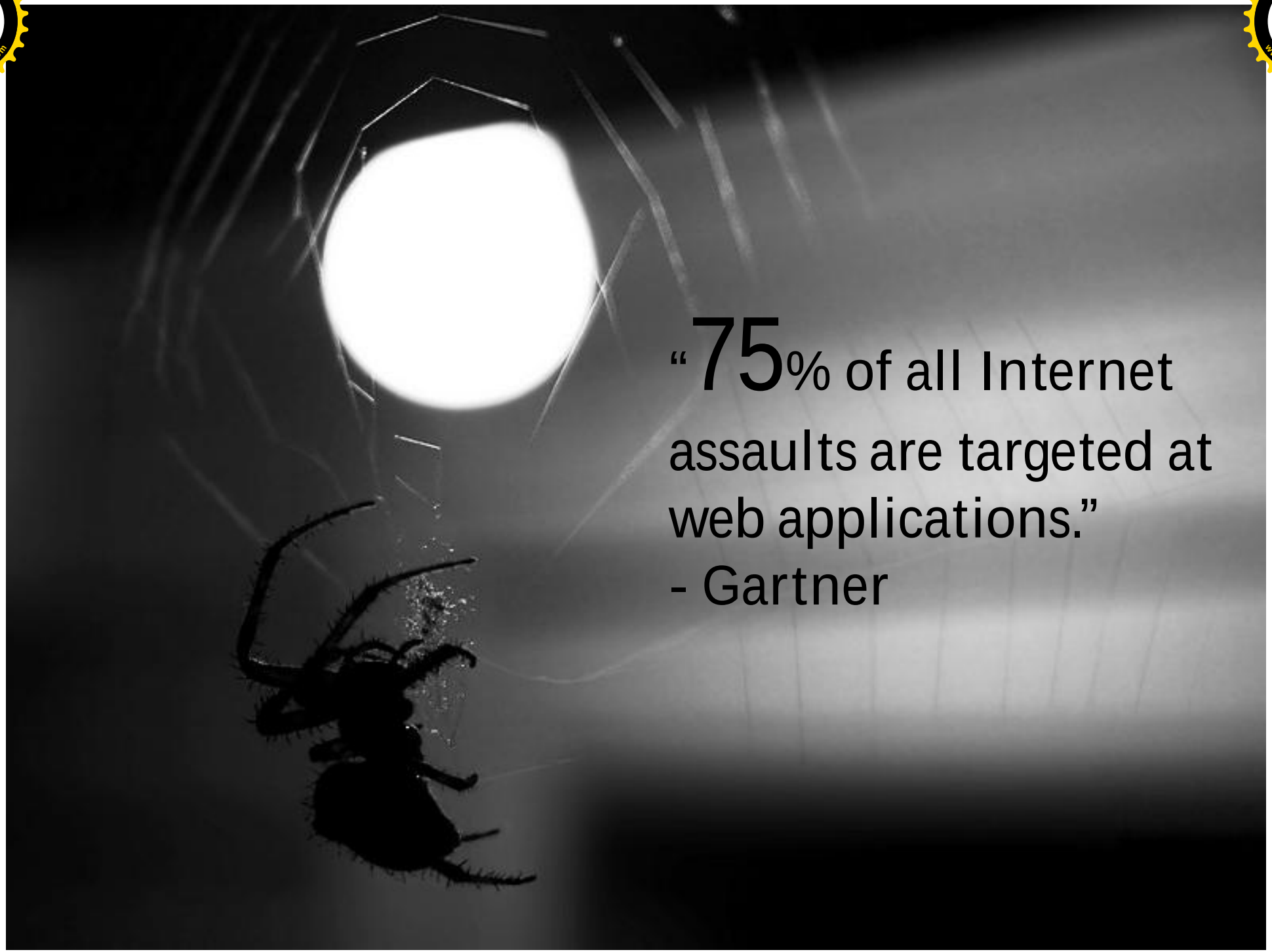

# 常見攻擊手法與防護

敦陽科技 蘇展志

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

# 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





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

| 事件 | | 日期 | 主機 | 站名/抬頭 | 來源 | 作業系統 | 工具 |
|---|---|---|---|---|---|---|---|
| | | 2008-09-10 | www.multimedia.com.tw | 妙題整合行銷 | Zone-h | Win 2003 | |
| | | 2008-09-10 | www.caric.com.tw | Caric伴侶動物研究訊息中心 | Zone-h | Win 2003 | |
| | | 2008-09-10 | www.ivote.com.tw | I VOTE愛投網 | Zone-h | Win 2003 | |
| | | 2008-09-09 | tourism.chna.edu.tw | 嘉南藥理科技大學觀光事業管理系 | Zone-h | Linux | |
| | | 2008-09-09 | www.itschic.com.tw | 逸如媚國際美容有限公司 | Serapis | | |
| | | 2008-09-09 | www.cncxyz.com.tw | 東永生股份有限公司 | Zone-h | Linux | |
| | | 2008-09-09 | it.tsangyow.com.tw | 倉佑資訊 | Zone-h | Win 2003 | |
| | | 2008-09-09 | www.cit.org.tw | 中華民國運輸學會 | Zone-h | Win 2000 | |
| | | 2008-09-09 | www.evenbetter.com.tw | 均沛實業 | Zone-h | Win 2000 | |
| | | 2008-09-09 | www.lunghwa.com.tw | Lung Hwa | Zone-h | Win 2000 | |
| | | 2008-09-09 | www.yourlife.tw | 生活資訊 | Zone-h | Linux | |
| | | 2008-09-09 | www.ultima.com.tw | 大騰電子 | Zone-h | Win 2000 | |
| | | 2008-09-09 | www.paris-miki.com.tw | 巴黎三城眼鏡 | Zone-h | Win 2003 | |
| | | 2008-09-09 | counter.calling.com.tw | 計數器 | Zone-h | Linux | |
| | | 2008-09-09 | web.calling.com.tw | CALLING WEB - 網站連結 | Zone-h | Linux | |
| | | 2008-09-09 | www.gdiy.com.tw | 好點子GOOD-DIY生活網 | Zone-h | Linux | |
| | | 2008-09-09 | www.chyfood.com.tw | 振福源企業有限公司 | Zone-h | Linux | |

網站導覽
本局介紹
新聞活動
犯罪預防
通緝令追追追
刑事鑑識科學
國際刑警
刑事雙月刊
影音資料專區
文件下載專區
便民服務專區
相關網站連結
中英雙語詞彙
民意調查
與我們連繫
回首頁



# 新聞活動 NEWS

新聞快訊 | 公告事項 | 活動&資訊公開
新聞快訊
友善列印 轉寄好友

| | |
|---|---|
| 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）<br>徐○玲（女、23歲）<br>余○群（男、37歲）<br>游○鴻（男、32歲）<br>王○志（男、30歲）<br>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 |



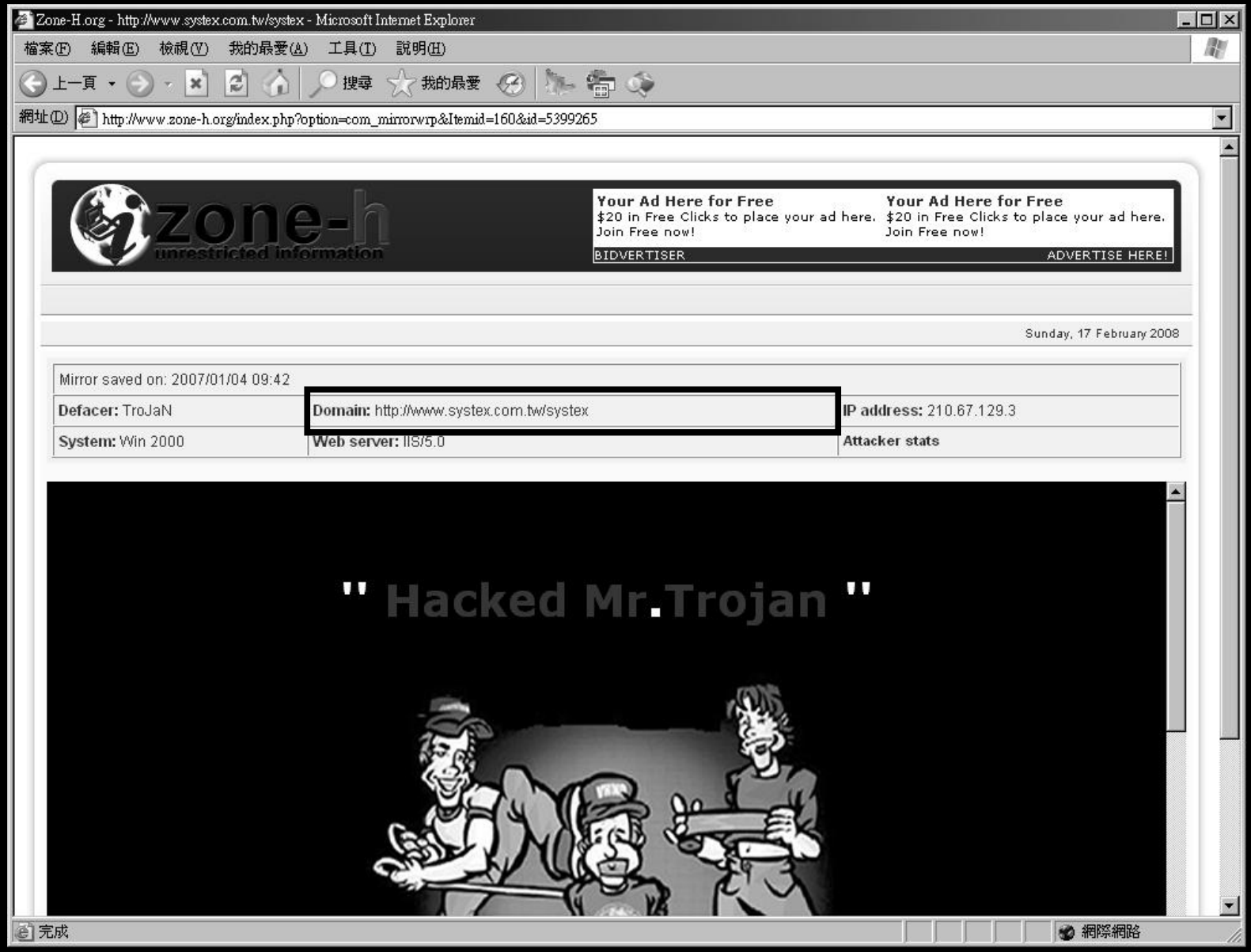
PDF-XChange
Click to buy NOW!
www.docu-track.com

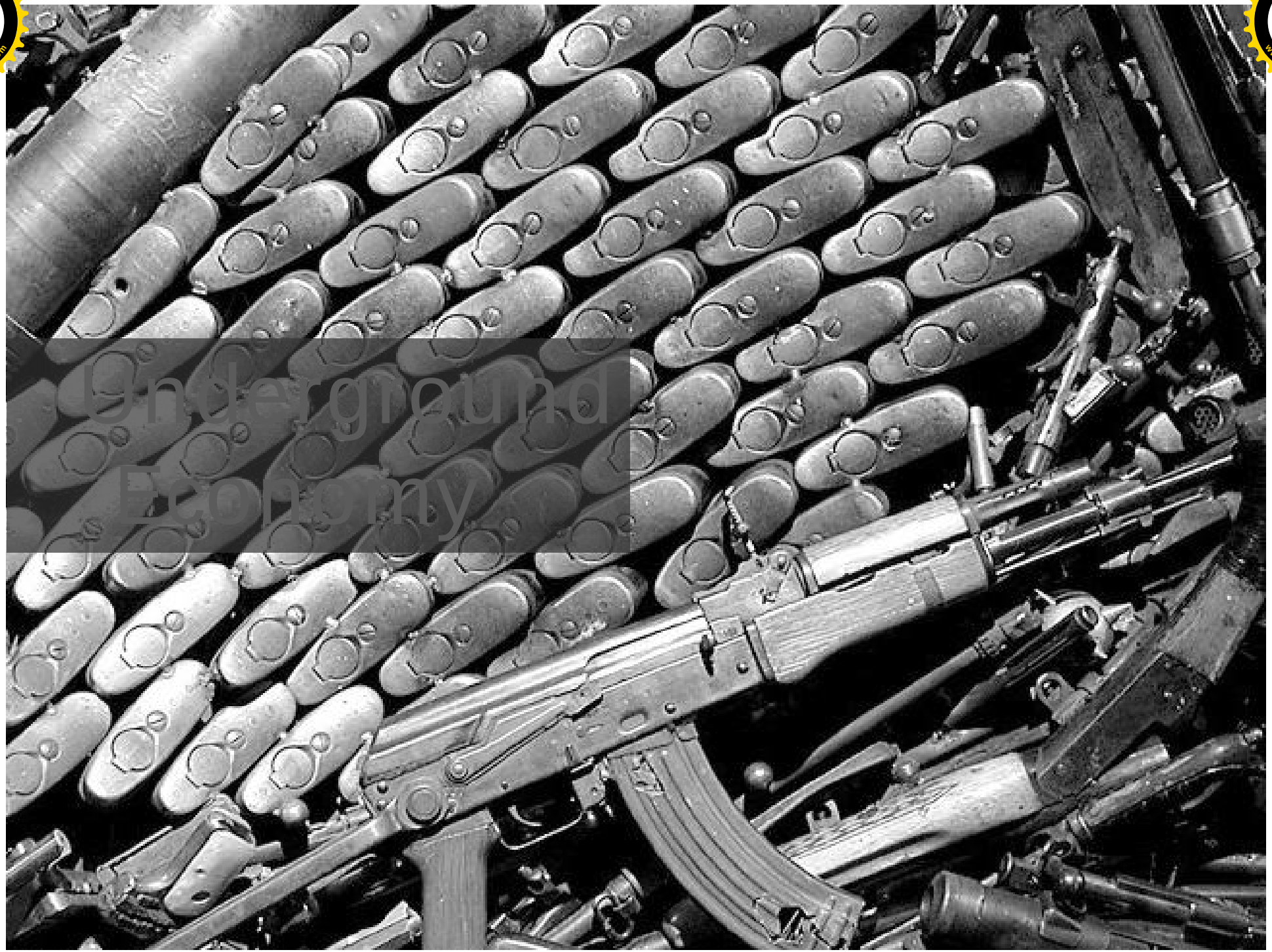


PDF-XChange
Click to buy NOW!
www.docu-track.com


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) 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
所有網頁 圖片 新聞 網上論壇 網誌搜尋 Gmail 更多▼ 登入
Google
教主專用Asp後門 inurl:help.asp filetype:asp site:tw
搜尋
進階搜尋 | 使用偏好
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
網際網路

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



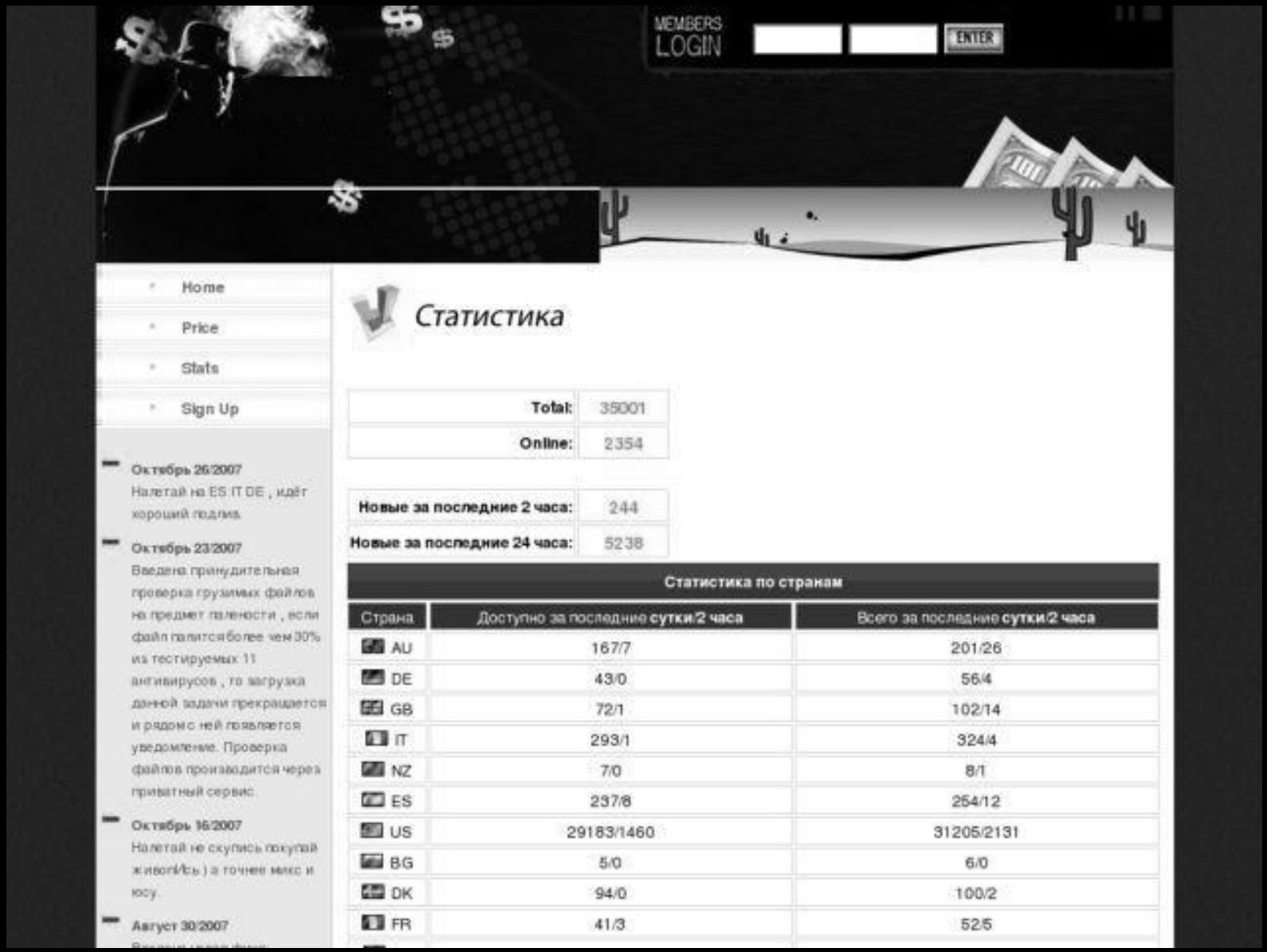



PDF-XChange
Click to buy NOW!
www.docu-track.com

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


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


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



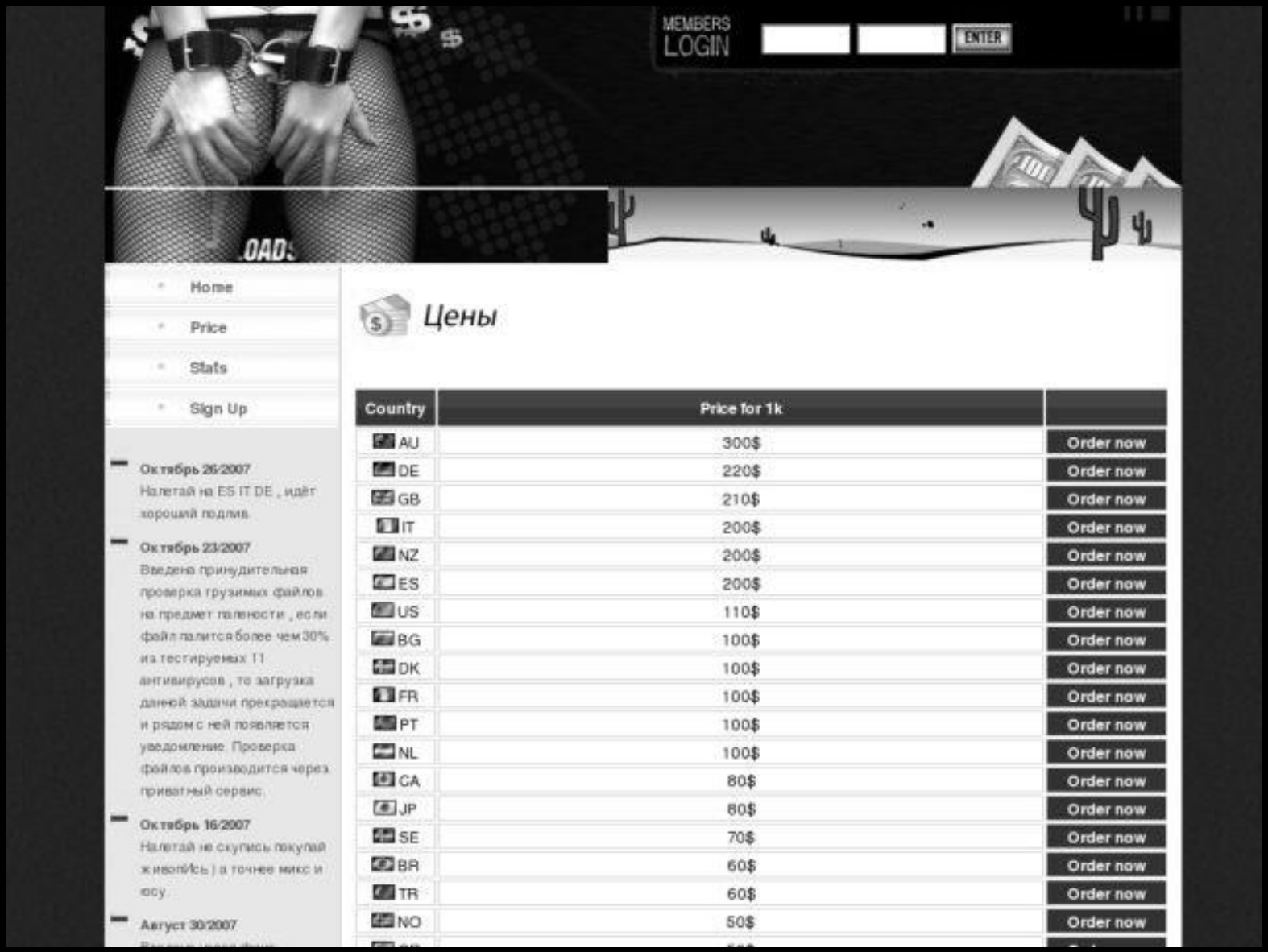

## Статистика

| | |
|---|---|
| **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 |



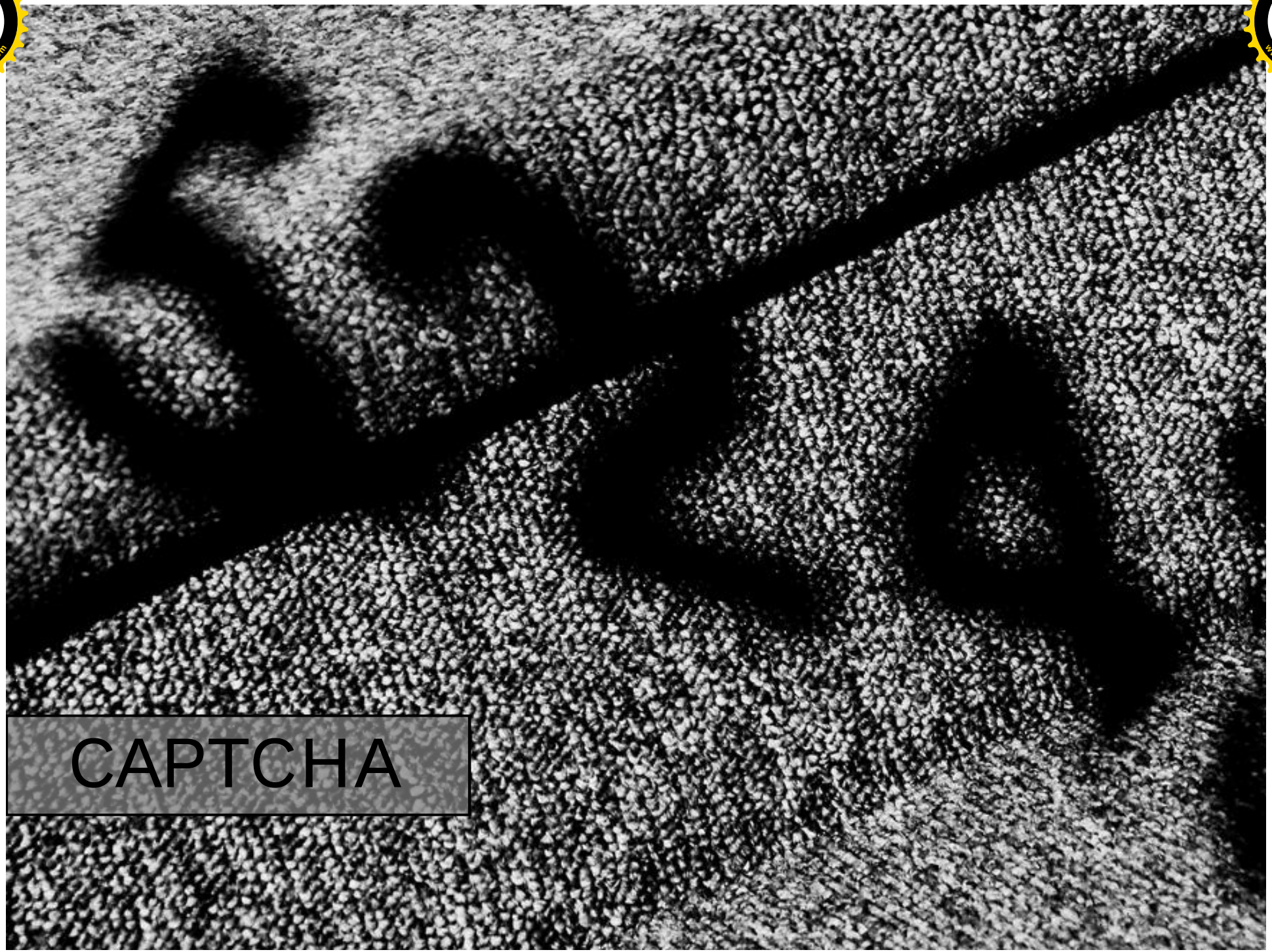
# 肉雞

| | | | | | |
|---|---|---|---|---|---|
| | [09.04]網逝鋤雲服務器後門 NEW | W1984<br>2008-09-04 | 4 | 53 | 2008-09-04 23:25<br>by: 羽de翼 |
| | [09.03]出售流量肉雞 | 494026212<br>2008-09-03 | 1 | 58 | 2008-09-04 01:17<br>by: 3389其黑 |
| | [09.01]出售自己編寫的1433抓雞工具 | sloat2008<br>2008-09-01 | 1 | 56 | 2008-09-03 15:17<br>by: zwz003 |
| | [07.28]出售大量肉雞並提供DDOS服務！老字號 | 龍寶寶<br>2008-07-28 | 4 | 120 | 2008-09-03 15:11<br>by: simon |
| | [09.02]急求7位QQ | 120115708<br>2008-09-02 | 5 | 74 | 2008-09-03 12:54<br>by: ayz |
| | [09.01]出售幾個免殺遠控，剛更新的 ( -5 ) [ 1 2 ] | jzysd<br>2008-09-01 | 15 | 120 | 2008-09-03 00:50<br>by: hongonly |
| | [07.16]要鴿子免殺DAT的來 [ 1 2 ] | t.y.p<br>2008-07-16 | 11 | 276 | 2008-09-02 21:37<br>by: fendouandy |
| | [09.02]長期出售盛大金牌帳號激活碼 | 鬼狼<br>2008-09-02 | 0 | 28 | 2008-09-02 13:31<br>by: 鬼狼 |
| | [08.30]出售個日本雞 [ 1 2 ] | 黑夜幽靈<br>2008-08-30 | 12 | 203 | 2008-09-02 02:16<br>by: yycyyc |
| | [09.01]出售幾台全能能服務器， | l45189946<br>2008-09-01 | 1 | 56 | 2008-09-01 19:18<br>by: songjie1230 |
| | [08.31]本人出售抓雞服務器 | 76514996<br>2008-08-31 | 1 | 41 | 2008-09-01 00:08<br>by: ycdd |
| | [08.31]服務器 專業户 | l45189946<br>2008-08-31 | 0 | 34 | 2008-08-31 17:05<br>by: l45189946 |

# 70

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

(McAfee)





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

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

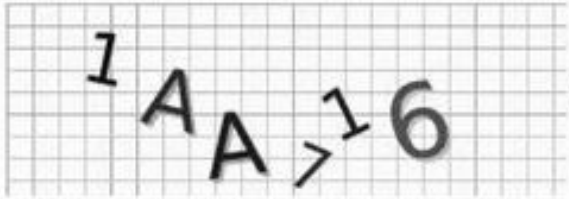
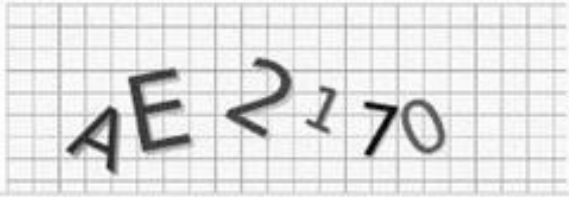
Main menu

- Home
- Contact Us

- Help
- Work
- Practice
- Qualify to Work
- **Tests made**
- Statistics
- Profile
- Logout

| 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 | | Failed |

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

Обновить статистику

**КУПИТЬ:** 100K | Gmail.com | OK

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

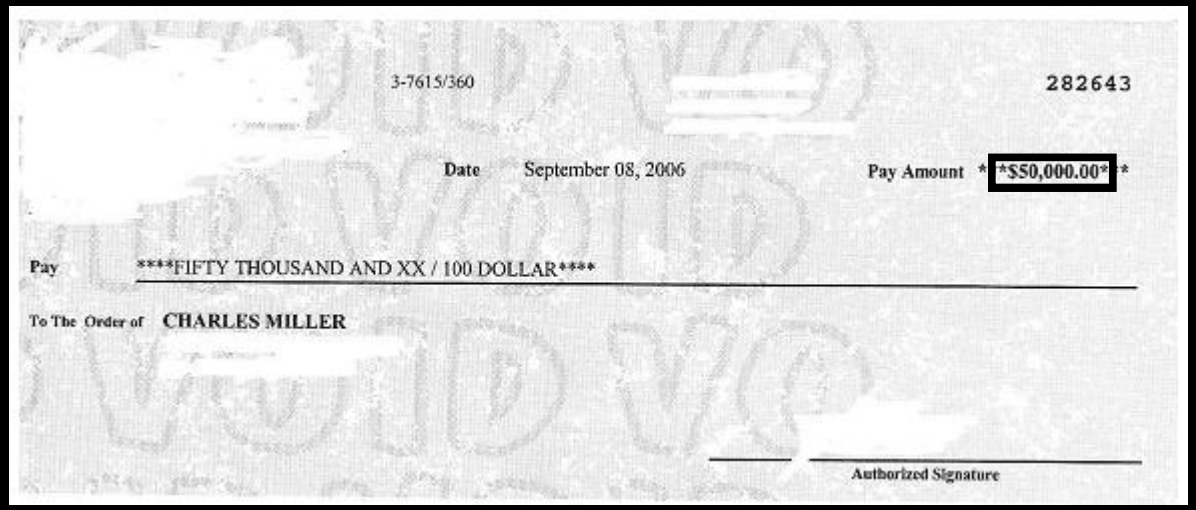
PDF-XChange
Click to buy NOW!
www.docu-track.com

| 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 | $\geq$ $1200 | Ebay auction site [21, 25] |
| Mozilla | $500 | Mozilla bug bounty program [4] |

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

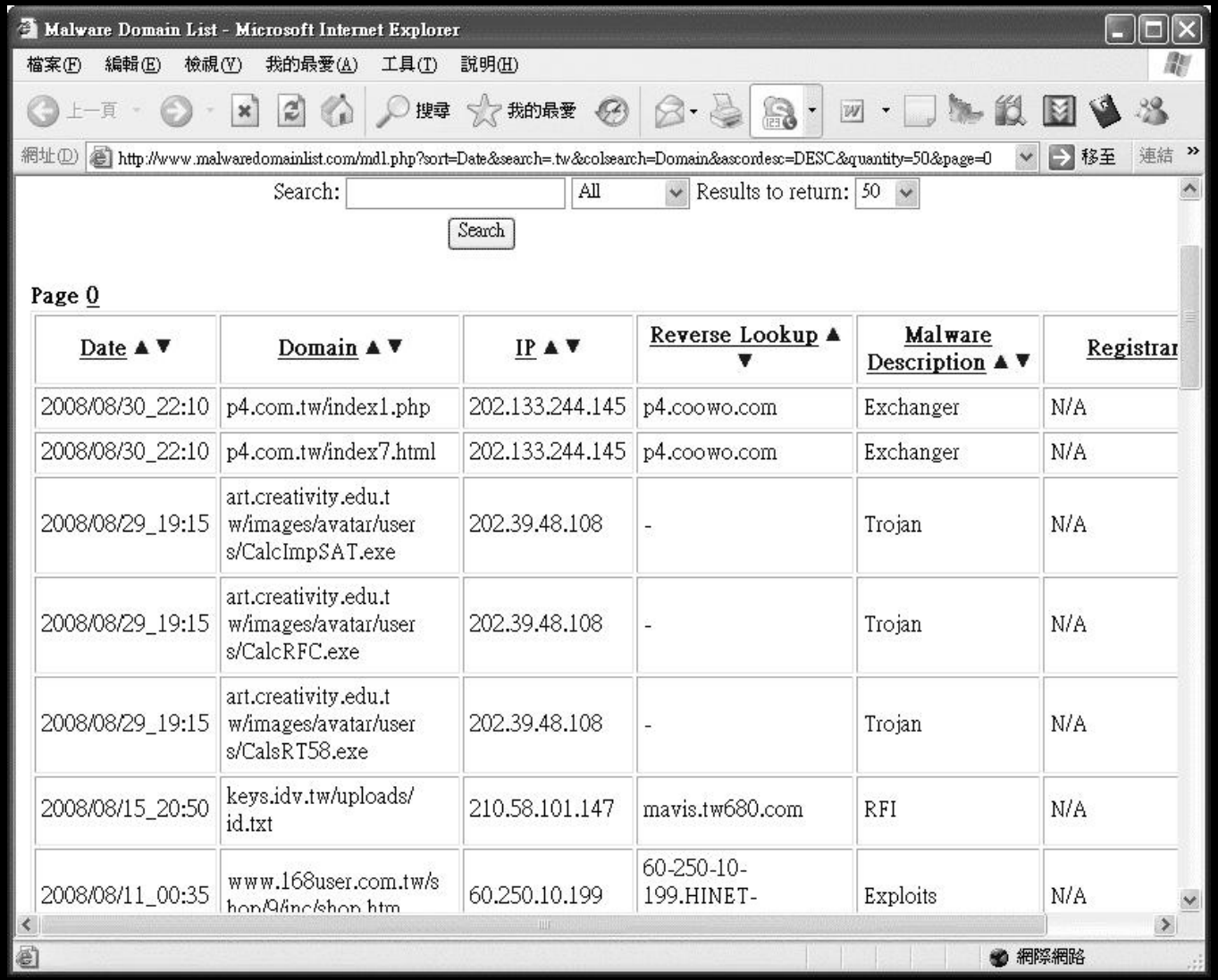
| Date | Action |
|---|---|
| 6/05 | Vulnerability discovered. |
| 11/07/05 | Submitted to prepub review at NSA. |
| 7/27/06 | Approved for release by prepub review. |
| 7/27/06 | Offered to government. |
| 8/10/06 | Verbally agreed to $80K conditional deal. |
| 8/11/06 | Exploit given for evaluation.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

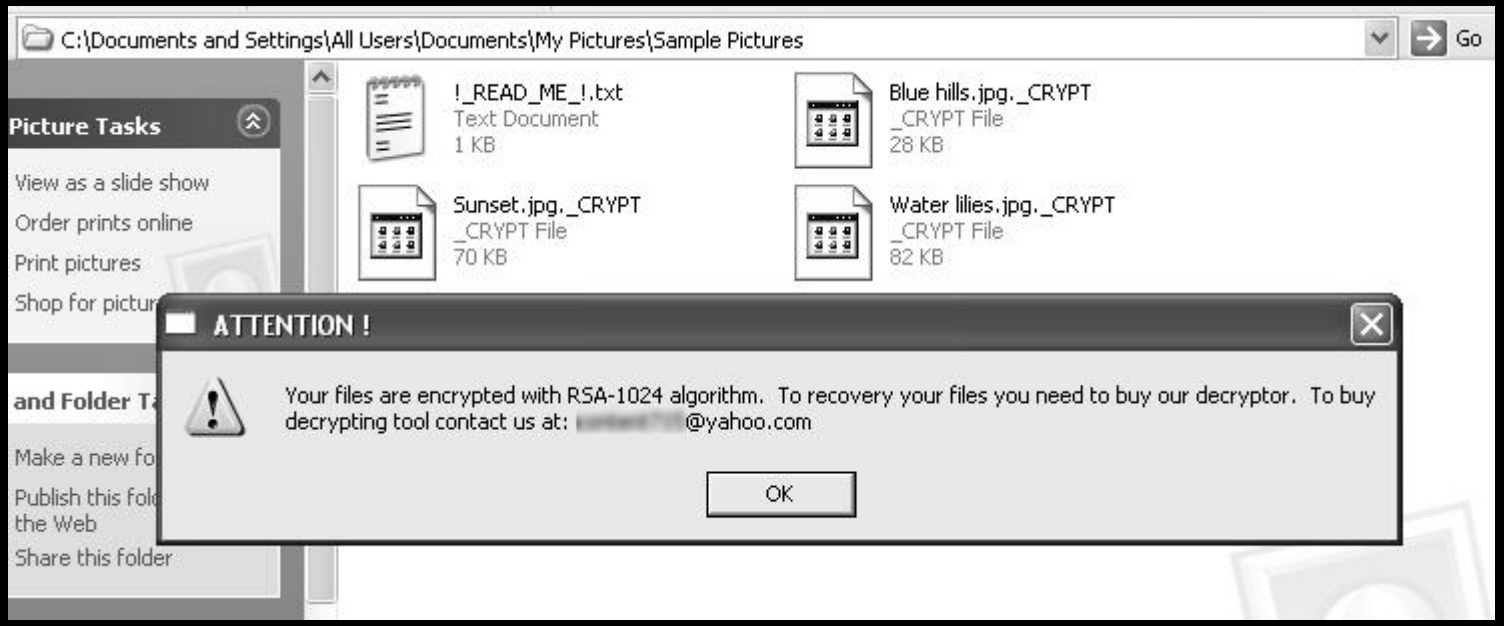
Table 2: "Successful" sale.




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

# Malware Domain List

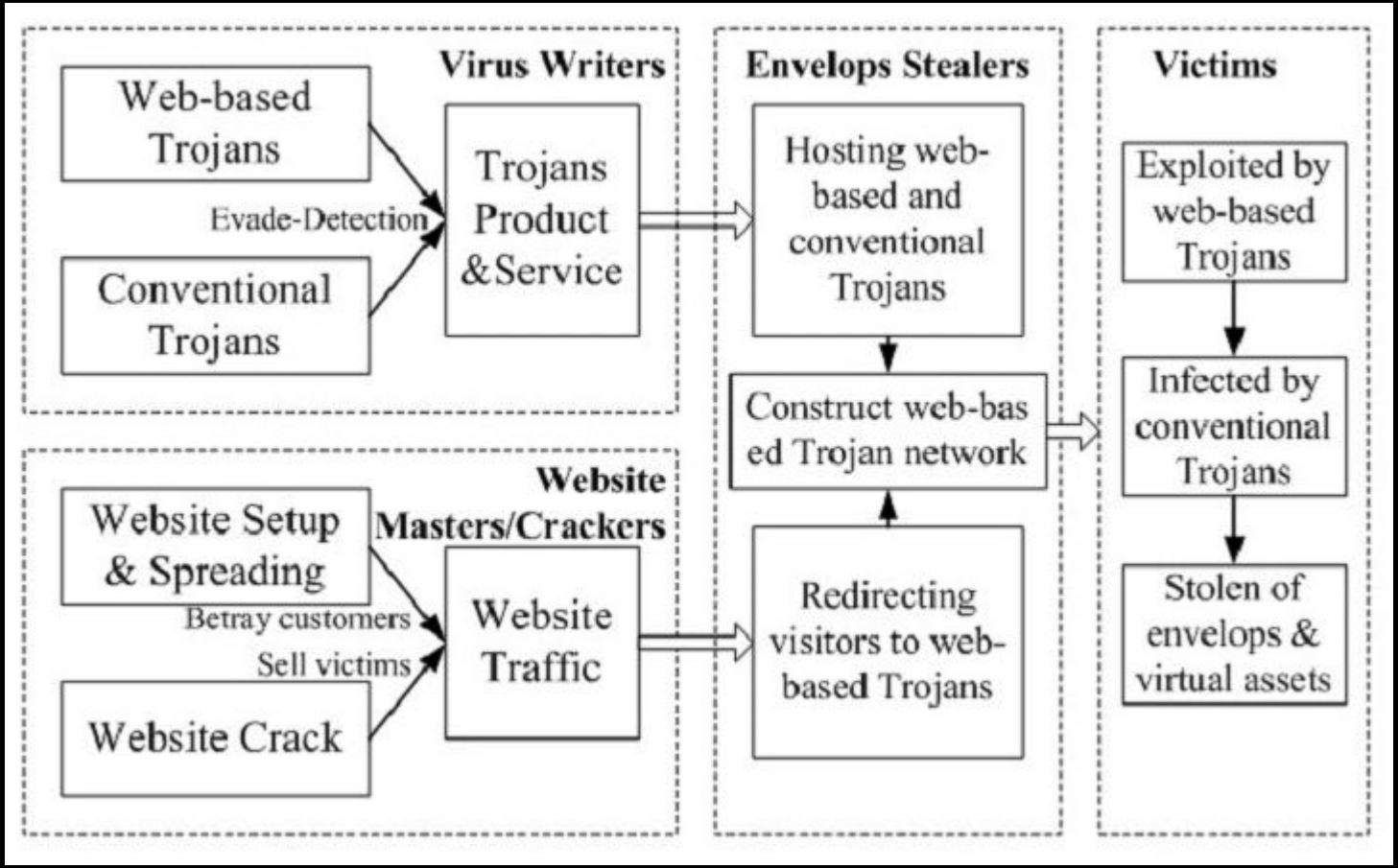


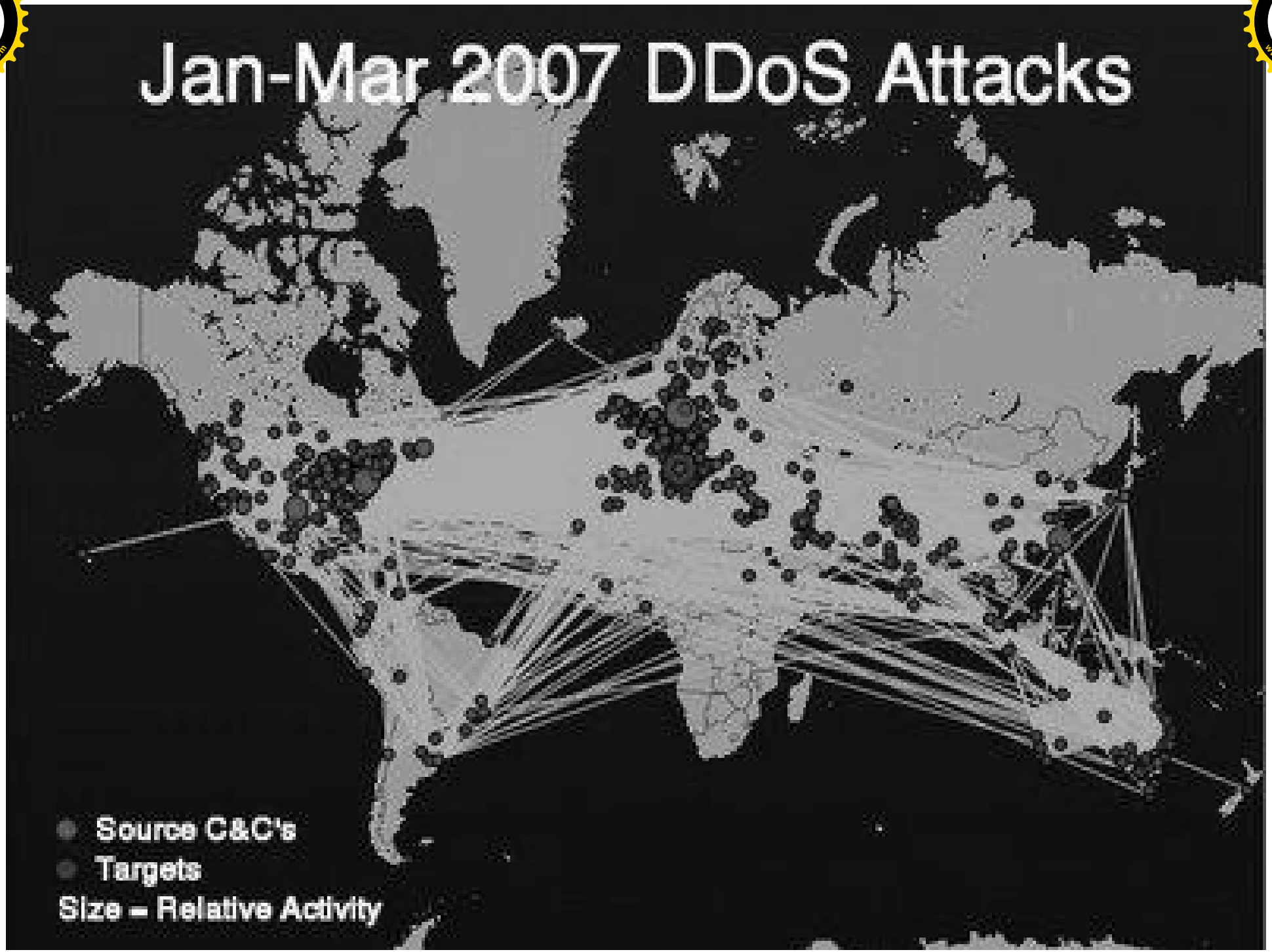




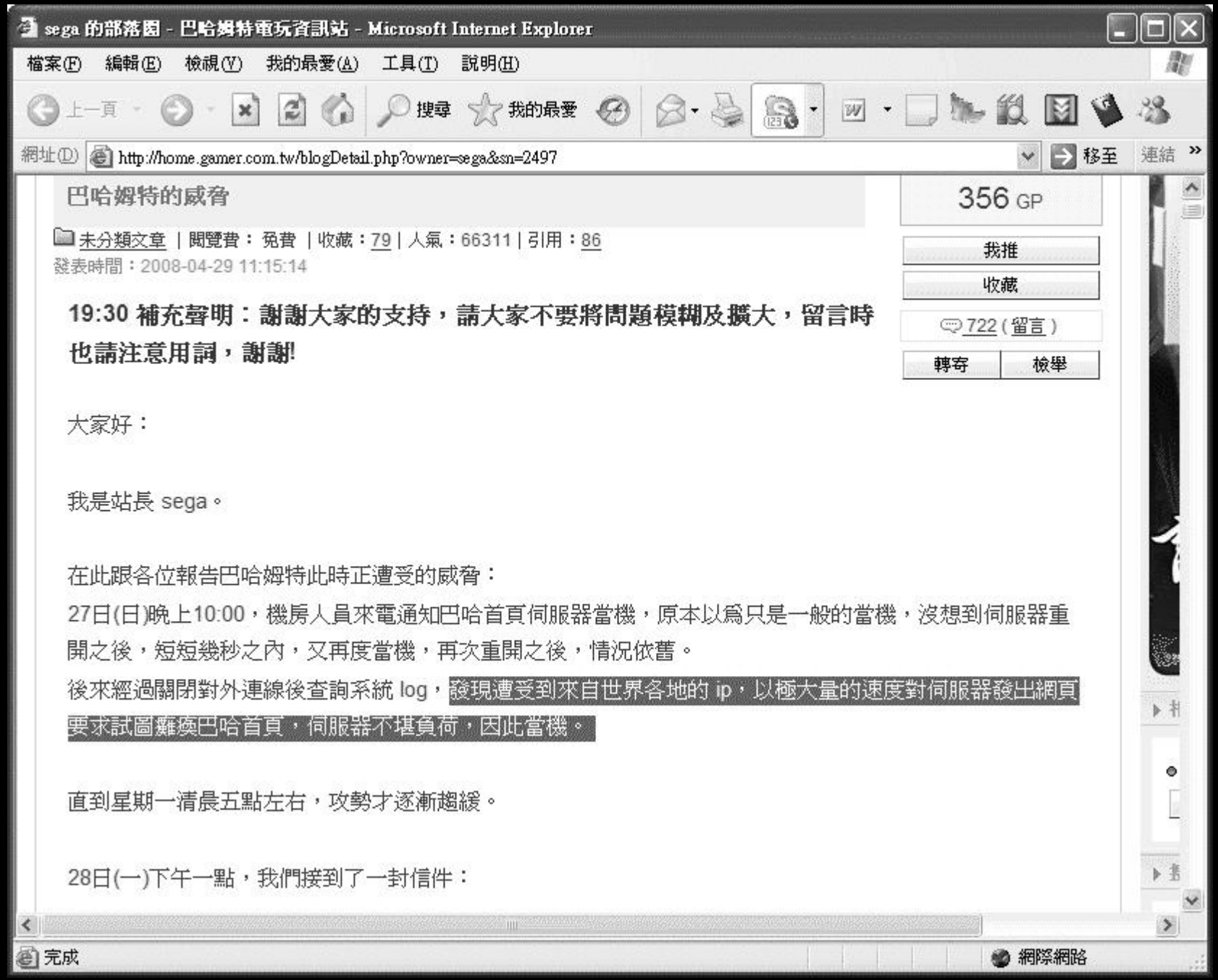
PDF-XChange
Click to buy NOW!
www.docu-track.com

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






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


sega 的部落圈 - 巴哈姆特電玩資訊站 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://home.gamer.com.tw/blogDetail.php?owner=sega&sn=2497
移至 連結
巴哈姆特的威脅
356 GP
我推
收藏
722 ( 留言 )
轉寄 檢舉
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
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：
完成
網際網路

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

[ exploits/shellcode ]

| -::DATE | -::DESCRIPTION | -::HITS | | | | | -::AUTHOR |
|---|---|---|---|---|---|---|---|
| 2008-07-14 | Yahoo Messenger 8.1 ActiveX Remote Denial of Service Exploit | 4934 | R | | D | X | Jeremy Brown |
| 2008-06-03 | C6 Messenger ActiveX Remote Download & Execute Exploit | 5334 | R | | D | X | Nine:Situations:Group |
| 2007-09-19 | Yahoo! Messenger 8.1.0.421 CYFT Object Arbitrary File Download | 14217 | R | | D | X | shinnai |
| 2007-09-03 | Telecom Italy Alice Messenger Remote registry key manipulation Exploit | 6134 | R | | D | X | rgod |
| 2007-09-01 | Yahoo! Messenger (YVerInfo.dll <= 2007.8.27.1) ActiveX BoF Exploit | 9577 | R | | D | X | minhbq |
| 2007-08-29 | Yahoo! Messenger 8.1.0.413 (webcam) Remote Crash Exploit | 5801 | R | | D | | wushi |
| 2007-08-29 | MSN messenger 7.x (8.0?) VIDEO Remote Heap Overflow Exploit | 22664 | R | | D | | wushi |
| 2007-06-08 | Yahoo! Messenger Webcam 8.1 (Ywcupl.dll) Download / Execute Exploit | 14642 | R | | D | | Excepti0n |
| 2007-06-08 | Yahoo! Messenger Webcam 8.1 (Ywcvwr.dll) Download / Execute Exploit | 7884 | R | | D | | Excepti0n |
| 2007-06-07 | Yahoo! Messenger Webcam 8.1 ActiveX Remote Buffer Overflow Exploit 2 | 7619 | R | | D | X | Excepti0n |
| 2007-06-07 | Yahoo! Messenger Webcam 8.1 ActiveX Remote Buffer Overflow Exploit | 5863 | R | | D | X | Excepti0n |
| 2007-04-09 | PHP121 Instant Messenger 2.2 Local File Inclusion Vulnerability | 3513 | R | | D | | Dj7xpl |
| 2006-04-15 | Novell Messenger Server 2.0 (Accept-Language) Remote Overflow Exploit | 10382 | R | M | D | | H D Moore |
| 2006-04-12 | PHP121 Instant Messenger <= 1.4 Remote Code Execution Exploit | 5178 | R | | D | | rgod |
| 2005-02-09 | MSN Messenger PNG Image Buffer Overflow (linux compile) | 10052 | R | | D | | dgr |
| 2005-02-09 | MSN Messenger PNG Image Buffer Overflow Download Shellcoded Exploit | 15532 | R | | D | | ATmaCA |
| 2004-11-15 | Secure Network Messenger <= 1.4.2 Denial of Service Exploit | 2823 | R | | D | | ClearScreen |
| 2004-09-23 | PopMessenger <= 1.60 Remote Denial of Service Exploit | 3272 | R | | D | | Luigi Auriemma |
| 2004-09-02 | AOL Instant Messenger AIM "Away" Message Remote Exploit | 7798 | R | M | D | | John Bissell |
| 2004-08-14 | AOL Instant Messenger AIM "Away" Message Local Exploit | 4036 | R | | D | | mandragore |
| 2004-08-08 | MS Messenger Denial of Service Exploit (MS03-043) (linux ver) | 3871 | R | | D | | VeNoMouS |
| 2003-12-16 | MS Windows Messenger Service Remote Exploit FR (MS03-043) | 8246 | R | | D | | MrNice |
| 2003-10-18 | MS Windows Messenger Service Denial of Service Exploit (MS03-043) | 5380 | R | | D | | LSD-PLaNET |
| 2003-06-23 | Yahoo Messenger 5.5 Remote Exploit (DSR-ducky.c) | 6062 | 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.

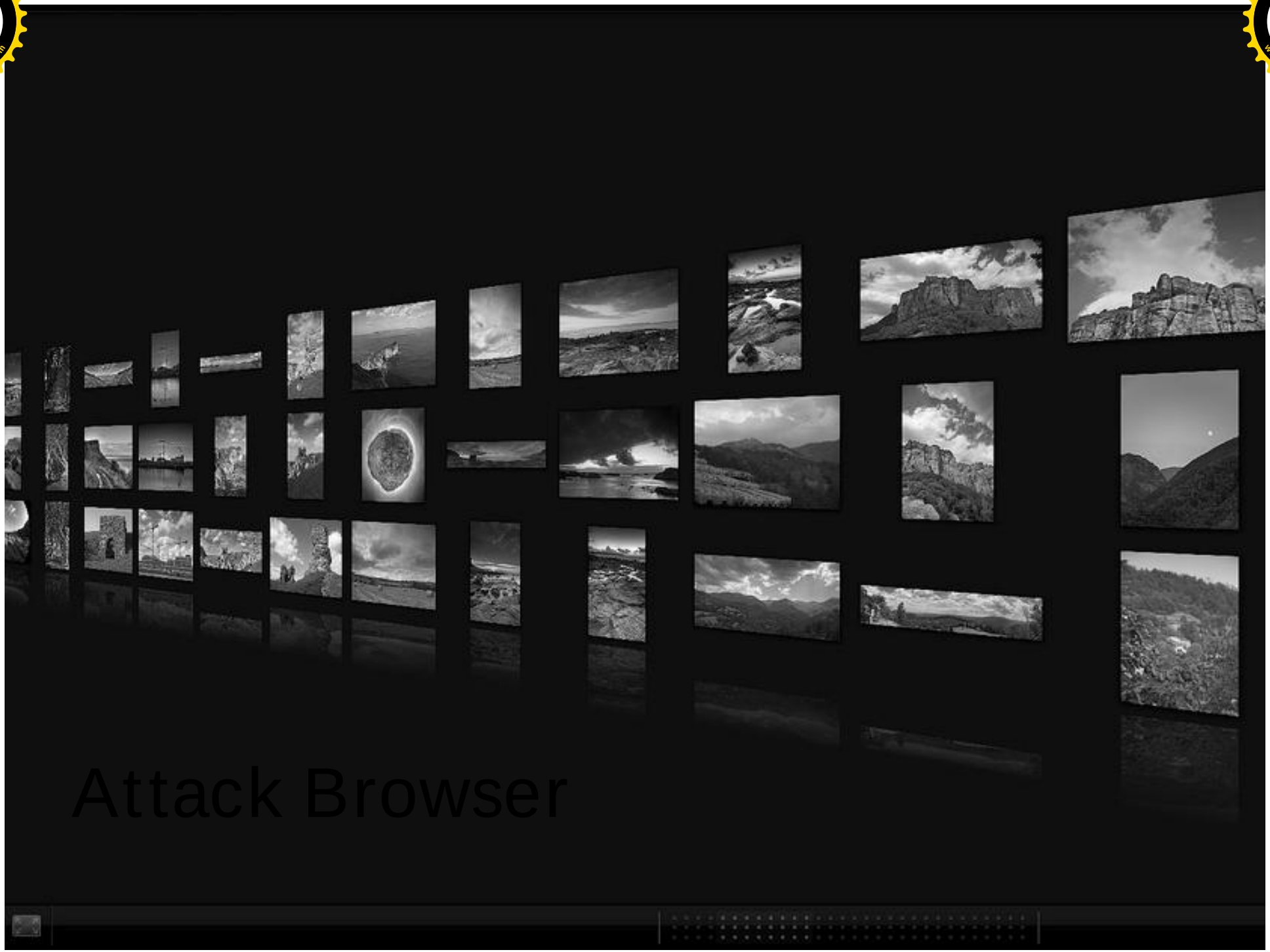
The IM Security Team in partnership with our customers and leading security and messaging companies identify and automatically protect our customers against these threats.

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 |

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



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

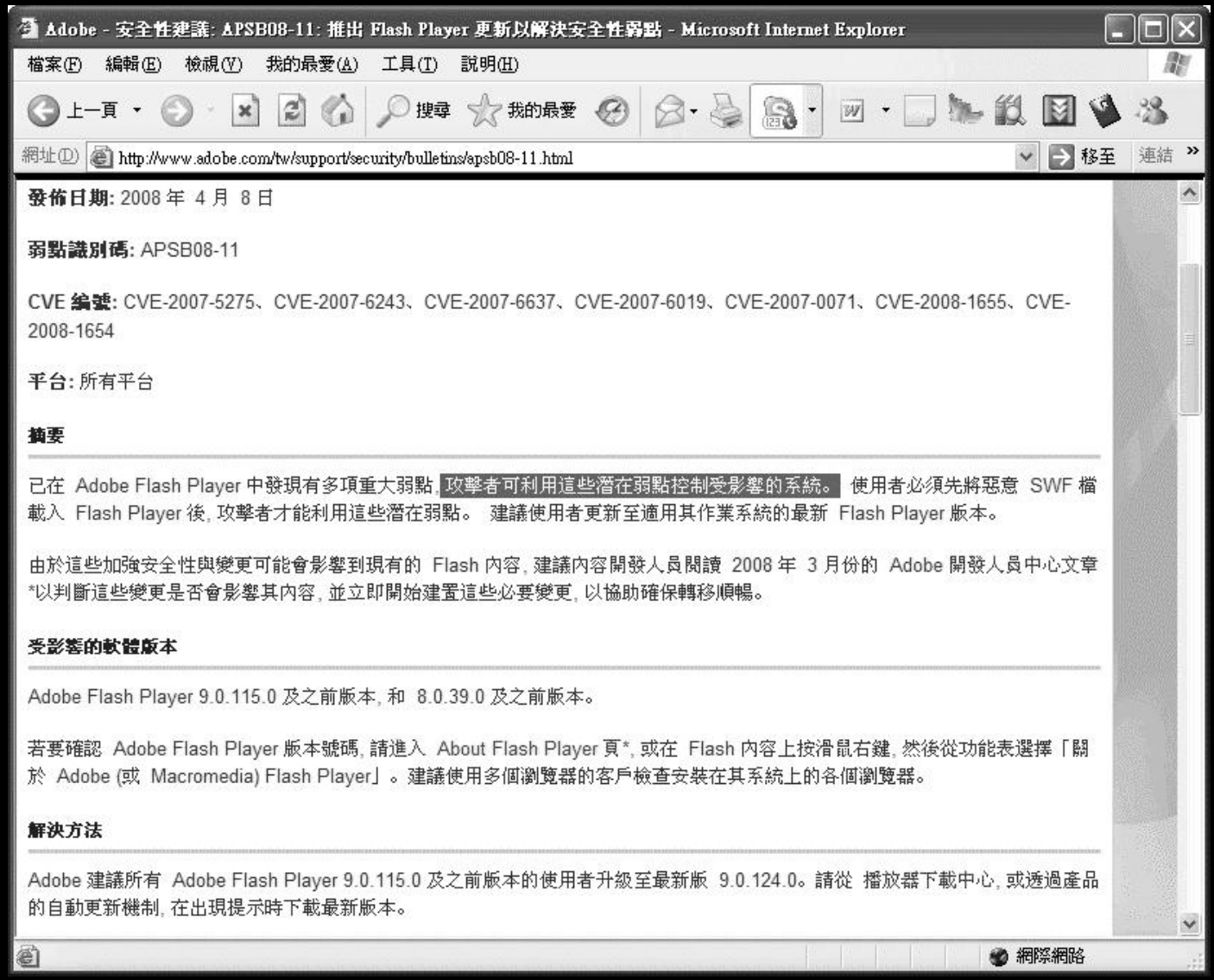
| -::DATE | -::DESCRIPTION | -::HITS | | | | | -::AUTHOR |
|---|---|---|---|---|---|---|---|
| 2008-05-14 | MS Internet Explorer (Print Table of Links) Cross-Zone Scripting PoC | 20781 | R | | D | X | Aviv Raff |
| 2007-11-11 | Microsoft Internet Explorer TIF/TIFF Code Execution (MS07-055) | 34930 | R | | D | | grabarz |
| 2007-07-31 | MS Internet Explorer 6 DirectX Media Remote Overflow DoS Exploit | 9781 | R | | D | X | Dr.Pantagon |
| 2007-05-10 | MS Internet Explorer <= 7 Remote Arbitrary File Rewrite PoC (MS07-027) | 17947 | R | | D | X | Andres Tarasco |
| 2007-03-26 | MS Internet Explorer Recordset Double Free Memory Exploit (MS07-009) | 20804 | R | | D | X | n/a |
| 2007-03-09 | MS Internet Explorer (FTP Server Response) DoS Exploit (MS07-016) | 7322 | R | | D | | Mathew Rowley |
| 2007-03-07 | Macromedia 10.1.4.20 SwDir.dll Internet Explorer Stack Overflow DoS | 5938 | R | | D | X | shinnai |
| 2007-02-05 | MS Internet Explorer 6 (mshtml.dll) Null Pointer Dereference Exploit | 11655 | R | | D | X | AmesianX |
| 2007-01-18 | BrowseDialog Class (ccrpbds6.dll) Internet Explorer Denial of Service | 5080 | R | | D | X | shinnai |
| 2007-01-17 | MS Internet Explorer VML Download and Execute Exploit (MS07-004) | 21771 | R | | D | | pang0 |
| 2007-01-16 | MS Internet Explorer VML Remote Buffer Overflow Exploit (MS07-004) | 19248 | R | | D | X | LifeAsaGeek |
| 2006-12-29 | Macromedia Shockwave 10 (SwDir.dll) Internet Explorer Denial of Service | 5328 | R | | D | X | shinnai |
| 2006-12-29 | Macromedia Flash 8 (Flash8b.ocx) Internet Explorer Denial of Service | 6745 | R | | D | X | shinnai |
| 2006-12-29 | Adobe Reader 7.0.8.0 AcroPDF.dll Internet Explorer Denial of Service | 7133 | R | | D | X | shinnai |
| 2006-12-28 | RealPlayer 10.5 ierpplug.dll Internet Explorer Denial of Service Exploit | 6073 | R | | D | X | shinnai |
| 2006-12-14 | MS Internet Explorer 7 (DLL-load hijacking) Code Execution Exploit PoC | 13914 | R | | D | | Aviv Raff |
| 2006-11-10 | MS Internet Explorer 6/7 (XML Core Services) Remote Code Exec Exploit 3 | 16113 | R | | D | | M03 |
| 2006-11-10 | MS Internet Explorer 6/7 (XML Core Services) Remote Code Exec Exploit 2 | 20941 | R | | D | X | ~Fyodor |
| 2006-11-08 | MS Internet Explorer 6/7 (XML Core Services) Remote Code Exec Exploit | 24039 | R | | D | X | n/a |
| 2006-10-26 | MS Internet Explorer 7 Popup Address Bar Spoofing Weakness | 17644 | R | | D | X | n/a |
| 2006-10-24 | MS Internet Explorer (ADODB Execute) Denial of Service PoC | 13968 | R | | D | X | YAG KOHHA |
| 2006-09-29 | MS Internet Explorer WebViewFolderIcon setSlice() Exploit (c) | 13198 | R | | D | | LukeHack |
| 2006-09-29 | MS Internet Explorer WebViewFolderIcon setSlice() Exploit (pl) | 17943 | R | | D | | YAG KOHHA |
| 2006-09-28 | MS Internet Explorer WebViewFolderIcon setSlice() Exploit (html) | 22270 | R | | D | X | jamikazu |
| 2006-09-27 | MS Internet Explorer WebViewFolderIcon setSlice() Overflow Exploit | 15277 | R | | D | | H D Moore |
| 2006-09-25 | MS Internet Explorer (VML) Remote Buffer Overflow Exploit (SP2) (pl) | 17421 | R | M | D | | Trirat Puttaraksa |
| 2006-09-24 | MS Internet Explorer (VML) Remote Buffer Overflow Exploit (XP SP2) | 23264 | R | M | D | X | jamikazu |
| 2006-09-21 | MS Internet Explorer (VML) Remote Buffer Overflow Exploit (XP SP1) | 12492 | R | M | D | | Trirat Puttaraksa |
| 2006-09-20 | MS Internet Explorer (VML) Remote Buffer Overflow Exploit | 11856 | R | M | D | | nop |

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

| -::DATE | -::DESCRIPTION | -::HITS | | | | | -::AUTHOR |
|---|---|---|---|---|---|---|---|
| 2007-10-22 | Mozilla Firefox <= 2.0.0.7 Remote Denial of Service Exploit | 10467 | R | | D | | BugReport.IR |
| 2007-03-29 | Mozilla Firefox 2.0.0.3 / Gran Paradiso 3.0a3 DoS Hang / Crash Exploit | 9467 | R | | D | | shinnai |
| 2007-02-20 | Mozilla Firefox <= 2.0.0.1 (location.hostname) Cross-Domain Vulnerability | 14043 | R | | D | X | Michal Zalewski |
| 2006-10-31 | Mozilla Firefox <= 1.5.0.7/ 2.0 (createRange) Remote DoS Exploit | 9926 | R | | D | X | Gotfault Security |
| 2006-08-22 | Mozilla Firefox <= 1.5.0.6 (FTP Request) Remote Denial of Service Exploit | 11364 | R | | D | | Tomas Kempinsky |
| 2006-07-28 | Mozilla Firefox <= 1.5.0.4 Javascript Navigator Object Code Execution PoC | 18369 | R | | D | X | H D Moore |
| 2006-06-02 | Mozilla Firefox <= 1.5.0.4 (marquee) Denial of Service Exploit | 11621 | R | | D | X | n00b |
| 2006-05-18 | Mozilla Firefox <= 1.5.0.3 (Loop) Denial of Service Exploit | 10680 | R | | D | X | Gianni Amato |
| 2006-04-24 | Mozilla Firefox <= 1.5.0.2 (js320.dll/xpcom_core.dll) Denial of Service PoC | 14493 | R | | D | X | splices |
| 2006-04-13 | Mozilla Firefox <= 1.5.0.1, Camino <= 1.0 Null Pointer Dereference Crash | 6652 | R | | D | X | BuHa |
| 2006-02-08 | Mozilla Firefox 1.5 location.QueryInterface() Code Execution (osx) | 11245 | R | M | D | | H D Moore |
| 2006-02-07 | Mozilla Firefox 1.5 location.QueryInterface() Code Execution (linux) | 27516 | R | M | D | | H D Moore |
| 2005-12-12 | Mozilla Firefox <= 1.04 compareTo() Remote Code Execution Exploit | 10233 | R | M | D | X | Aviv Raff |
| 2005-12-07 | Mozilla Firefox <= 1.5 (history.dat) Looping Vulnerability PoC | 8646 | R | | D | X | ZIPLOCK |
| 2005-10-17 | Mozilla (Firefox <= 1.0.7) (Mozilla <= 1.7.12) Denial of Service Exploit | 8041 | R | | D | X | Kubbo |
| 2005-10-16 | Mozilla (Firefox <= 1.0.7) (Thunderbird <= 1.0.6) Denial of Service Exploit | 32696 | R | | D | X | posidron |
| 2005-09-26 | Mozilla Firefox <= 1.0.7 Integer Overflow Denial of Service Exploit | 8924 | R | | D | X | Georgi Guninski |
| 2005-07-13 | Mozilla Firefox <= 1.0.4 "Set As Wallpaper" Code Execution Exploit | 9481 | R | | D | X | Michael Krax |
| 2005-07-05 | Mozilla FireFox <= 1.0.1 Remote GIF Heap Overflow Exploit | 6819 | R | | D | | darkeagle |
| 2005-05-21 | Mozilla Firefox view-source:javascript url Code Execution Exploit | 11795 | R | | D | X | mikx |
| 2005-05-07 | Mozilla Firefox Install Method Remote Arbitrary Code Execution Exploit | 9243 | R | | D | X | Edward Gagnon |

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

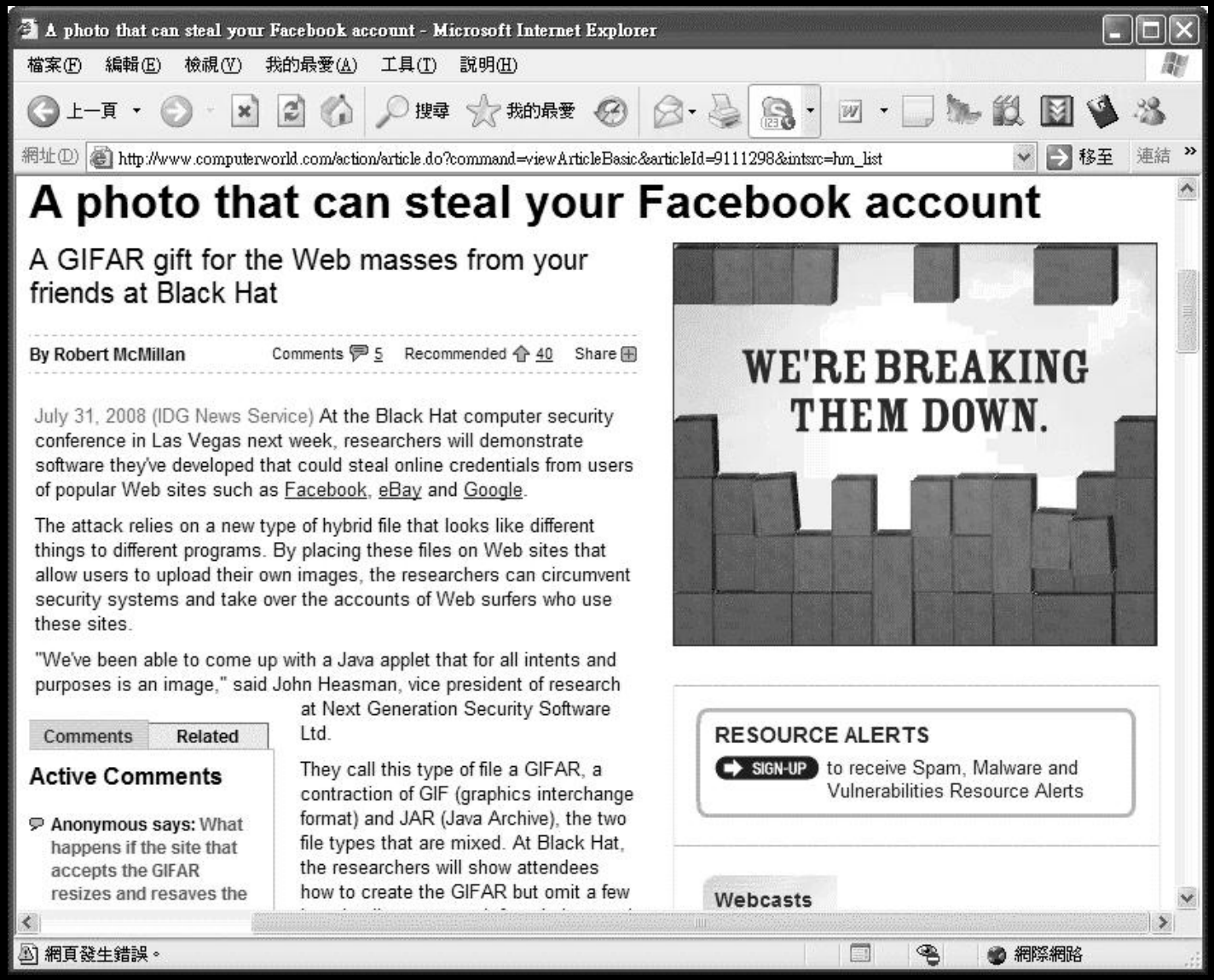
| -::DATE | -::DESCRIPTION | -::HITS | | | | | -::AUTHOR |
|---|---|---|---|---|---|---|---|
| 2008-09-11 | Maxthon Browser 2.1.4.443 UNICODE Remote Denial of Service PoC | 506 | R | | D | X | LiquidWorm |
| 2008-09-06 | Flock Social Web Browser 1.2.5 (loop) Remote Denial of Service Exploit | 1142 | R | | D | | LiquidWorm |
| 2008-09-05 | Google Chrome Browser 0.2.149.27 Inspect Element DoS Exploit | 3838 | R | | D | X | Metacortex |
| 2008-09-05 | Google Chrome Browser 0.2.149.27 A HREF Denial of Service Exploit | 3198 | R | | D | X | Shinnok |
| 2008-09-05 | Google Chrome Browser 0.2.149.27 (SaveAs) Remote BOF Exploit | 9830 | R | | D | | SVRT |
| 2008-09-04 | Google Chrome Browser 0.2.149.27 (1583) Remote Silent Crash PoC | 5121 | R | | D | | WHK |
| 2008-09-03 | Google Chrome Browser 0.2.149.27 Automatic File Download Exploit | 30720 | R | | D | | nerex |
| 2008-09-03 | Google Chrome Browser 0.2.149.27 malicious link DoS Vulnerability | 20309 | R | | D | | Rishi Narang |
| 2008-07-30 | HIOX Browser Statistics 2.0 Arbitrary Add Admin User Exploit | 1259 | R | | D | | Stack |
| 2008-07-30 | HIOX Browser Statistics 2.0 Remote File Inclusion Vulnerability | 2534 | R | | D | | Ghost Hacker |
| 2008-06-08 | BrowserCRM 5.002.00 (clients.php) Remote File Inclusion Vulnerability | 2556 | R | | D | | ahmadbady |
| 2008-03-14 | win32 Download and Execute Shellcode Generator (browsers edition) | 39255 | | | D | | YAG KOHHA |
| 2007-09-14 | Ajax File Browser 3b (settings.inc.php approot) RFI Vulnerability | 4236 | R | | D | | arfis project |
| 2007-09-12 | Apple Quicktime (Multiple Browsers) Command Execution PoC (0day) | 10642 | R | | D | X | pdp |
| 2007-05-18 | LeadTools Thumbnail Browser Control (lttmb14E.ocx) Remote BoF Exploit | 3871 | R | | D | X | shinnai |
| 2007-03-18 | Avant Browser <= 11.0 build 26 Remote Stack Overflow Crash Exploit | 2827 | R | | D | | DATA_SNIPER |
| 2007-01-19 | DivX Player 6.4.1 (DivXBrowserPlugin npdivx32.dll) IE DoS | 6343 | R | | D | X | shinnai |
| 2006-08-13 | Nokia Symbian 60 3rd Edition Browser Denial of Service Crash | 6889 | R | | D | X | Qode |
| 2006-07-01 | Opera Web Browser 9.00 (iframe) Remote Denial of Service Exploit | 4912 | R | | D | | y3dips |
| 2006-02-22 | Mac OS X Safari Browser (Safe File) Remote Code Execution Exploit | 9505 | R | M | D | | H D Moore |
| 2005-09-22 | Mozilla Browsers 0xAD (HOST:) Remote Heap Buffer Overrun Exploit (v2) | 21014 | R | | D | X | SkyLined |
| 2005-04-18 | Mozilla Browsers x (Link) Code Execution Exploit | 8298 | R | | D | X | Michael Krax |
| 2005-01-11 | Veritas Backup Exec Agent 8.x/9.x Browser Overflow (c version) | 6244 | R | M | D | | class101 |
| 2004-12-30 | Mozilla Browser <= 1.7.3 NNTP Code Heap Overflow (PoC) | 4884 | R | | D | X | Maurycy Prodeus |
| 2004-11-29 | Multiple Browsers Nested Array sort() Loop Stack Overflow Exception | 5131 | R | | D | X | SkyLined |
| 2004-10-22 | Multiple (Almost all) Browsers Tabbed Browsing Vulnerabilities | 4848 | R | | D | X | Jakob Balle |


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
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。
網際網路


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
Acrobat漏洞可能引發Web攻擊
CNET新聞專區：Joris Evers
2007/01/05 13:04:49
觀看回應
使用者眾多的Acrobat Reader安全弱點可能成爲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，一旦點入連結就會啓動惡意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挾合作夥伴大軍壓境
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
網際網路


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
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
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
升級到 IE7
更好的瀏覽效果，強化的功能。 下載由 Google 自訂的 IE7
模擬入侵測試
找出安全風險和漏洞，提升網絡保安， 加強防衛，避免資料外洩。
www.i-totalsecurity.net/
Hermes可移式迷你機房
server+儲存,按需擴充,MIS早回家 採用intelXeon處理器,節能省電,效益高
資安-10大熱門網站
提供資安知識總整理、以及 資安相關大熱門網站目錄
www.104guide.cc
Google 提供的廣告
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，
完成
網際網路


Secunia PSI (RC3)
Secunia Personal Software Inspector
Overview
Insecure
End-of-Life
Patched
Scan
Settings
Profile
Feedback
Upgrade
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
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
WE'RE BREAKING THEM DOWN.
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
網頁發生錯誤。
網際網路


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