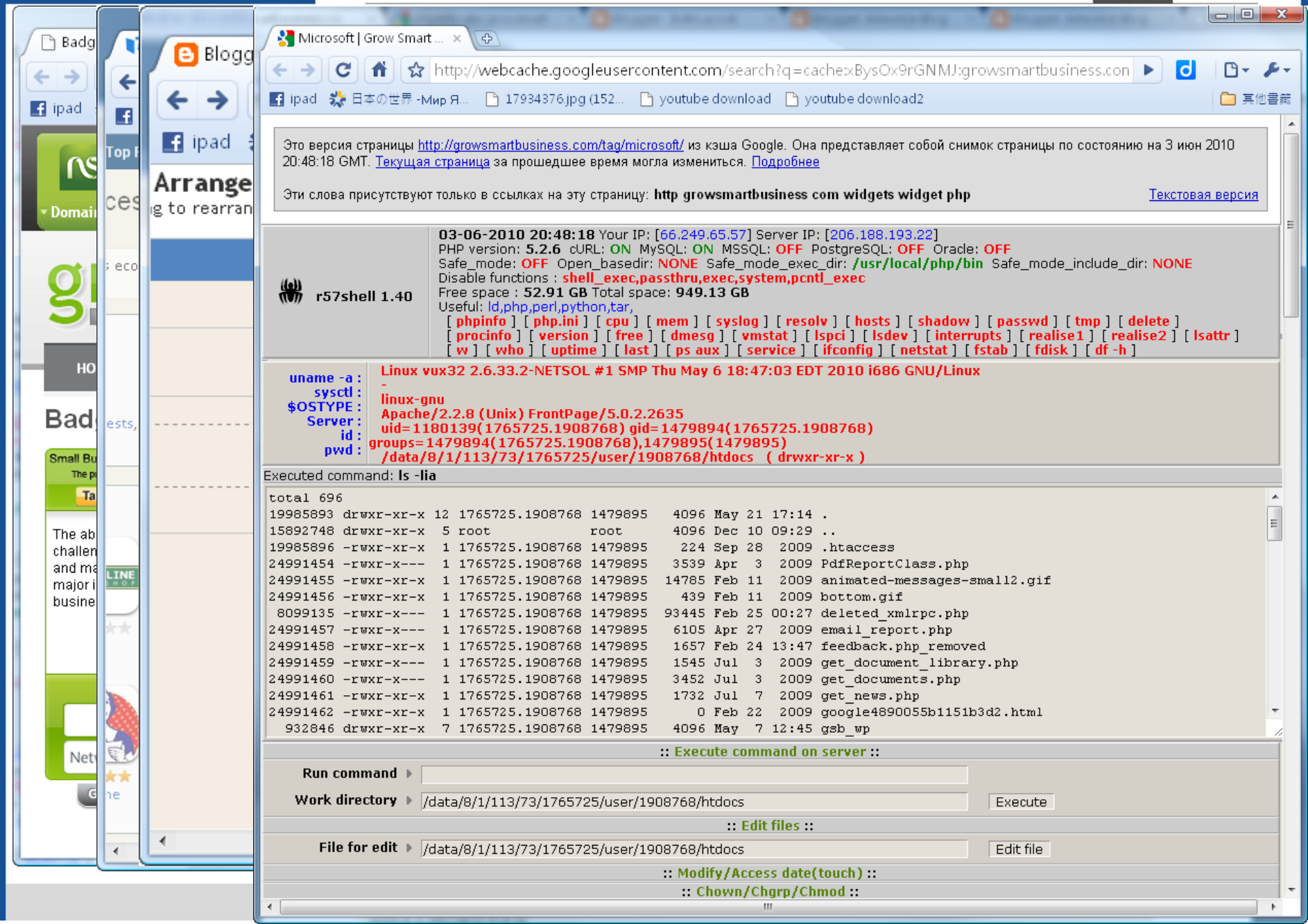


你的電腦 = 我的電腦

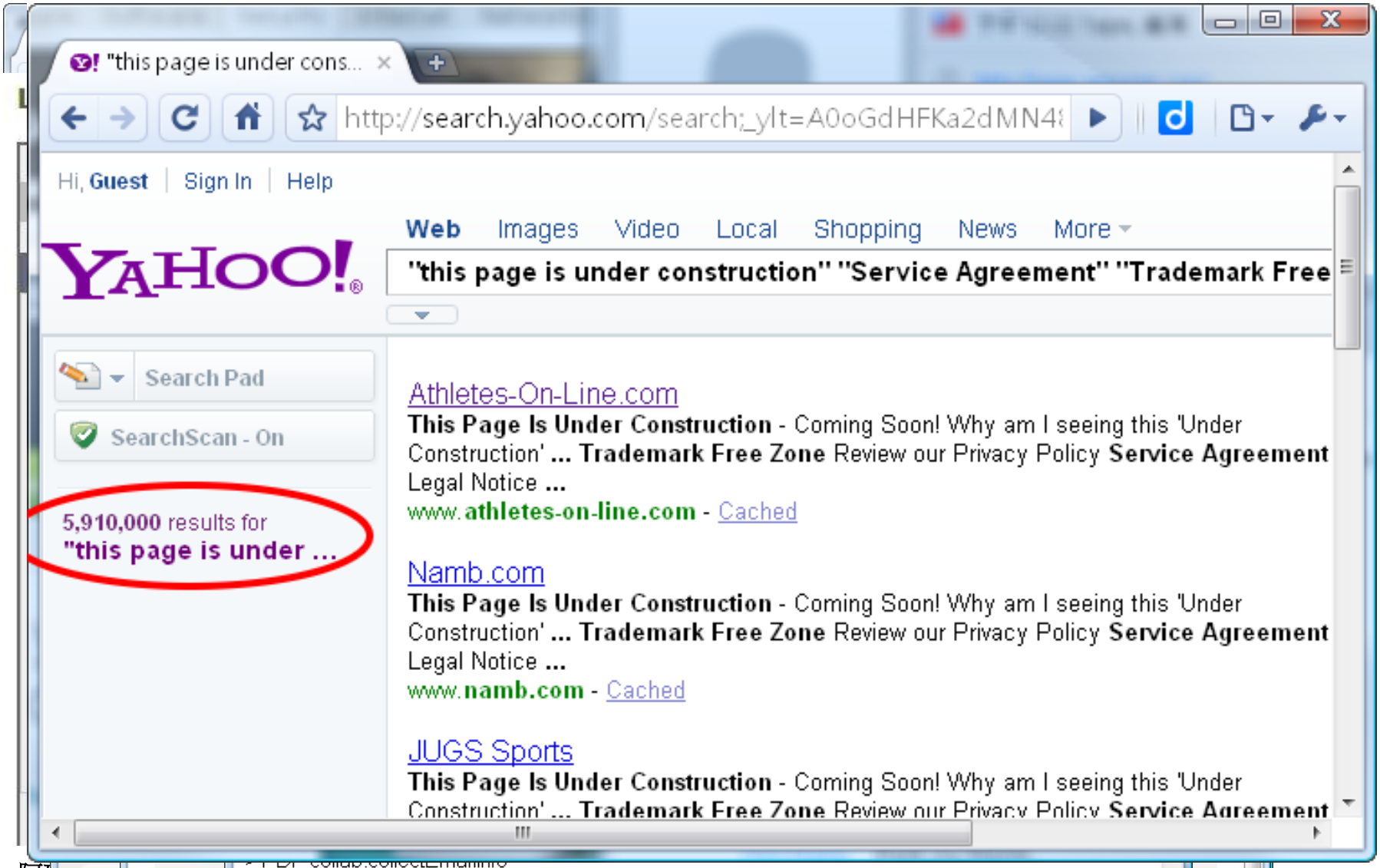
雲的電腦 = 我的電腦



PaaS – Web Hosting



PaaS – Web Hosting



PaaS - 利用雲端黑雲端

NOWnews【重點新聞】網安／驚！駭客兜售150萬筆Facebook帳號 - Windows Internet Explorer

http://www.nownews.com/2010/04/26/91-2596165.htm

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

我的最愛 | 駭客 - Google ... | NOWnews【...

網頁(P) 安全性(S) 工具(O)

網安／驚！駭客兜售150萬筆Facebook帳號(2010/04/26 09:42)

記者蘇湘雲／綜合報導

Facebook成立6年，全球會員人數突破4億，台灣會員近900萬人，不斷被點名成為網路詐騙熱門管道，一份網路安全調查報告證實，一名自稱為Kirllos的駭客竊取了150萬筆Facebook帳號，並以極低的價格在駭客論壇中兜售。

（看全部文章→ 《母親節／媽咪不是黃臉婆！撇保養品，要當手機潮娘》）

駭客兜售150萬筆Facebook帳號

避免使用相同的密碼並定期變更

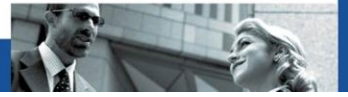
友人的1000筆帳號售價為45美元。

網際網路 | 受保護模式: 啟動

100%

當黑客漫步 SaaS


YouTube
Broadcast Yourself™
QuickTime
1
Windows Live
eMule
Gmail
by Google
BETA
Windows
Media
real
iTunes
skype
BitTorrent
napster



OWASP TOP 10

OWASP（開放Web軟體安全計畫－Open Web Application Security Project）2010 TOP 10：

OWASP Top 10 – 2007 (Previous)		OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	↑	A1 – Injection
A1 – Cross Site Scripting (XSS)	↓	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	=	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	=	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	↑	A7 – Failure to Restrict URL Access
<not in T10 2007>	+	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	↓	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	↓	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	-	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	-	<dropped from T10 2010>

About Cross Site Script

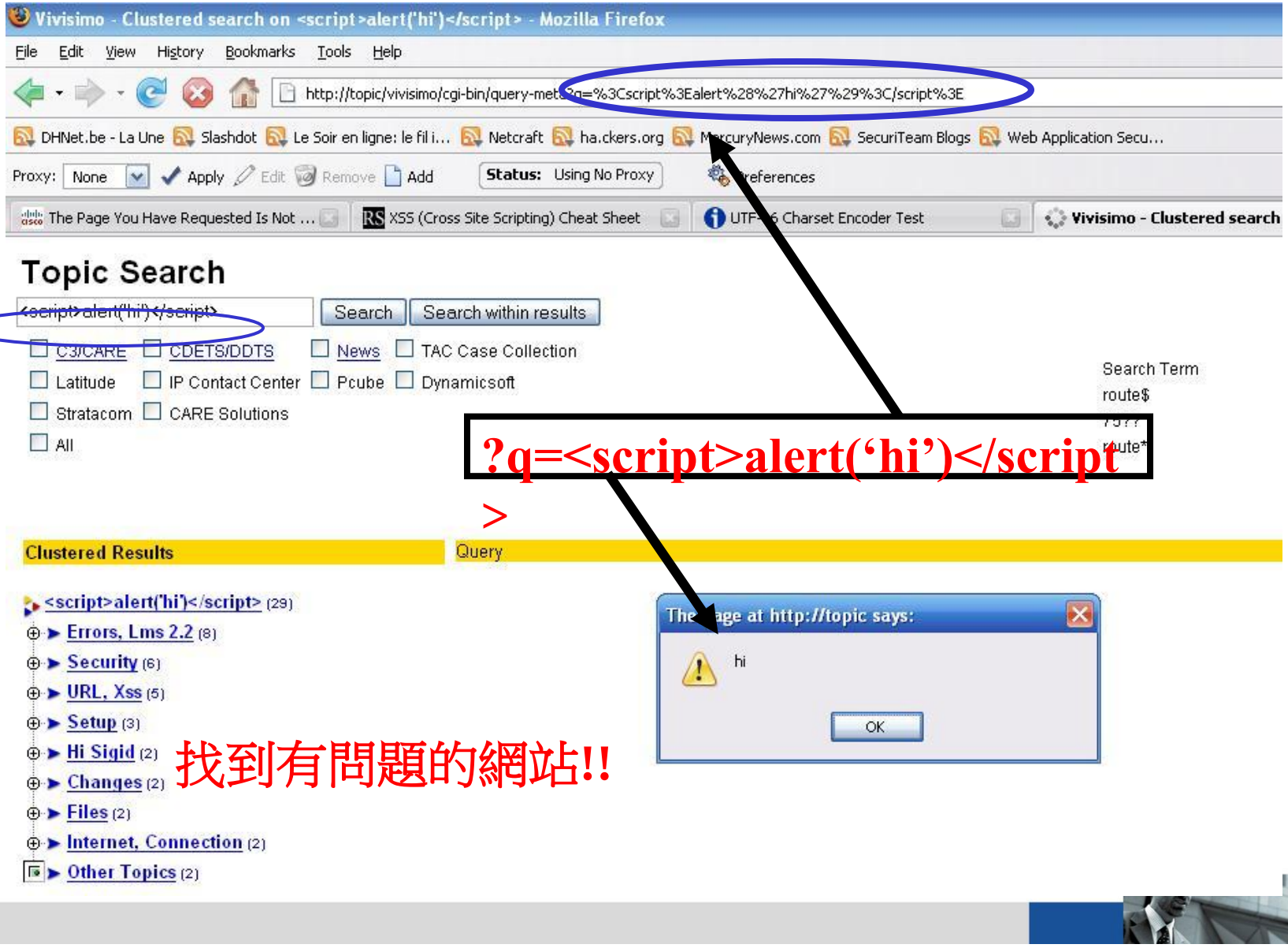
- Cross Site Script 簡稱 XSS

- Cross Site:　跨網站
- Script:　一段程式碼

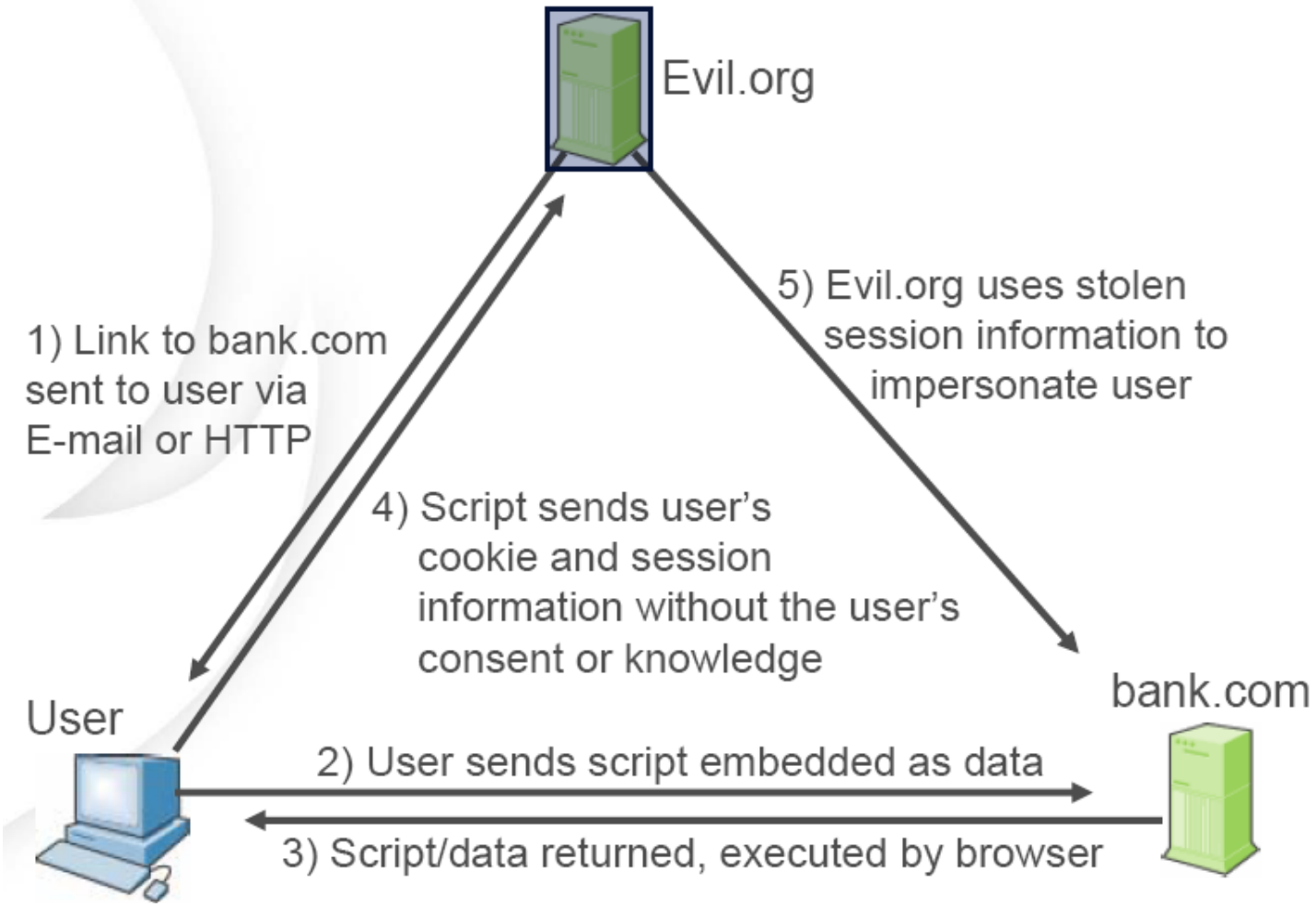
跨過網站進行一段程式語法攻擊的手法

簡稱: 跨網站攻擊

確認XSS弱點


Vivisimo - Clustered search on <script>alert('hi')</script> - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://topic/vivisimo/cgi-bin/query-met?q=%3Cscript%3Ealert%28%27hi%27%29%3C/script%3E
DHNet.be - La Une Slashdot Le Soir en ligne: le fil i... Netcraft ha.ckers.org MercuryNews.com SecuriTeam Blogs Web Application Secu...
Proxy: None Apply Edit Remove Add Status: Using No Proxy
The Page You Have Requested Is Not ... XSS (Cross Site Scripting) Cheat Sheet Vivisimo - Clustered search
Topic Search
<script>alert('hi')</script>
Search Search within results
C3/CARE CDETS/DDTS News TAC Case Collection
Latitude IP Contact Center Pcube Dynamicsoft
Stratacom CARE Solutions
All
Search Term
route$
?q=<script>alert('hi')</script
>
Clustered Results
Query
<script>alert('hi')</script> (29)
Errors, Lms 2.2 (8)
Security (6)
URL, Xss (5)
Setup (3)
Hi Sigid (2)
Changes (2)
Files (2)
Internet, Connection (2)
Other Topics (2)
The page at http://topic says:
hi
OK
找到有問題的網站!!

XSS攻擊流程


Evil.org
1) Link to bank.com sent to user via E-mail or HTTP
5) Evil.org uses stolen session information to impersonate user
4) Script sends user's cookie and session information without the user's consent or knowledge
User
bank.com
2) User sends script embedded as data
3) Script/data returned, executed by browser

XSS攻擊偽裝

一、包裝、誘惑:

佛要金裝、人要衣裝，攻擊要偽裝!!

攻擊語法: http://www.bank.com.tw/login.aspx?user="我是攻擊字串"

包裝與誘惑的結合:

二、散播:

- 1.利用Email告知某網站有重大訊息
- 2.公告
- 3.在各大討論區、留言板發佈此連結

- 目的是引誘使用者在毫無預警的情況下去點取此連結，而成為XSS攻擊的受害者。

XSS攻擊Demo

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

http://altoro.testfire.net/

最常瀏覽的網站 新手上路 即時新聞

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win an 8GB iPod Nano
Completing this short survey will enter you in a draw for 1 of 50 iPod Nanos. We look forward to hearing your important feedback.

Privacy Policy | Security Statement | © 2009 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is

完成

About SQL-Injection

SQL:　結構化查尋語言

(Structure Querying Language)

Injection:　輸入、注入

結構化查尋語言的輸入攻擊手法 !!

簡稱: 資料庫攻擊

SQL-Injection

Hi,Web Server
我想看哈利波特
-死神的聖物

Web Server

Hi,資料庫，
那邊有哈利波特-死
神的聖物嗎?

SQL Server

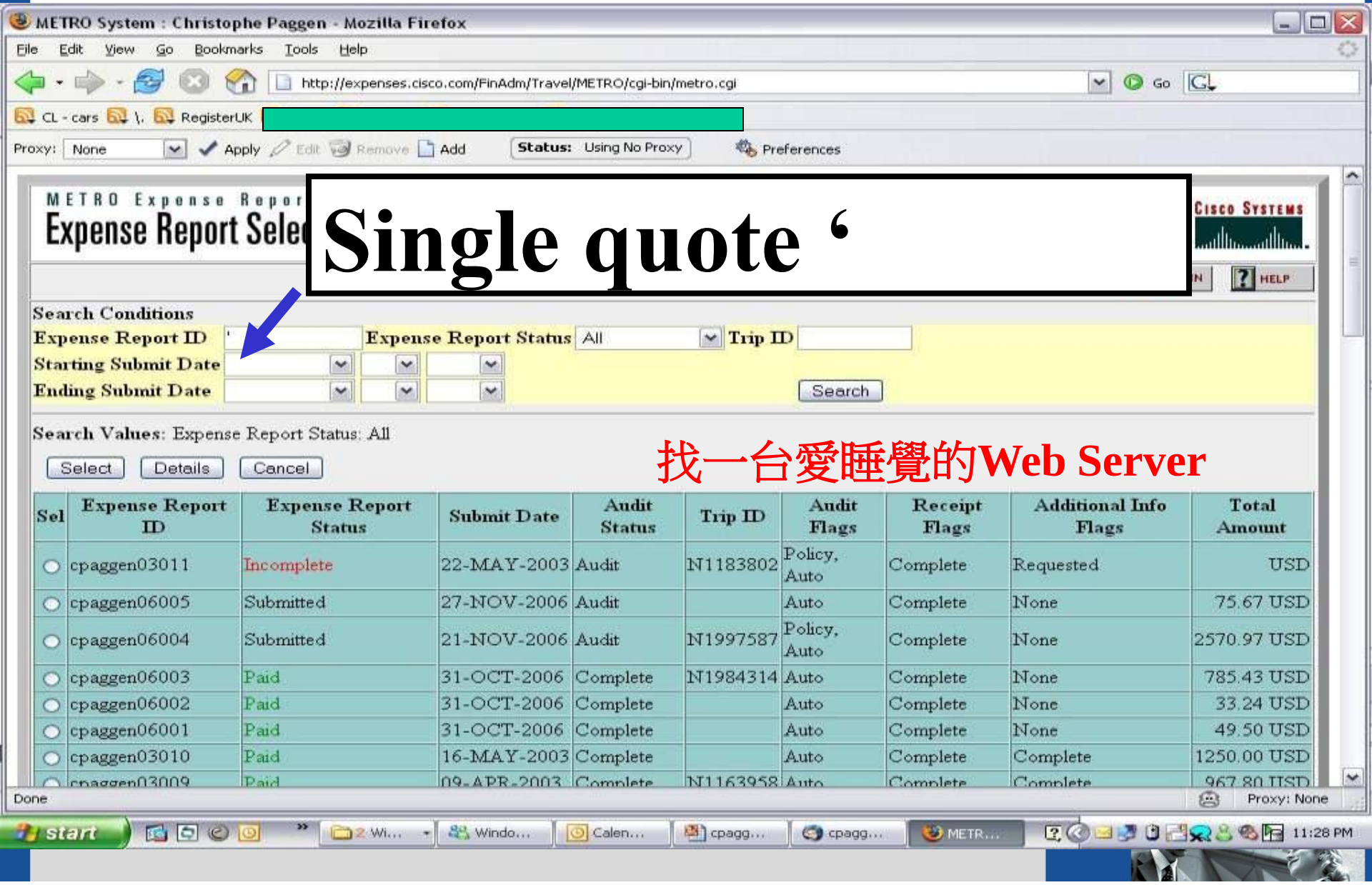
Hi,資料庫，
那邊有哈利波特-死
神的聖物嗎?

ZZzzz…

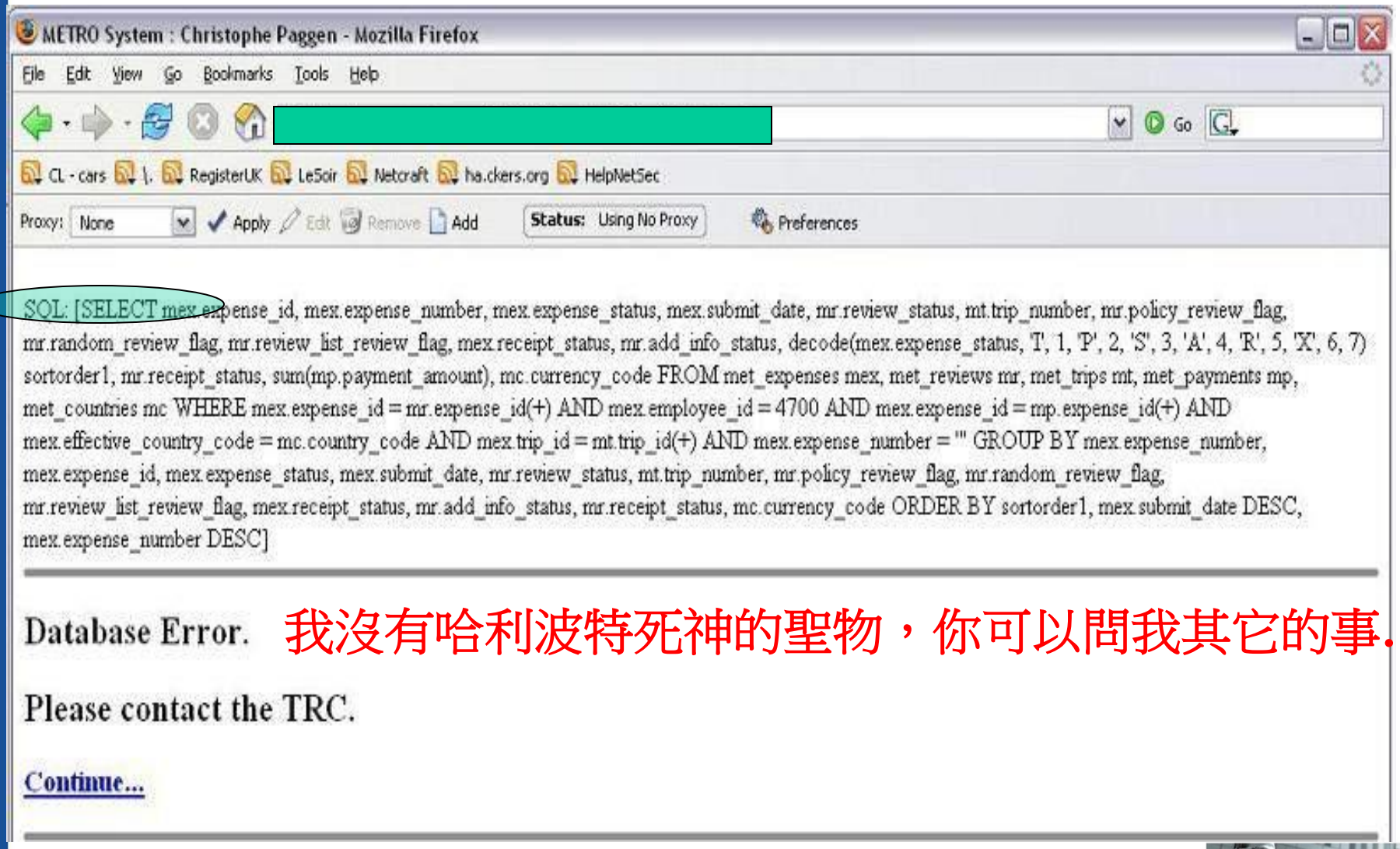
愛睡覺的
Web Server

SQL Server

SQL-Injection 弱點確認



SQL-Injection 弱點確認



SQL-Injection攻擊Demo

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

http://altoro.testfire.net/

最常瀏覽的網站 新手上路 即時新聞

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win an 8GB iPod Nano
Completing this short survey will enter you in a draw for 1 of 50 iPod Nanos. We look forward to hearing your important feedback.

Privacy Policy | Security Statement | © 2009 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is

完成

SQL-Injection 解說


```
String query = "SELECT cardnum FROM accounts
      WHERE username = '" + strUName +
      "' AND password = " + strCType + ";";
```

Expected input:

```
SELECT cardnum FROM accounts
      WHERE username = 'John'
      AND password = 243s23;
```

Result: Returns John's saved credit card number

SQL-Injection 解說


```
String query = "SELECT cardnum FROM accounts
      WHERE username = '" + strUName +
      "' AND password = " + strCType + ";";
```

Malicious input:

```
SELECT cardnum FROM accounts
      WHERE (username = 'John'
      AND password = 2) OR (1 = 1);
```

Result: Returns all saved credit numbers.

黑客漫步在 SaaS

SaaS 改變使用者使用網路的方式

讓使用者更容易使用網路。

也同時改變黑客使用網路的方式

讓黑客更容易黑網路。

Agenda

1. 關於雲端服務
2. 生活中的雲端科技
3. 駭客漫步在雲端
4. 雲端使用安全

DNS 防護

Table of Contents

Protect Your DNS Infrastructure

Status	Countermeasure
ON	Invalid Packets
OFF	Black / White List
OFF	Zombie Detection
ON	TCP SYN Authentication
OFF	DNS Authentication
OFF	TCP Connection Reset
OFF	Payload Regular Expression
OFF	Source /24 Baselines
OFF	Protocol Baselines
OFF	DNS Malformed
OFF	DNS Rate Limiting
OFF	DNS NXDomain Rate Limiting
OFF	DNS Regular Expression
OFF	HTTP Malformed
OFF	HTTP Rate Limiting
OFF	HTTP Regular Expression
OFF	SIP Malformed
OFF	SIP Request Limiting
OFF	Shaping

Interview With A Convicted Hacker: Robert Moore Tells How He Broke Into Routers And Stole VoIP Services

On his way to federal prison, the 23-year-old hacker says breaking into computers at telecom companies and major corporations was "so easy a caveman could do it."

By **Sharon Gaudin** , InformationWeek
] 26, 2007 08:36 H

Convicted hacker Robert Moore, who is set to go to federal prison this week, says breaking into 15 telecommunications companies and hundreds of businesses worldwide was incredibly easy because simple IT mistakes left gaping technical holes.

Moore, 23, of Spokane, Wash., pleaded guilty to conspiracy to commit computer fraud and is slated to begin his two-year sentence on Thursday for his part in a scheme to steal voice over IP services and sell them through a separate company. While prosecutors call co-conspirator Edwin Pena the mastermind of the operation, Moore acted as the hacker, admittedly scanning and breaking into telecom companies and other corporations around the world.

Related Articles

- Accused VoIP Fraudster Sought As Fugitive
- VoIP Security Alert: Hackers Start Attacking For Cash

More Internet Insights

White Papers

- Shared IT Infrastructure - New Storage Buying Criteria

"It's so easy. It's so easy a caveman can do it," Moore told *InformationWeek*, laughing. "When you've got that many computers at your fingertips, you'd be surprised how many are insecure."

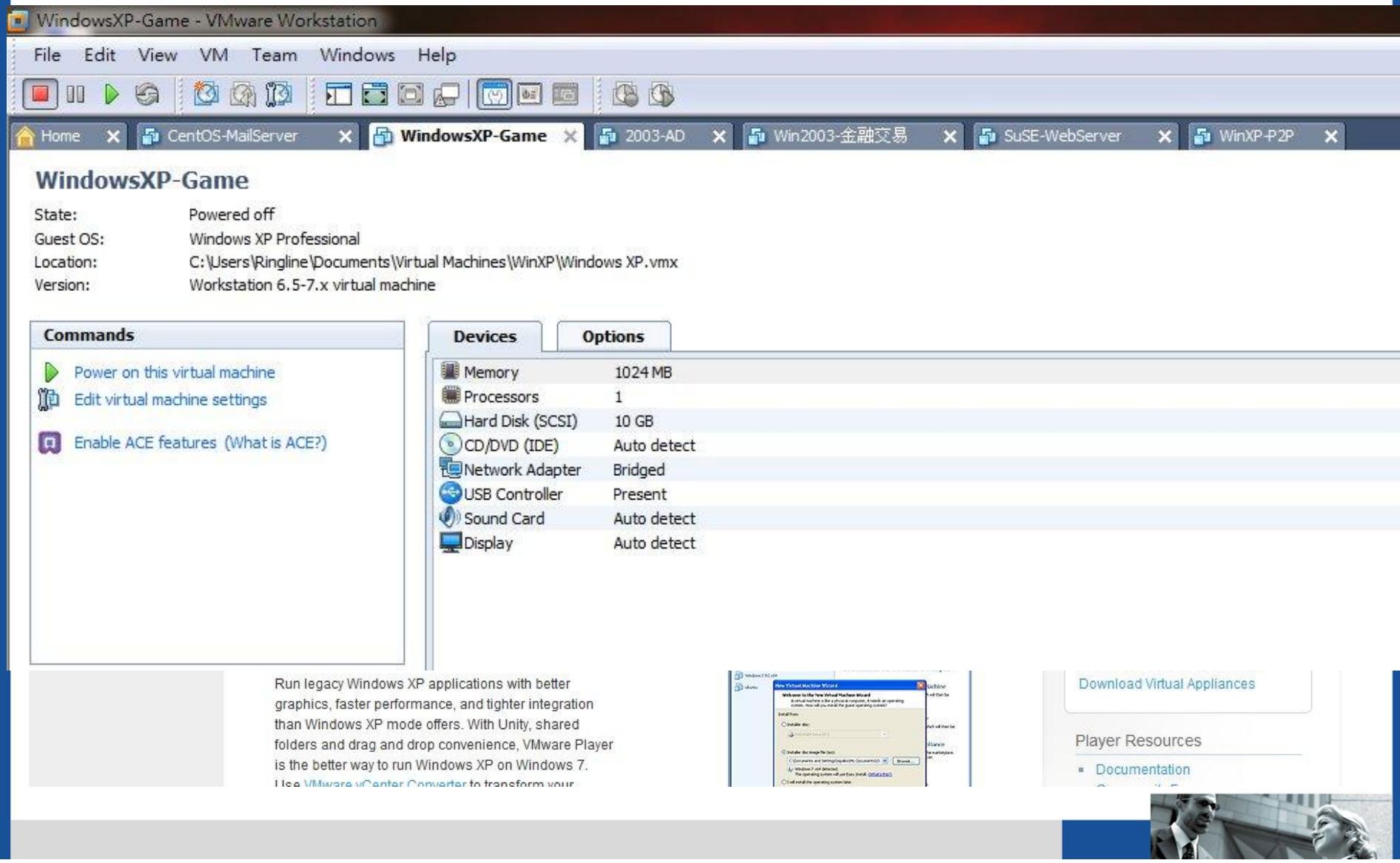
Pena, who is charged with acting as a legitimate wholesaler of Internet-based phone services as part of what the government called a "sophisticated fraud," fled the country a year ago and is wanted as a fugitive. Assistant U.S. Attorney Erez Liebermann said Pena allegedly stole and then sold more than 10 million minutes of service at deeply discounted rates, netting more than $1 million from the scheme.

45~50%
使用預設密碼

沒有更新

個人防護

http://www.vmware.com/products/player/



密碼安全

卡優新聞網 - 焦點新聞 > 卡訊 > - Windows Internet Explorer

http://www.cardu.com.tw/news/detail.htm?nt_pk=8&ns_pk=9679

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

我的最愛 卡優新聞網 - 焦點新聞 > 卡訊 >

網頁(P) 安全性(S) 工具(O)

申請費用。

從持卡人角度來看，只要完成申辦「Visa驗證」服務後，未來在網路商店挑選商品，進行結帳程序時，除了一般線上交易的標準流程：輸入Visa卡號、卡片有效日期、卡片背面末三碼之外，在訂單送出前，還會要求輸入「Visa驗證」個人密碼，以核對持卡人身份。

Visa強調，使用「Visa驗證」服務網購有著更安全的交易機制保護，不但可增強持卡人的交易信心，網路特約商店也可藉此提升交易安全性，以增加知名度與顧客忠誠度。尤其卡友不須透過ATM轉帳，就有可能享有發卡銀行所推出的紅利點數及現金回饋等優惠，讓持卡人更能享受愉快的網購經驗。

此外，中國信託更將此技術升級為「網路刷卡簡訊動態密碼(One Time Passcode)認證服務」，卡友註冊完成設定後，於網路特約商店購物時，系統會主動發送驗證密碼簡訊至持卡人指定的手機門號，使用者不須背記太多組密碼而產生混淆。此外，每次所傳送的密碼僅限當次交易有效，若逾時10分鐘未輸入密碼則自動失效，提供持卡人更安心、更安全、更便利的認證平台。

Visa持卡人可透過網路申請「Visa驗證」服務，或洽詢銀行客服人員協助辦理。完成線上註冊(網路/電話)程序後，就可立即使用相關安全購物服務。目前全台共有十二家銀行提供「Visa驗證」服務，包括中國信託、台新銀行、台灣中小企銀、土地銀行、日盛銀行、合作金庫銀行、永豐銀行、第一銀行、國泰世華銀行、新光銀行、彰化銀行及聯邦銀行。

網路購物安心刷卡　Visa驗證強力把關

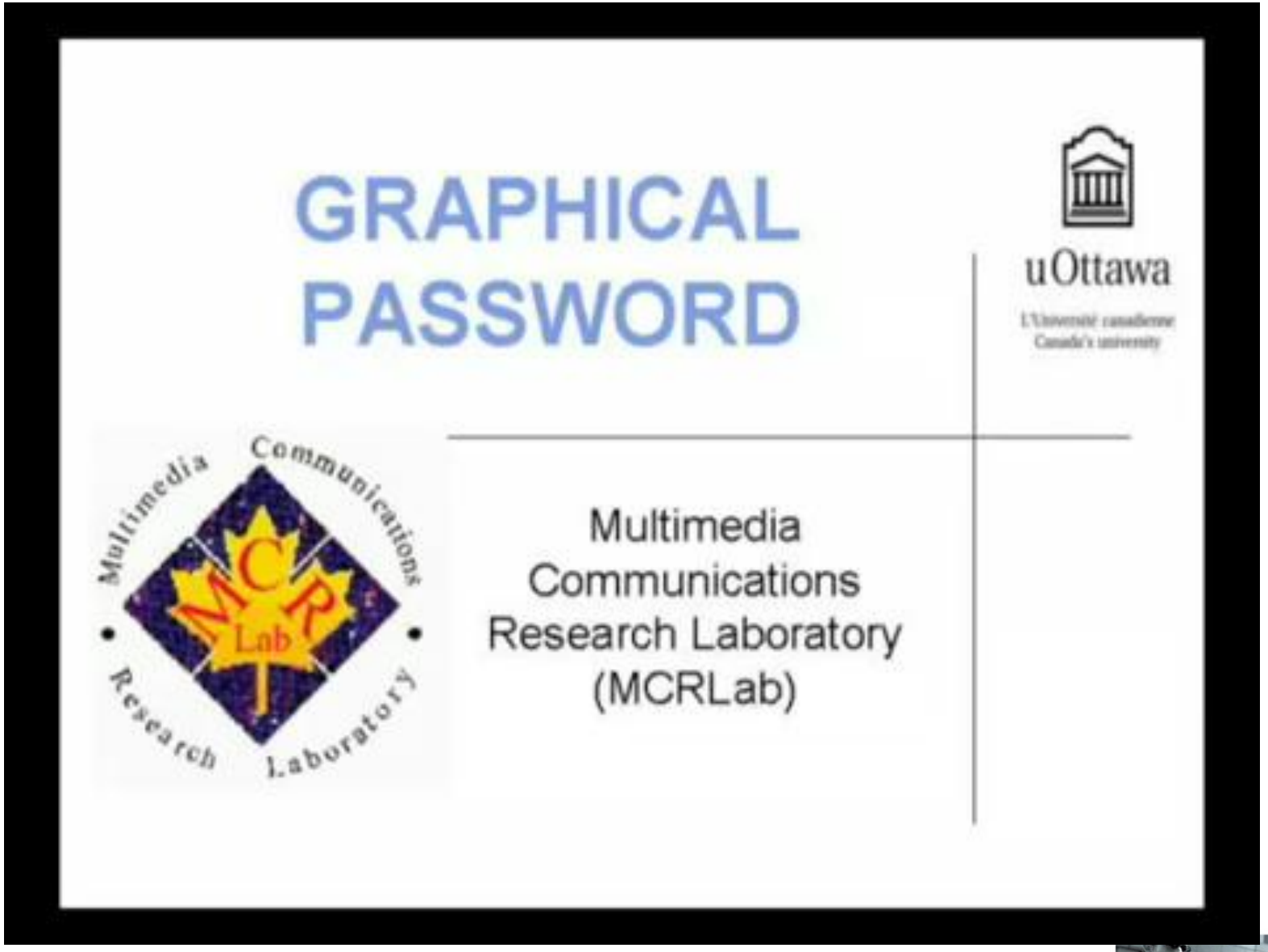
提高網路交易安全　降低他人盜用風險

「Visa驗證」可增加網路交易的安全性(圖/卡優新聞網)

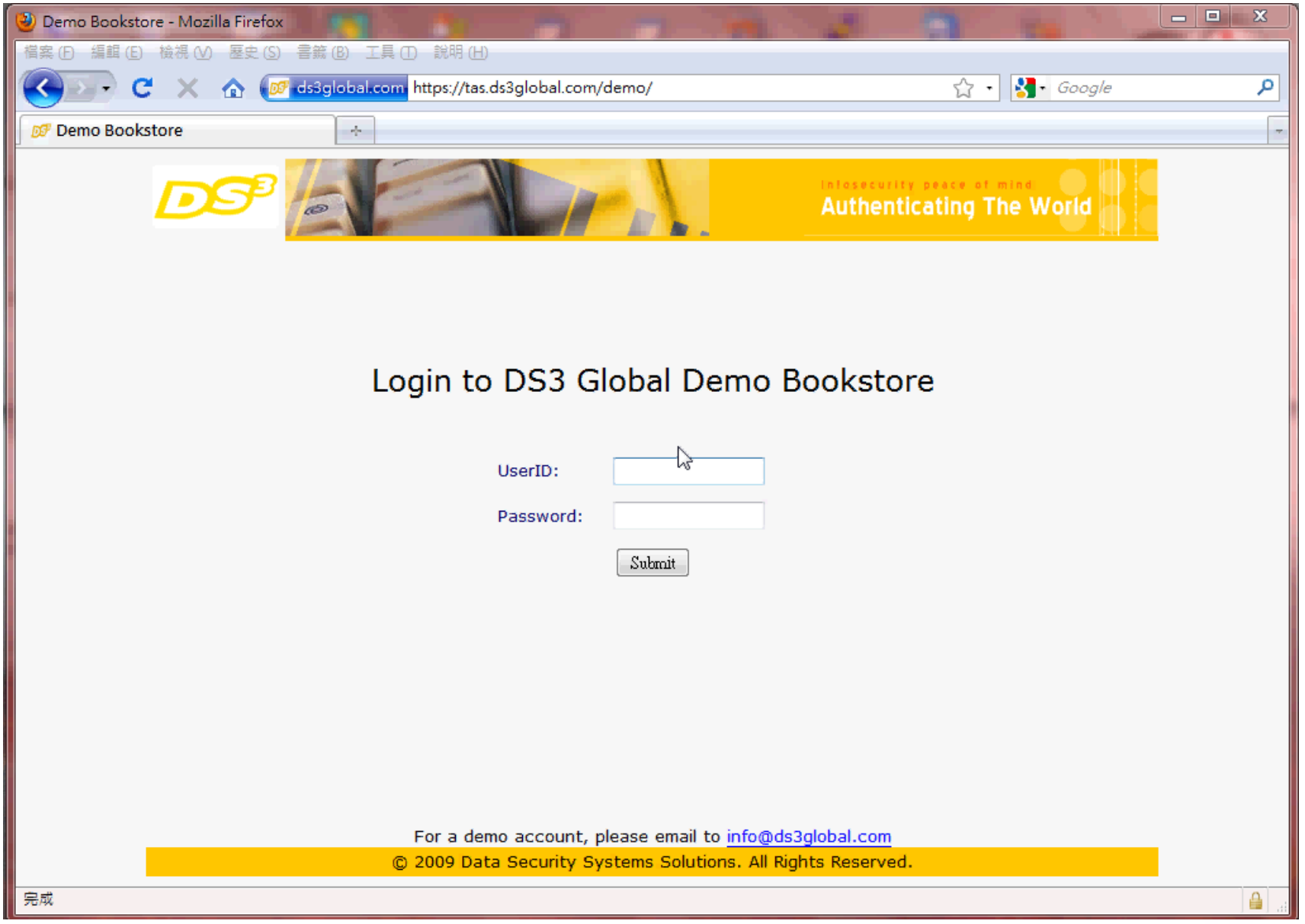
網際網路 | 受保護模式: 啟動　100%

One Time Password

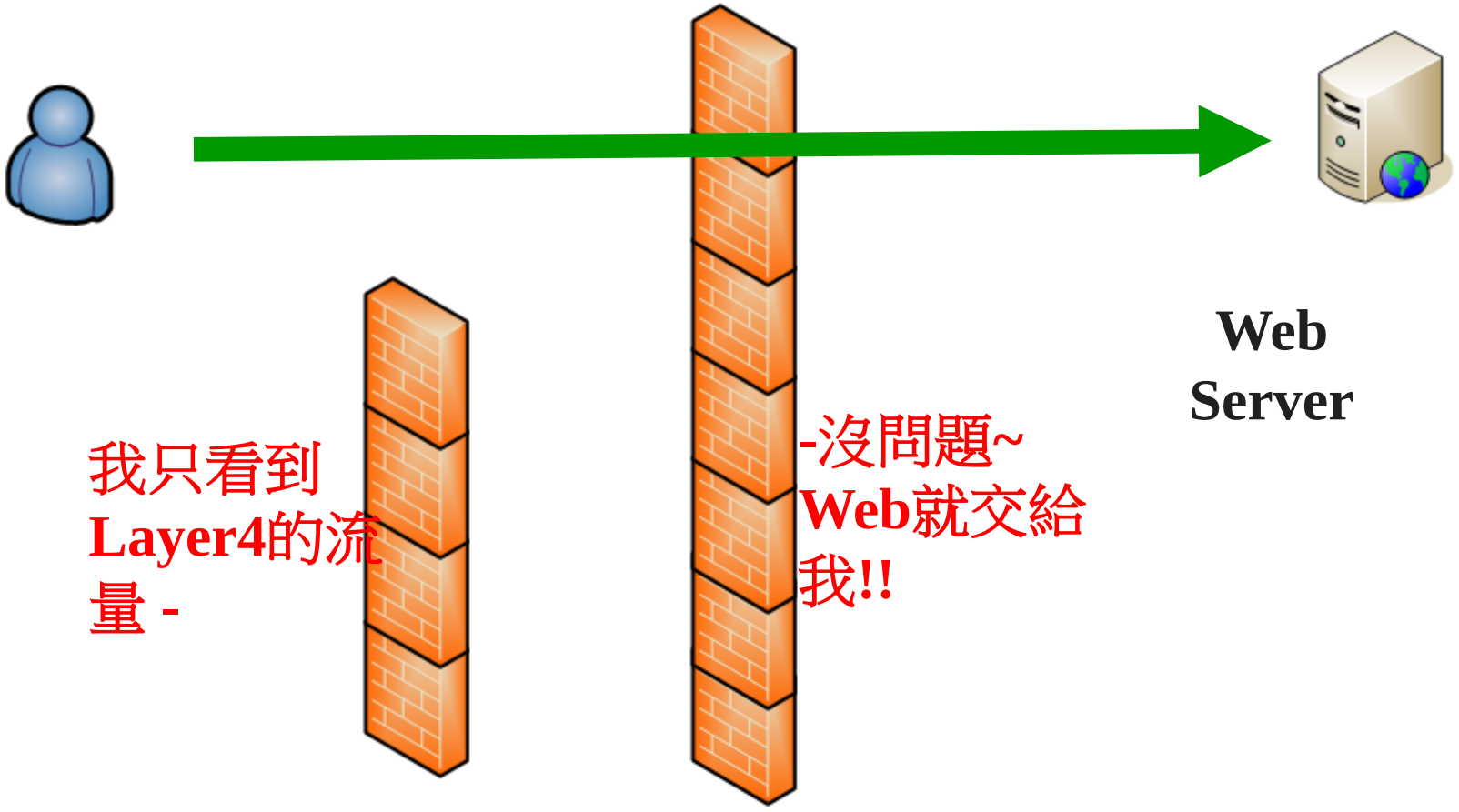
圖形化密碼


GRAPHICAL
PASSWORD
uOttawa
Multimedia
Communications
Research Laboratory
(MCRLab)

One Time Password

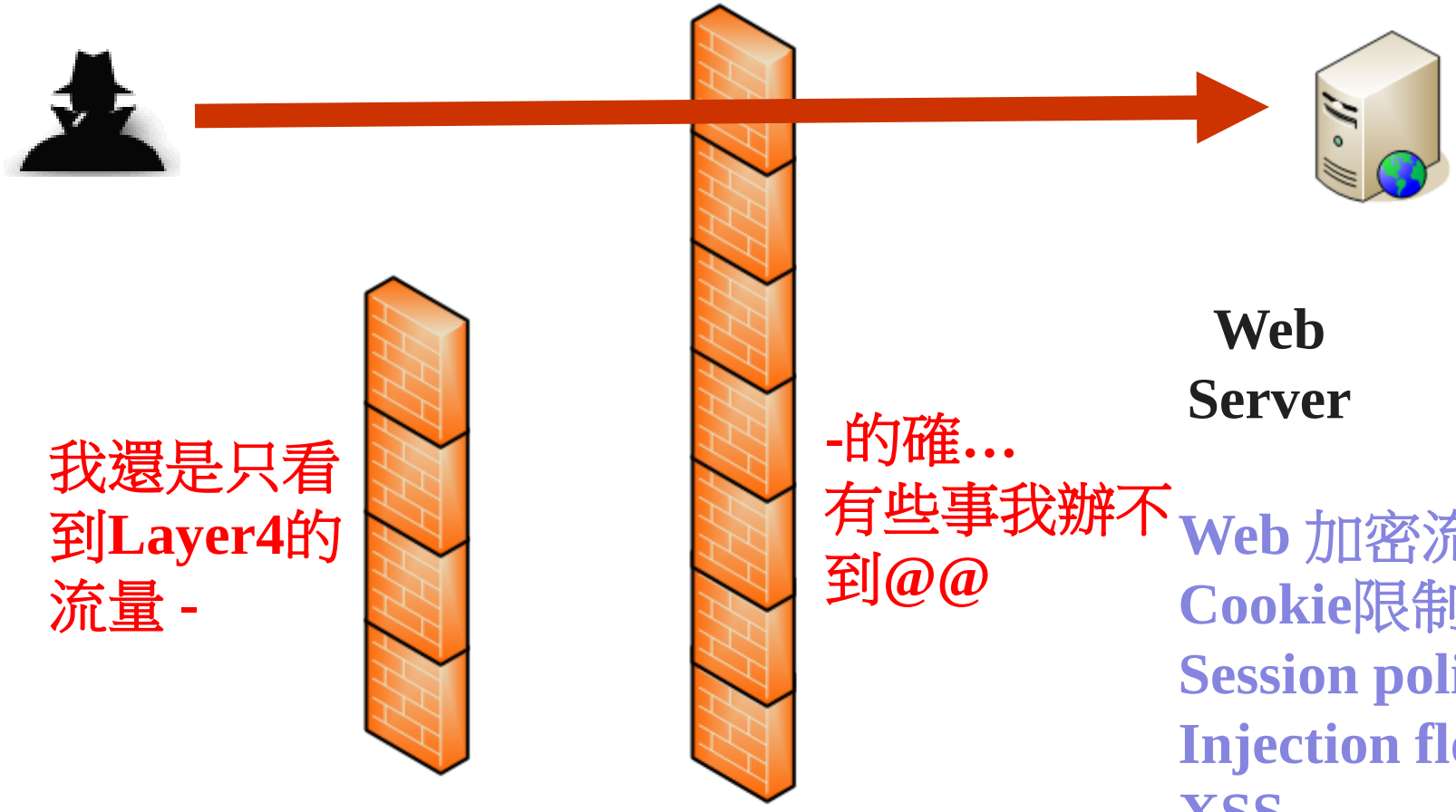


用WAF 保護網站



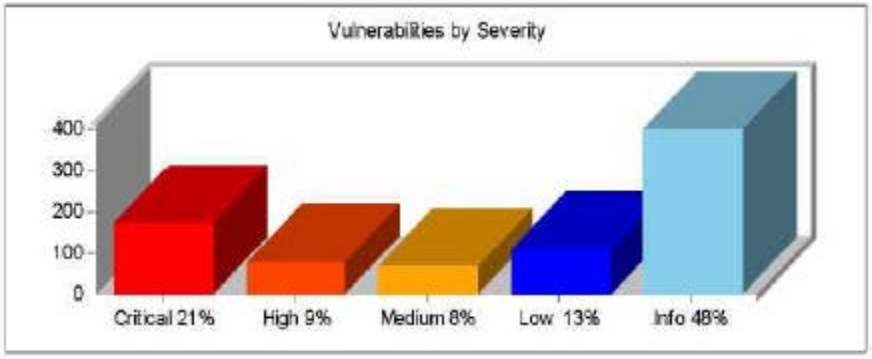
用WAF 保護網站

發生攻擊時

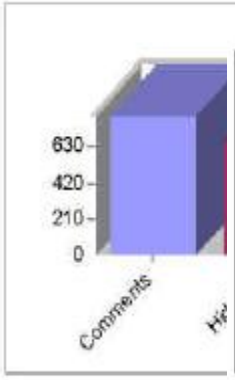


用WAF 保護網站

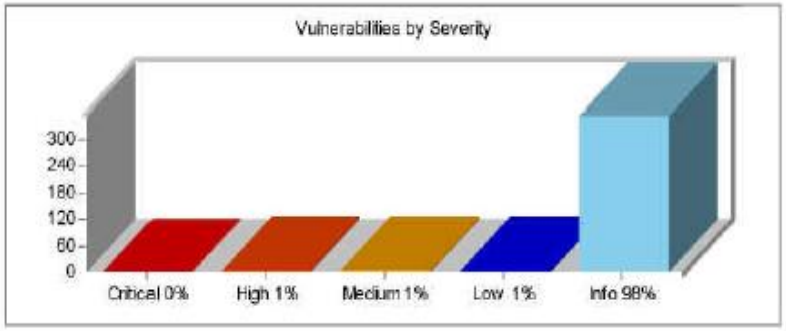
Critical:	175
High:	79
Medium:	67
Low:	110
Info:	401



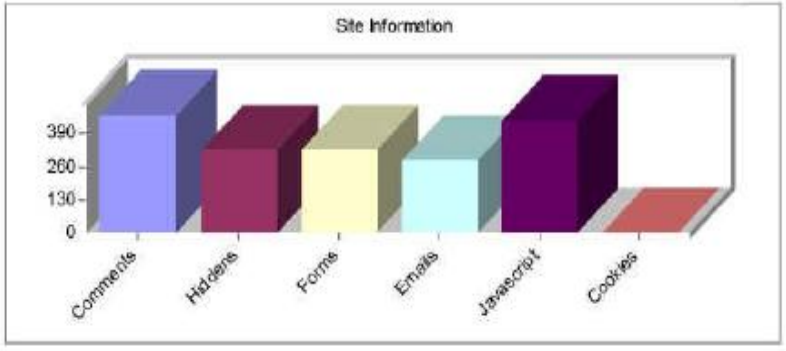
Comments:	810
Hiddens:	656
Forms:	613
Emails:	62
Javascript:	778
Cookies:	3



Critical:	0
High:	3
Medium:	2
Low:	2
Info:	349



Comments:	459
Hiddens:	325
Forms:	321
Emails:	281
Javascript:	442
Cookies:	2



把自己的Code修好

*"**Security 3.0** means changing our approach to security. It is by building security into our processes and applications, by proactive means of finding vulnerabilities before they are created and mitigating the vulnerabilities during the development phase."*

John Prescatore, VP & Distinguished Analyst, Gartner

May 21, 2007, Security-As-A-Service Conference, San Francisco

Security 3.0 表示我們對於確保安全作法的變革。建立安全的程序與應用系統，在弱點被利用之前，從開發階段就主動地找出弱點並修正它。

源始碼檢測報告

深度分析

掃描結果數據概觀

弱點分佈

受到攻擊難易度分析

弱點總數與檔案資訊

詳細內容

檢測開始時間	2008年5月26日 下午06時51分10秒
檢測耗時	46 秒, 760 毫秒
Scanned Files	50
Scanned Lines	8510
Vulnerable Files	21
Vulnerable Statement	66
Resulting Vulnerabi	153
Vuln ntry	9

登入者

使用者 admin
名字 Admin Domain
角色 網域管理者
登出

現行專案

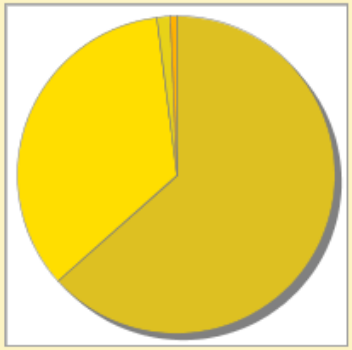
yapig
角色 專案經理
語言 PHP (ver. 4+, 5+)

即時助手

已正確設定專案，可立即進行檢測！
立即檢測！

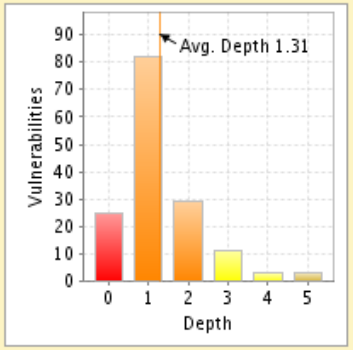
檢測總覽

Vulnerability Distribution



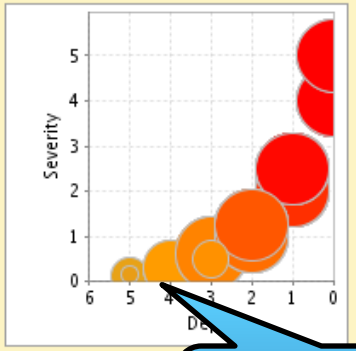
- Cross-Site Scripting (CWE 79)
- Resource Injection (CWE 99)
- HTTP Response S ting (CWE 113)
- File Inclusi 98)

Vulnerability Depth Distribution

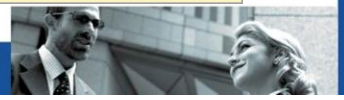


- Directly exposed vulnerabilities
- Vulnerabilities with high risk
- Vulnerabilities at moderate depths
- Vulnerabilities at low exposure depths

Vulnerability Severity Distribution



	問題類型	函式追蹤	嚴重性	Depth	問題位置	進入點
admin_func.php	Cross-Site Scripting (CWE 79)	#1	5.000	0	288	add_gallery.php
functions.php	Cross-Site Scripting (CWE 79)	#1	5.000	0	165	add_gallery.php
thanks_comment.php	Cross-Site Scripting (CWE 79)	#1	5.000	0	10	add_comment.php
add_gallery.php	Cross-Site Scripting (CWE 79)	#1	5.000	0	124	add_gallery.php
admin_func.php	Cross-Site Scripting (CWE 79)	#2	5.000	0	230	add_gallery.php
functions.php	Cross-Site Scripting (CWE 79)	#2	5.000	0	177	add_gallery.php
admin_func.php	Resource Injection (CWE 99)	#3	4.000	0		
admin_func.php	Resource Injection (CWE 99)	#4	4.000	0		
admin_func.php	Resource Injection (CWE 99)	#5	4.000	0		
admin_func.php	Resource Injection (CWE 99)	#6	4.000	0		



掃描報告解析

[Severity Score 2.500]
Vulnerable Entry Point: [redacted]up/act_signup_successful.php

(vulnerable file)
database_mysql_class.php
[query()]

On line 216 of database_mysql_class.php the known sensitive function **mysql_query** was invoked with the tainted parameter(s) **$sql**.

```
216:                if ($this->result_id=mysql_query($sql,$this->link_id)){
```

act_signup_successful.php

On line 61 of act_signup_successful.php , **function query($sql)** was invoked with the tainted parameter(s) **tainted variable(s) $q_str**.

```
61: $db->query($q_str);
```

On line 60 of act_signup_successful.php variable **$q_str** gets assigned a tainted value .

```
60: $q_str='select sum(if(idnum="'.$idnum1.'",1,0)) as tmp1,sum(if(idnum="'.$idnum2.'",1,0)) as
tmp2,sum(if(idnum="'.$idnum3.'",1,0)) as tmp3 ,sum(if(stage="'.$stage.'",1,0)) as tmp4 from
kids_act_signup ';
```

(tainted origin)
act_signup_successful.php

On line 12 of act_signup_successful.php variable **$idnum3** gets assigned a tainted value .

```
12: $idnum3=$_REQUEST['idnum3'];
```

沒檢查就進行資料庫查詢!
SQL Inj.!

到底那個需要過濾?

原始使用者輸入

搜尋引擎使用安全

http://www.siteadvisor.com/

搜尋引擎使用安全

http://securebrowsing.finjan.com


趨勢科技WTP - Windows Internet Explorer
Trend Micro WTP Add-On
TREND MICRO WTP Add-On
安全設定
Proxy設定
啓動網頁威脅防護
查詢方式：
加密的 HTTP
保護層級：
中
啓動僵屍病毒掃瞄
監視 HTTP 要求
監視 SMTP 流量
監視 IRC 要求
監視 DNS 查詢
偵測到威脅時顯示通知
立即更新
確定
取消

Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this URL is benign. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this URL is malicious.

Submission date: **2011-05-23 12:18:36 (UTC)**
Current status: **finished**
Antivirus report: View downloaded file analysis
Webscan result: **0 /16 (0.0%)**

VT Community

not reviewed
Safety score: -

Compact

Print results

URL analysis tool	Result
Avira	Clean site
BitDefender	Clean site
Dr.Web	Clean site
Firefox	Clean site
G-Data	Clean site
Google Safebrowsing	Clean site
Malc0de Database	Clean site
MalwareDomainList	Clean site
Opera	Clean site
ParetoLogic	Clean site
Phishtank	Clean site
TrendMicro	Clean site
Websense ThreatSeeker	Clean site
Wepawet	Clean site

- V
- 38
- ht

免費雲端掃毒工具

- VirSCAN.org：
- 目前支援 37 款防毒引擎
- http://www.virscan.org/

結　論

雲端是個概念 不是新技術

雲端目的為親近使用者

黑客會善用雲端資源來...黑黑黑

使用者需提高安全意識 善用防護工具

問題討論

Thank you!

Hoyeh_tsai@kh.ringline.com.tw

07-5569402#7736