TippingPoint

現代網路攻擊模式與網路安全使用手則

提升校園資訊安全

石謂龍 Robin Shih
HP TippingPoint資安技術顧問
rshih@hp.com

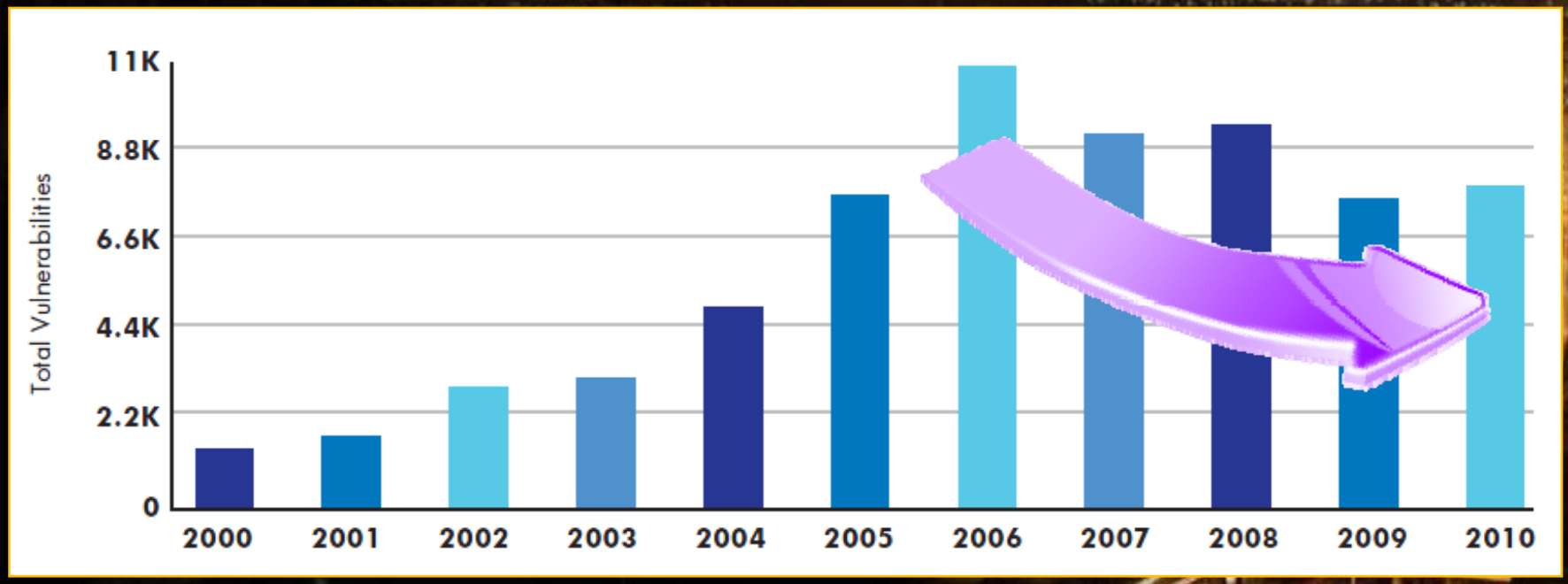
Agenda

TippingPoint
IPS-SECURED NETWORKS

- 前言--網路犯罪活動持續成長
- 現代網路攻擊模式與實例說明
- 何謂「網路釣魚」?
- 校園網路安全使用手則
- Q & A

Vulnerability Discoveries

- The good news….

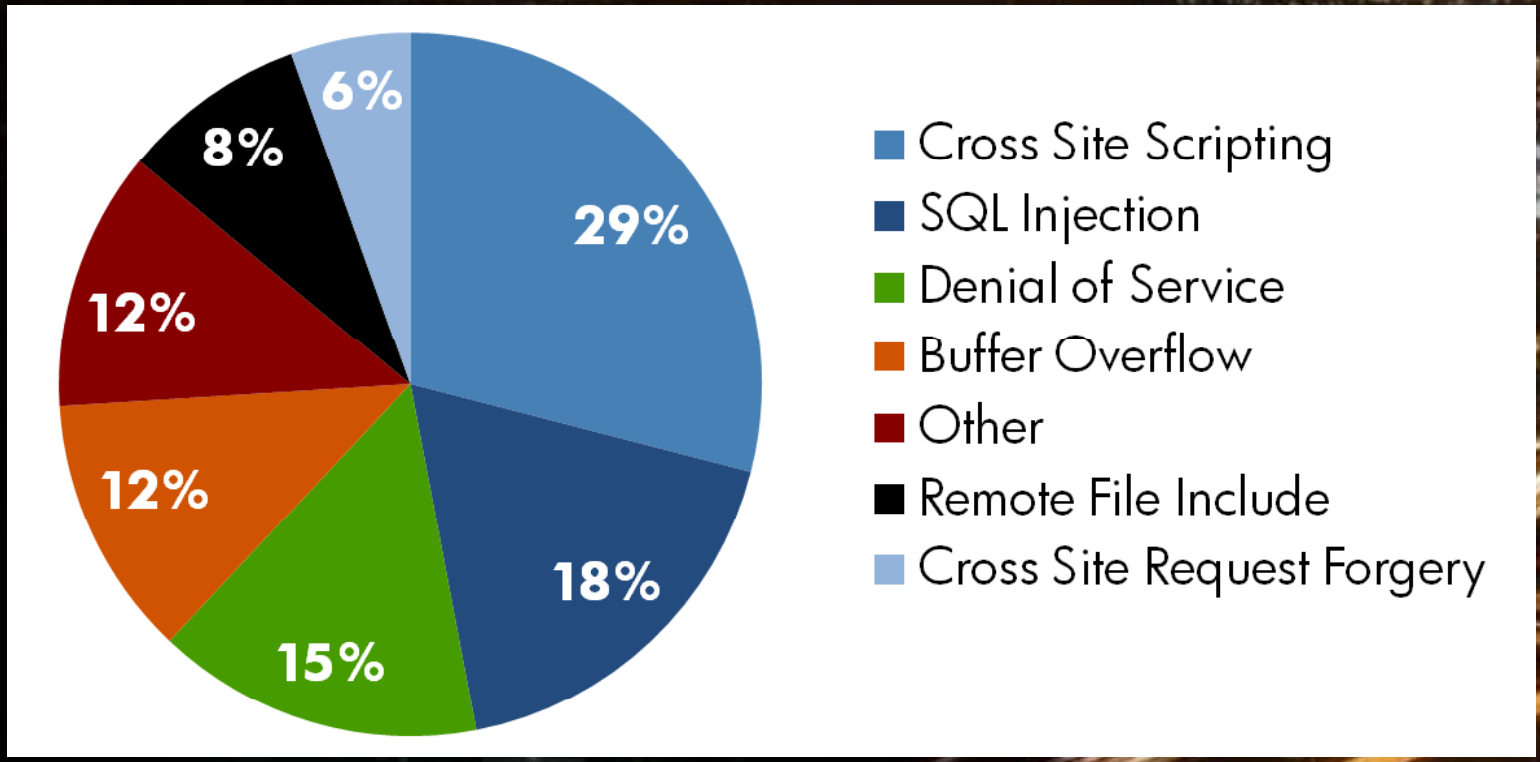


- The trend is leveling
- Better software development practices

Source: Open Source Vulnerability Database

New Web Vulnerabilities by Type

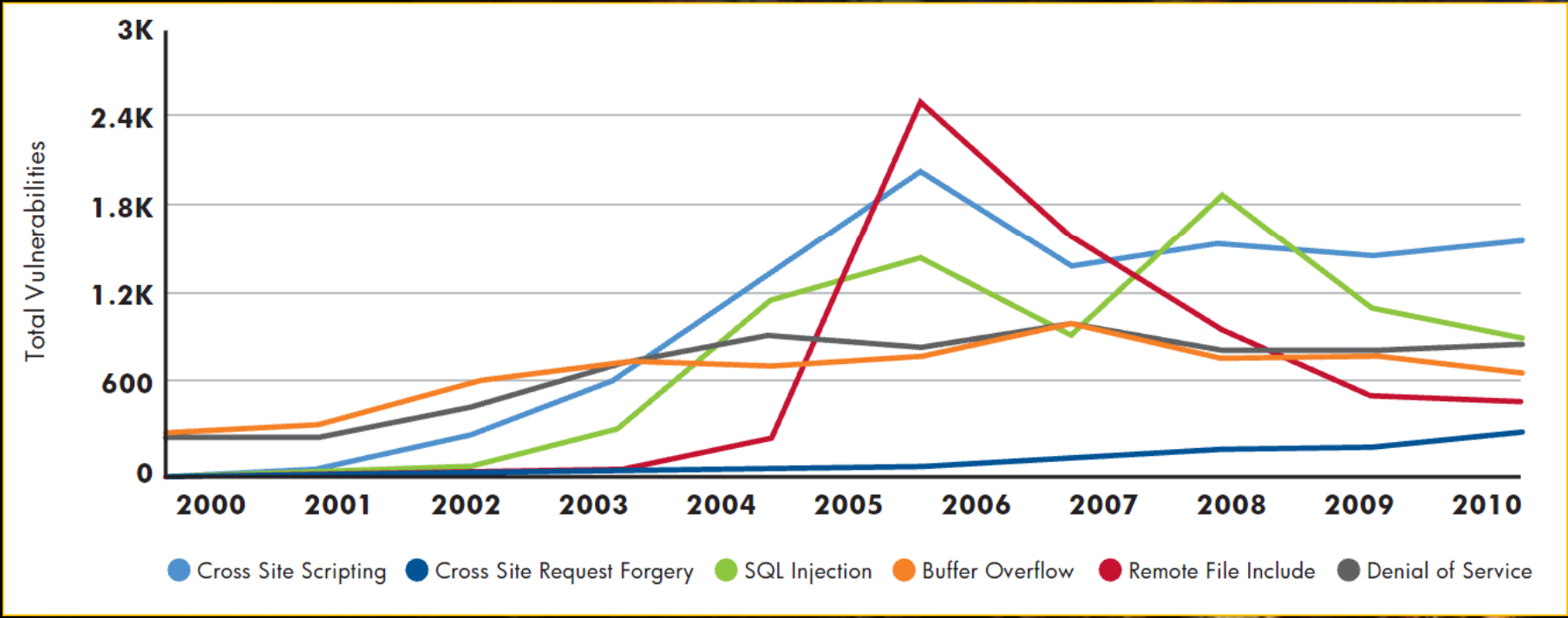
About half of all new vulnerabilities in 2010 were in web applications



Web 2.0, AJAX, Flash, HTML 5 enable new attack vectors

Source: Open Source Vulnerability Database

Web Vulnerability Trends

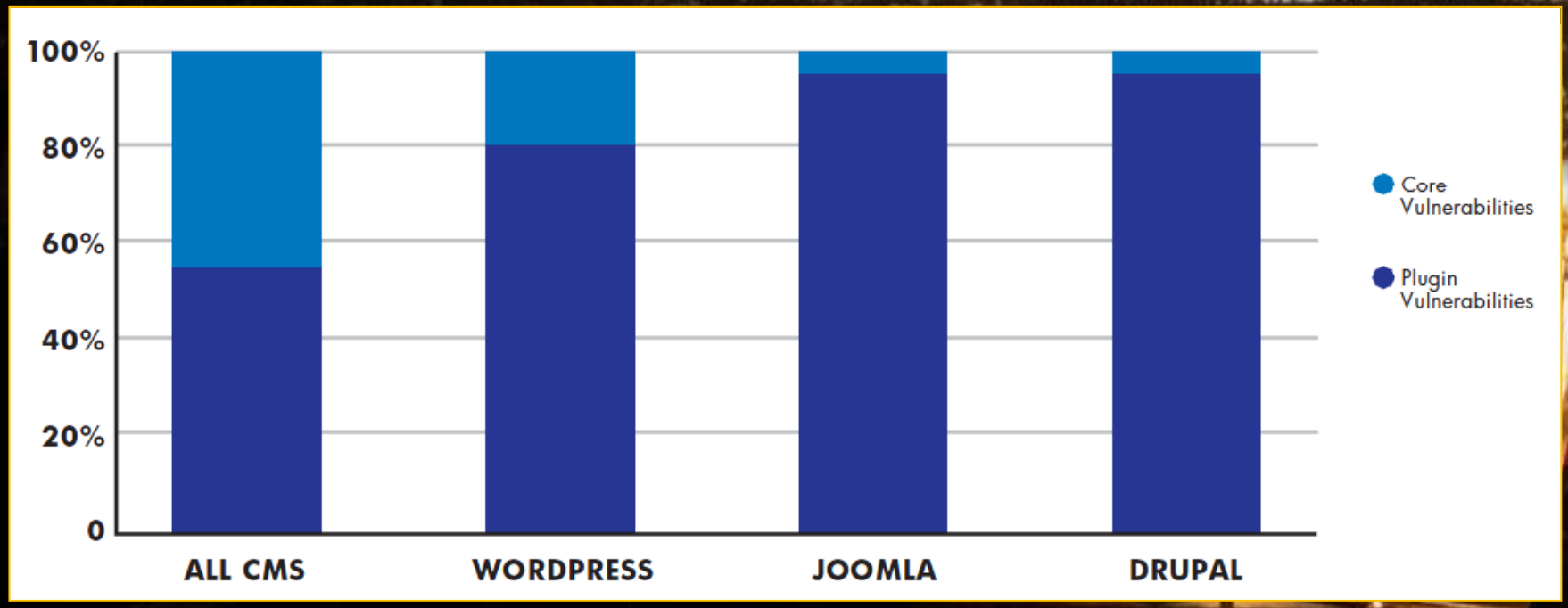


- #1 Cross-site scripting
- #2 SQL injection
- #3 Denial of Service

Source: Open Source Vulnerability Database

Vulnerabilities in Content Management Systems

- Plug-ins provide more vectors for attacks



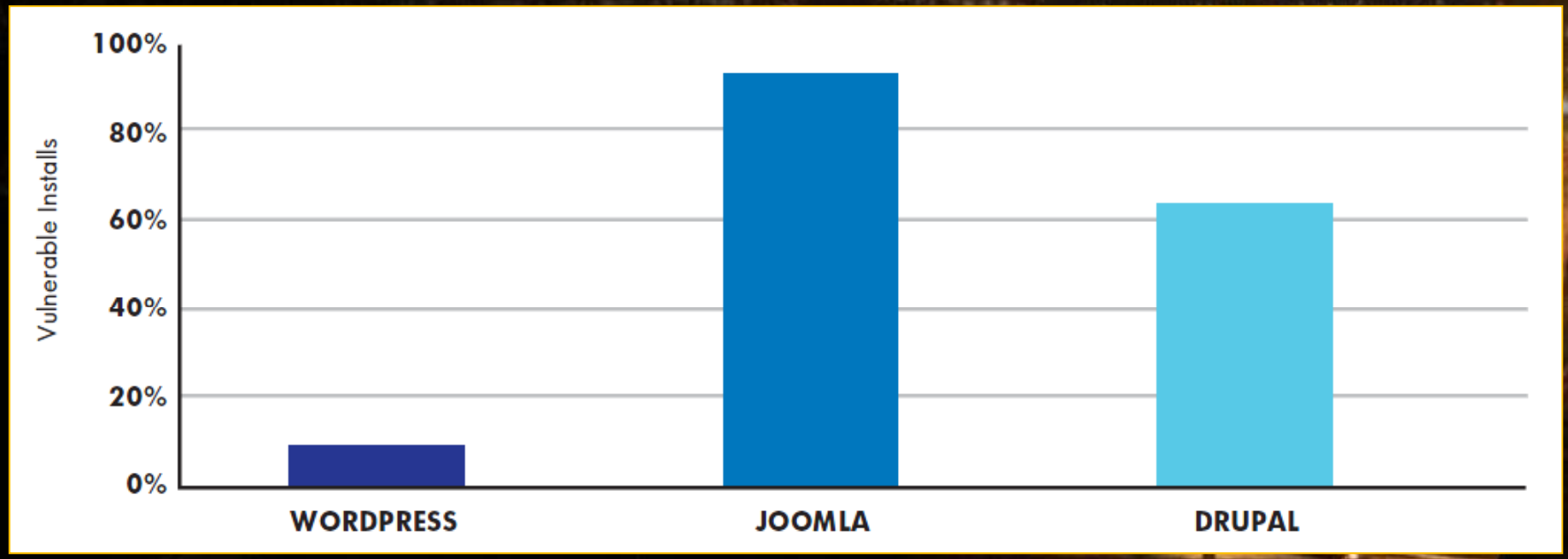
Over 50% of CMS vulnerabilities reported against plug-ins

Over 80% for the top 3 CMS applications

Source: Open Source Vulnerability Database

Internet Facing CMS Systems

- Many unpatched systems remain vulnerable to attacks



10% of Wordpress installations are vulnerable

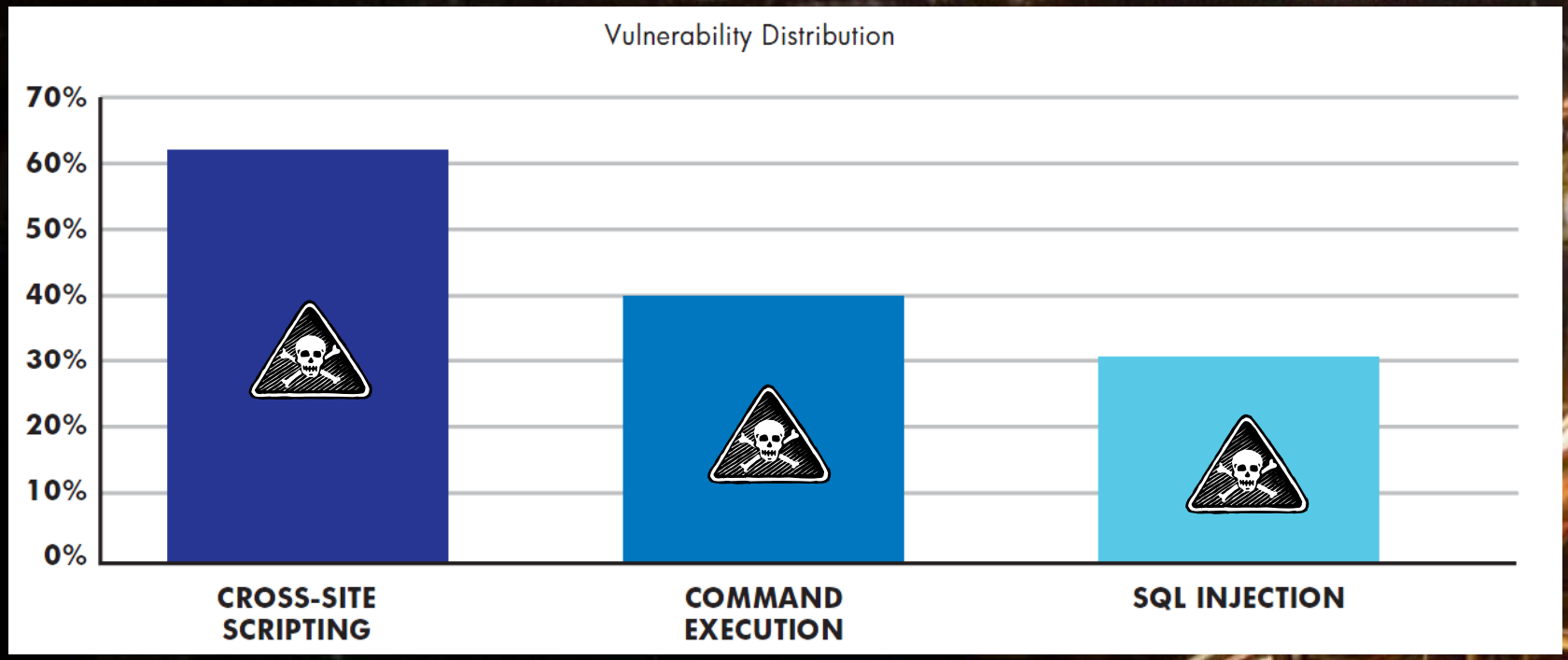
90% of Joomla installations are vulnerable

60% of Drupal installations are vulnerable

Source: HP DVLabs

Custom Web Applications

- Ample opportunity for attackers



71% had at least one serious vulnerability

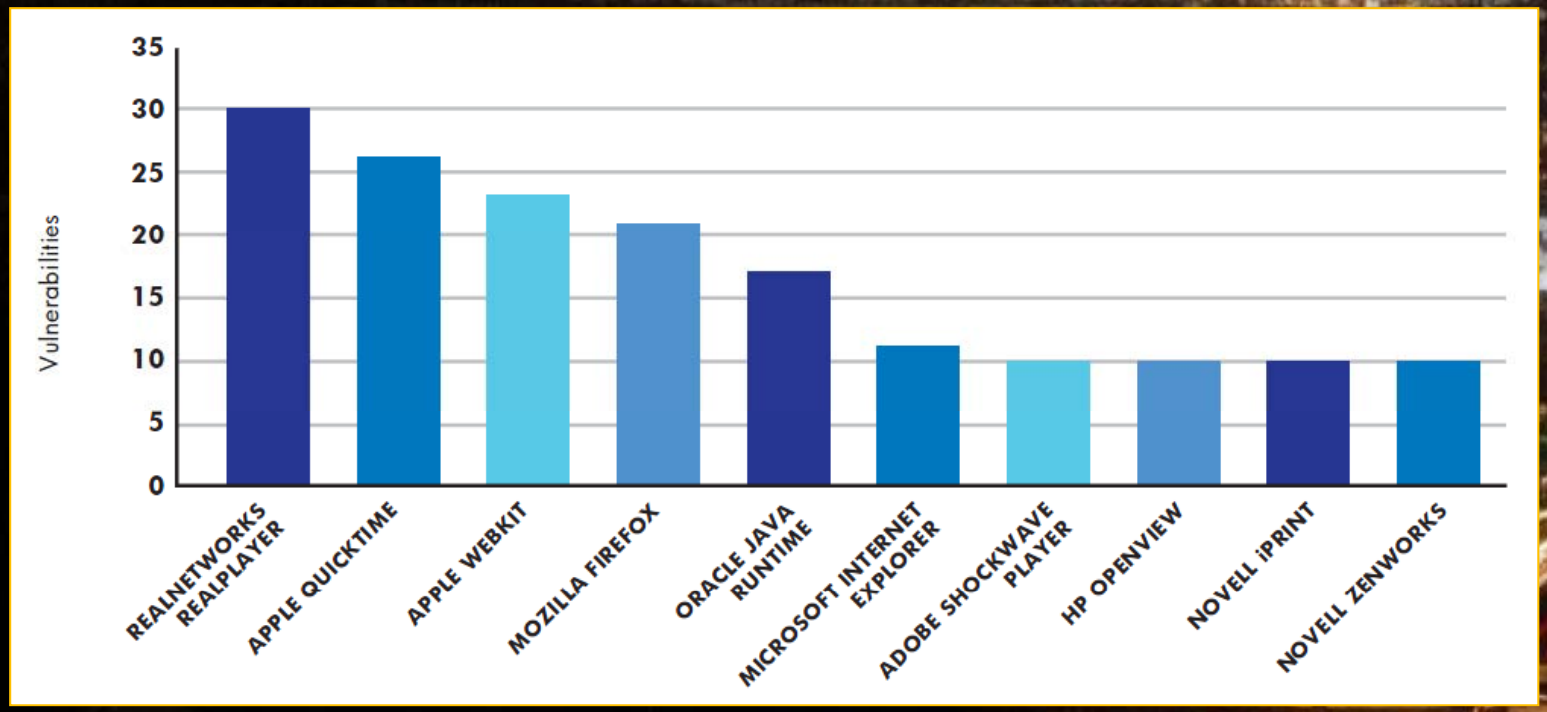
49% had at least one critical vulnerability

11% had no vulnerabilities

Source: HP WebInspect

ZDI Vulnerabilities by Application

- Browsers, media players and plug-ins

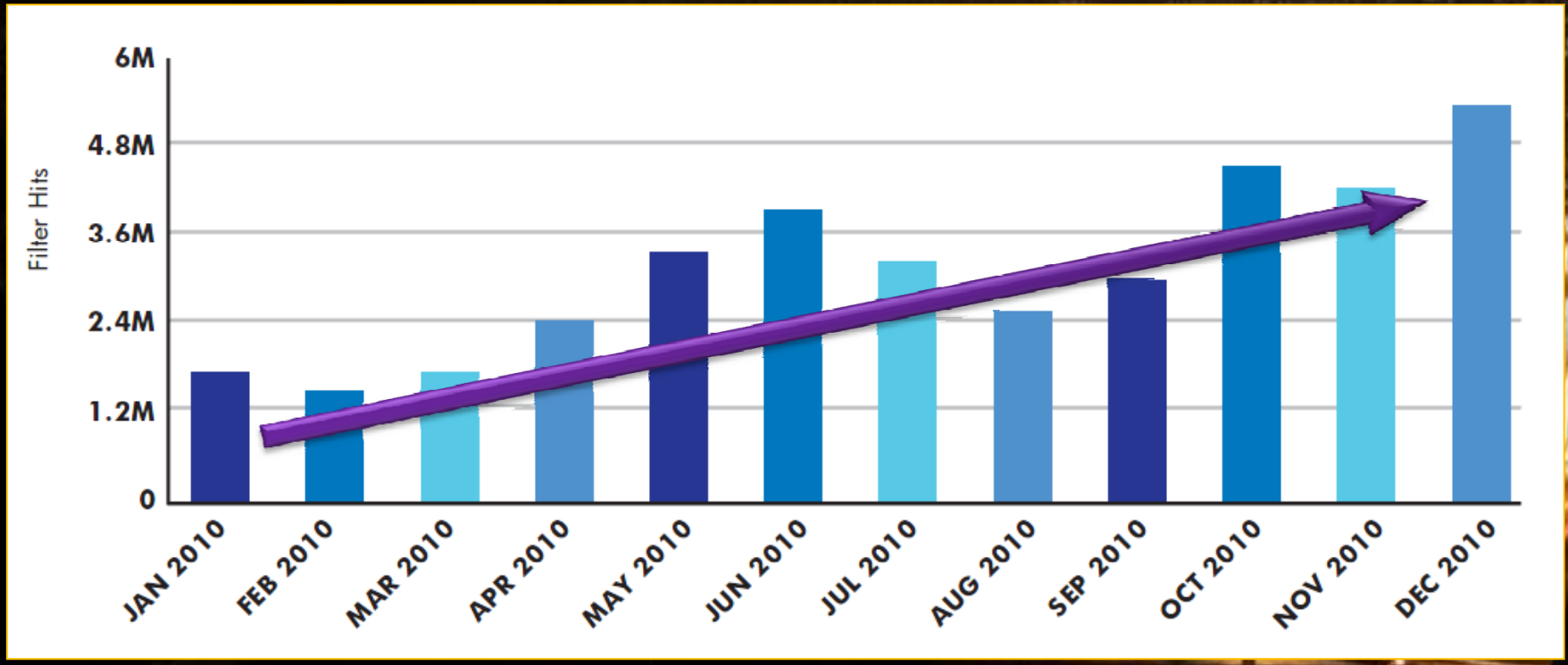


- 320 vulnerabilities disclosed by DVLabs and ZDI in 2010
- 7 of the top 10 vulnerabilities were related to web browsers

Source: HP DVLabs, Zero Day Initiative (ZDI)

Attack Trends: Client Side

The bad news…

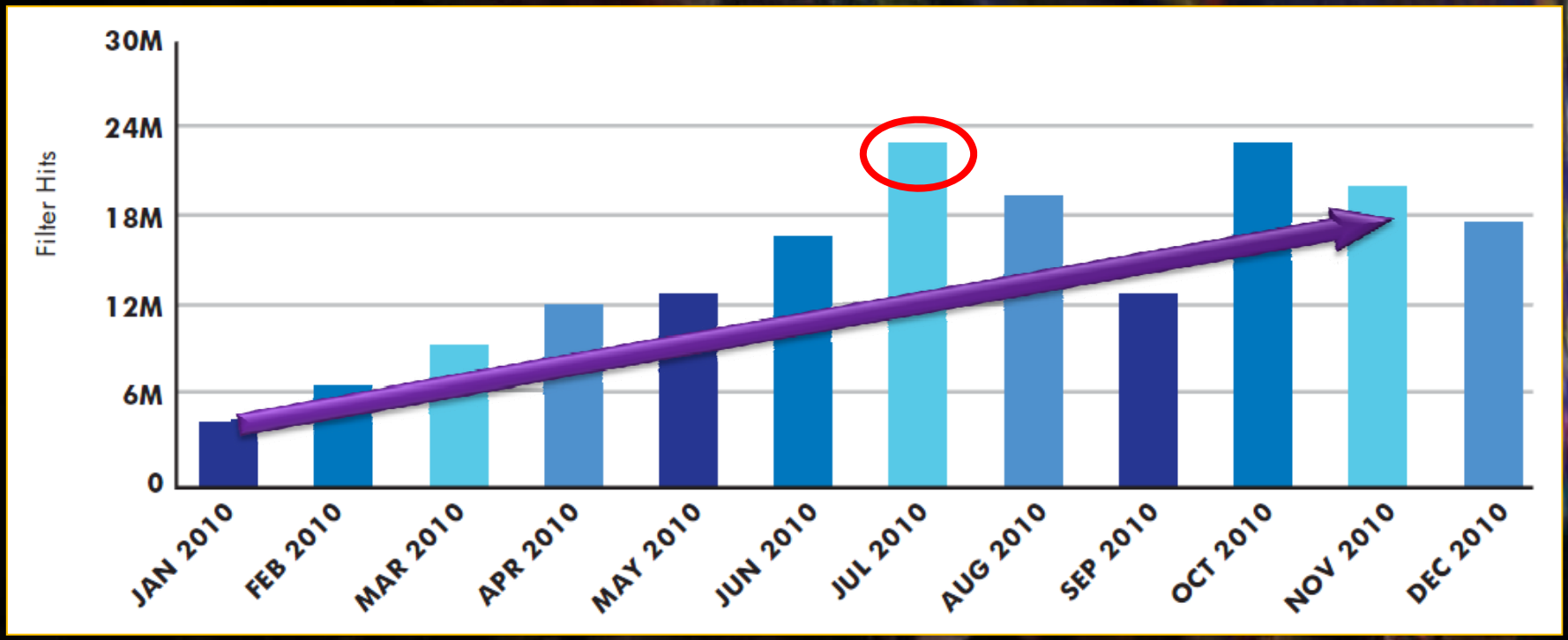


- Significant increase in attacks during 2010
- Peak of 5 million attacks in January
- 5x increase over 12 months
- Top attacks: Malicious JavaScript and PHP file-include

Source: HP DVLabs, ThreatLinQ Global Threat Portal

Attack Trends: Server Side

Also bad news…

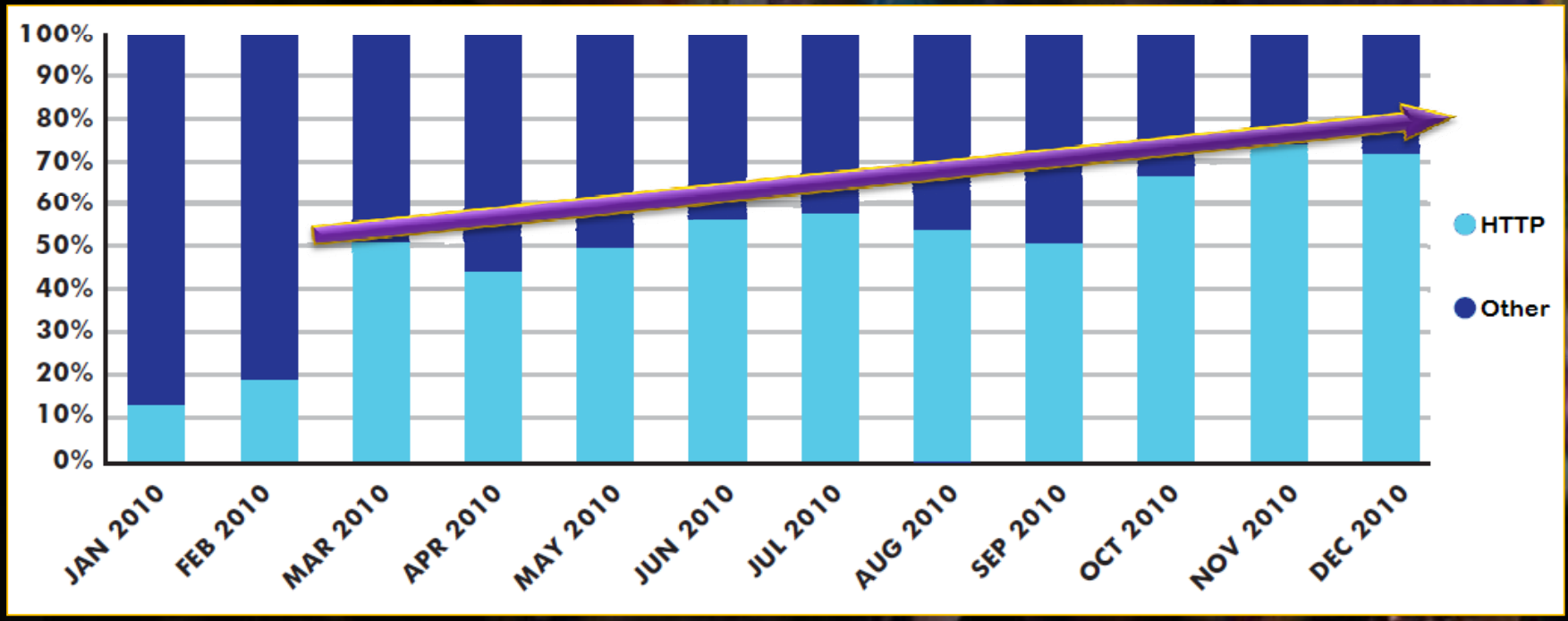


- Peak of 23 million attacks in July -- 4x more than client-side
- 4x increase from December to January
- 3 million PHP Remote File Include attacks in July

Source: HP DVLabs, ThreatLinQ Global Threat Portal

Attack Trends: Web vs Legacy

Attack targets shifting from legacy to web applications



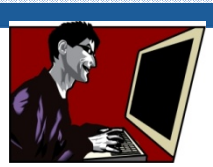
- Percentage of HTTP attacks increase to 70% over 12 months
- Fewer legacy/SMB types of attacks

Source: HP DVLabs, ThreatLinQ Global Threat Portal

現代網路攻擊模式與實際案例說明

開始之前先了解攻擊作為

TippingPoint
IPS-SECURED NETWORKS



駭客的終極目標→奪取電腦的控制權

常見手法

1.透過漏洞入侵電腦

Exploit

2.引誘使用者在不知情下安裝控制程式

3.騙取帳號密碼

Spear Phishing

Whaling

Web Application

SQL Injection

XSS

PHP File Include

Trojan

Spyware

HP TippingPoint IPS

4.暴力猜測

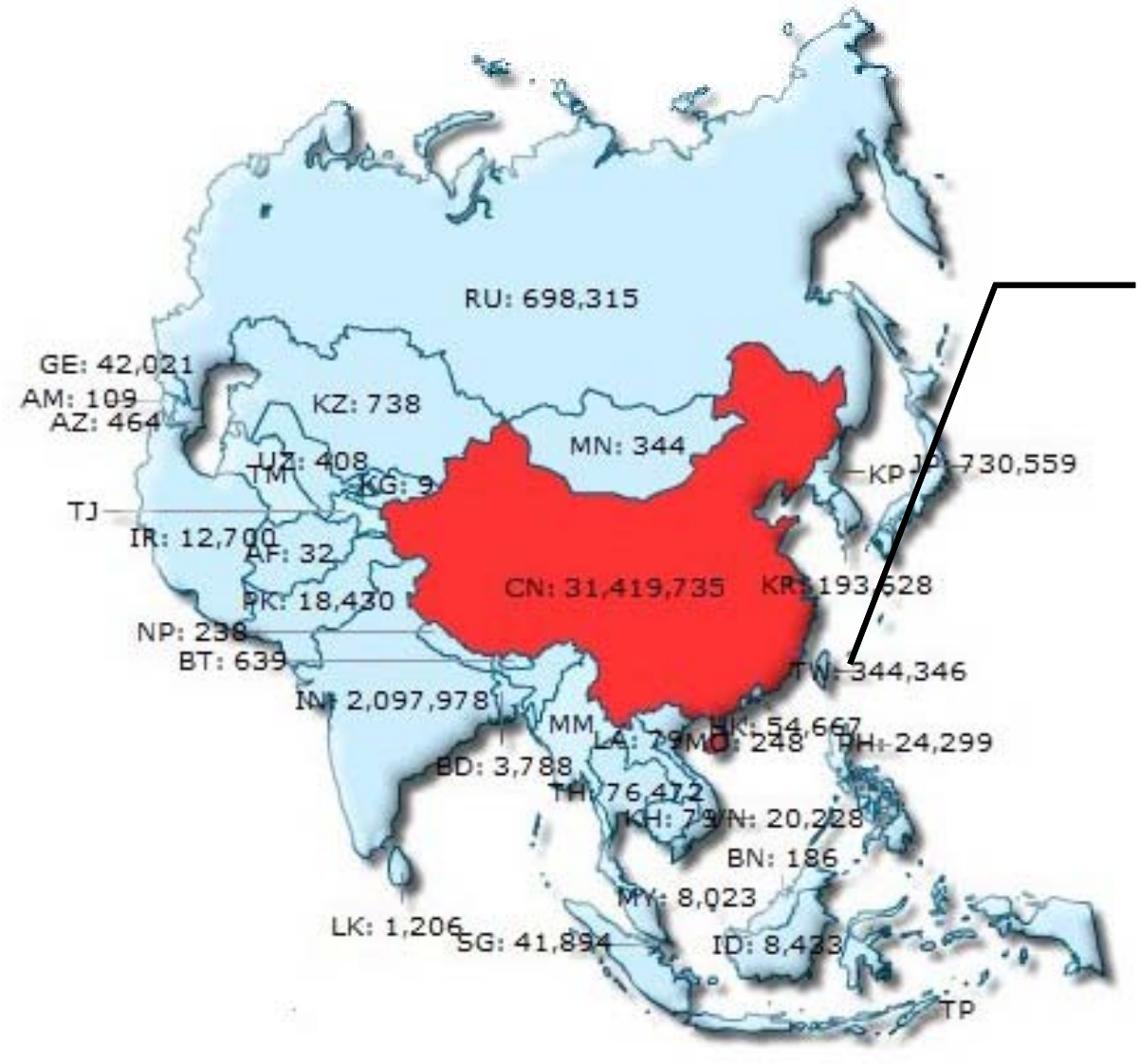
DDoS

Botnet

網路惡意活動亞洲統計資料

2011 1-4月

TippingPoint
IPS-SECURED NETWORKS



Taiwan Specific

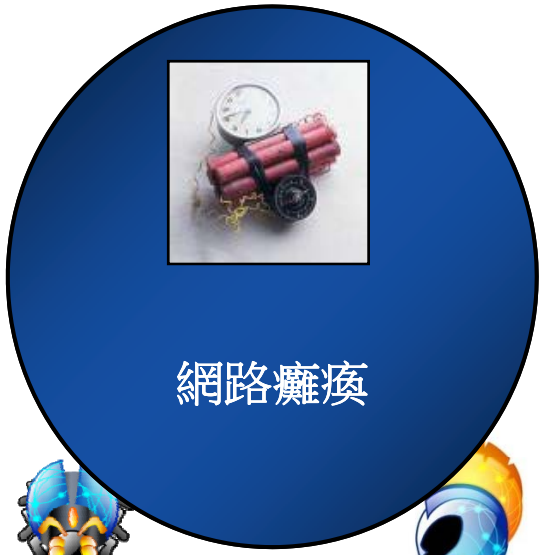
344,346 attacks

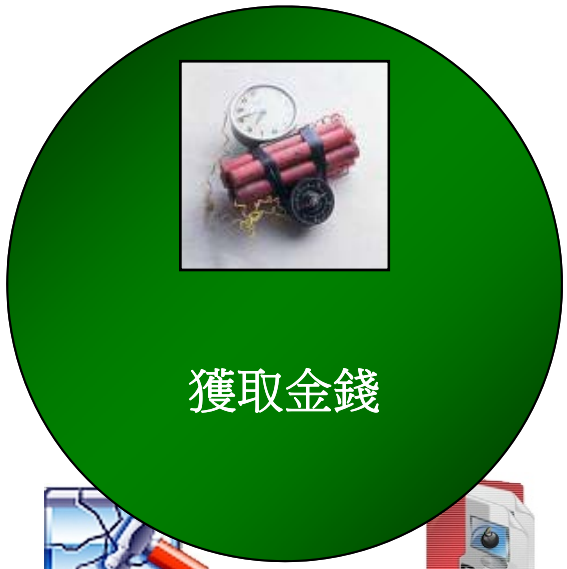
Jan. 1 – Apr. 30, 2011

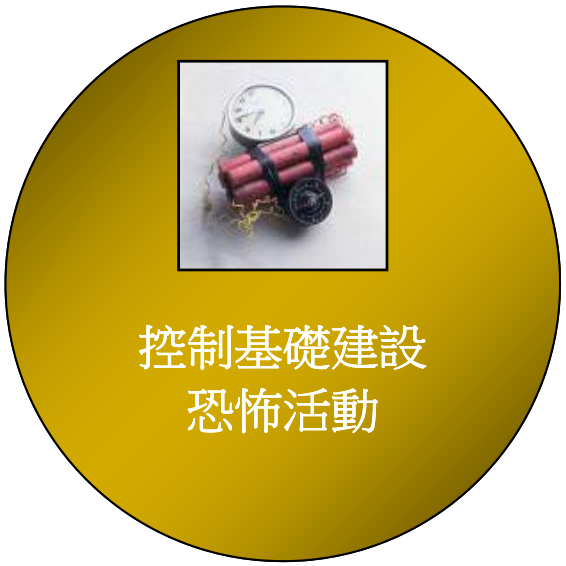
Source: DVLabs Lighthouse Program

攻擊分類與目的

TippingPoint
IPS-SECURED NETWORKS







Virus

Trojan

P2P

Worm

O/S Specific Attacks

DDoS

Application Specific Attacks

PHP File Include

SQL Injection

Data Phishing

XSS

DDoS

SCADA

The ti… ast … is it really behind us?

How eas… it to … penetrate … critical applications and … al data?

- ***C… …rfare***
- ***N… … state, local i… …cture***
- ***Politically motivated attacks***

Amateur Hacker / Criminal

Organized Crime

Terrorist, Political Activist

Rival Corporation

Angry / unethical employee or contactor

Outsourced or sub-contracted firm

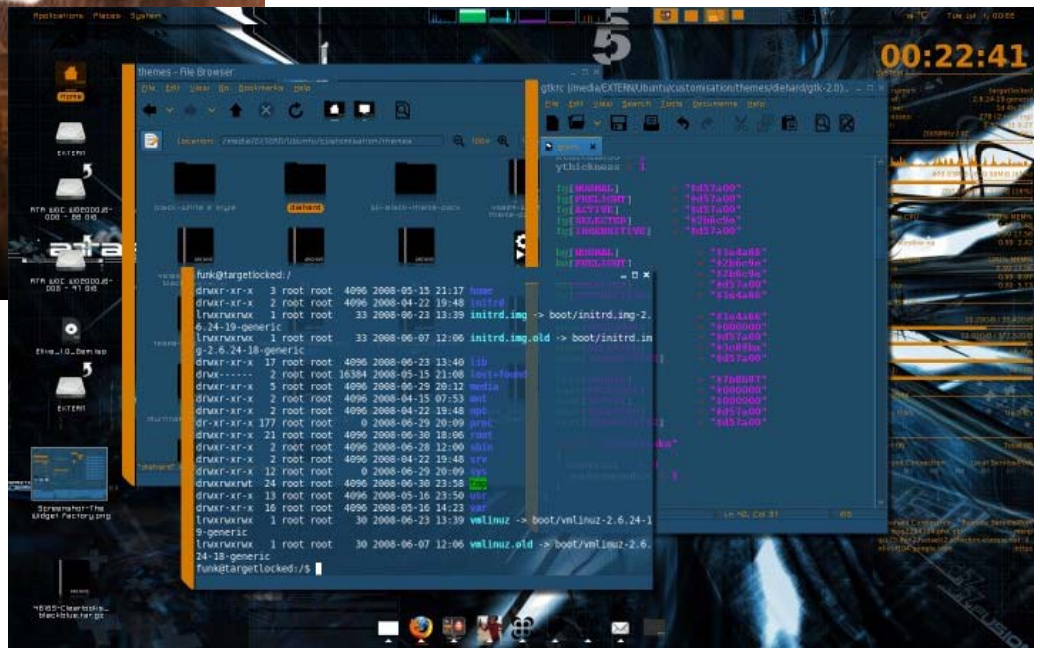
Unethical advertisers

終極警探4

描述駭客透過網路控制交通設施等基礎建設

TippingPoint

IPS-SECURED NETWORKS



公路電子看板遭駭客入侵--前有活屍

TippingPoint
IPS-SECURED NETWORKS

前面有活屍？　美國交通電子看板經常被駭客惡搞(2009/02/05 16:08)

德州奧斯汀市一條公路旁邊的電子看板上寫著：「小心！前面有活屍」。(圖／美聯社)

記者朱錦華／綜合報導

美國公路的交通電子看板經常遭到駭客惡搞，例如他們會把「前面有落石」竄改成「前面有活屍」（zombies），或「前面有迅猛龍」等。公路安全單位非但一點也不覺得有趣，反而覺得不勝其擾。

最近的一次惡搞，周二(3日)發生在伊利諾州柯林維爾附近的255號州際公路。一面電子看板出現了：「活屍出現，前面道路封閉」的字樣。

類似的惡作劇還出現在印第安納波里斯、德州的奧斯汀等地。

伊利諾州的通輸主管部門位非常擔心，這種惡作劇會對用路人造成困擾或分心，釀成意外。在伊利諾州，惡整交通電子看板，最高可罰250美元。

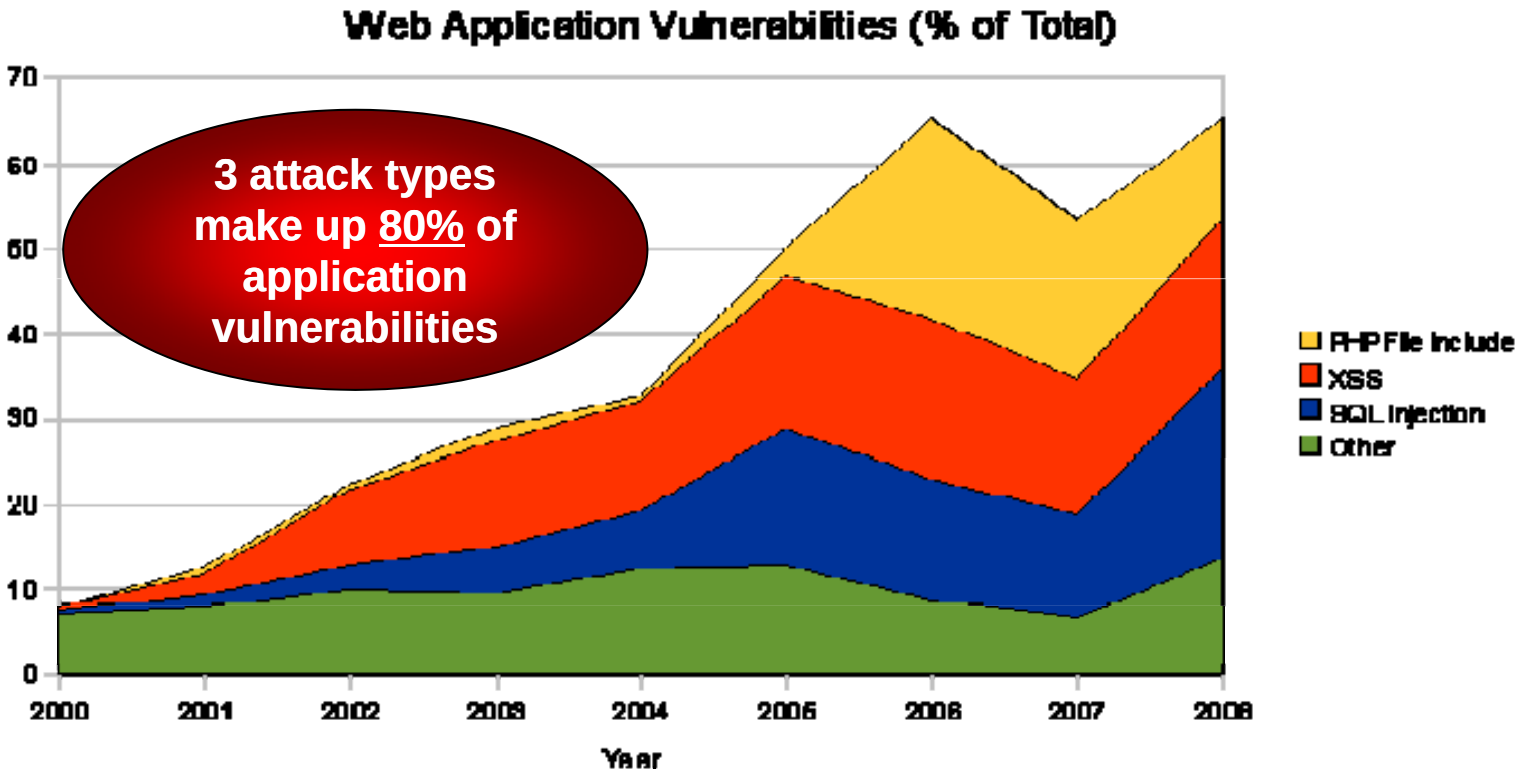
獲取金錢為目的的攻擊

Prevalence of Web Vulnerabilities

Web application vulnerabilities:

- 2/3 of all discovered application vulnerabilities
- 80% come from: PHP File Include, XSS, and SQL Injection attacks

Financially Motivated Attacks



以金錢為目標的攻擊案例

網頁入侵 +網路釣魚--騙取帳號密碼

TippingPoint

IPS-SECURED NETWORKS

Financially Motivated Attacks

Bank of America Higher Standards

Dear BOA Military Bank Customer,

This is your official notification from Ban
deactivated and deleted if not renewed in
Contact assigned to this account. As the
will be deactivated and deleted.

Click here and **Renew Now** your BOA

If you are not enrolled to Online Banking
and Social Security Number as Passwo

SERVICE : BOA Military Bank Paymen

EXPIRE DATE: December 25, 2006

Thank you, sincerely,

Eric Wilkinson, Customer Service

==========
CUST
==========

http://militarybankonline.bankofamerica.com7id-bank-logo.. id_user23891.krblrice.com.mav.pt/.https:/militarybankonline.bankofamerica.com Active URL from Portugal Telecom (As of 4:30 AM today!)

Bank of America

Military Bank Online

Welcome to Military Bank Online

Attention Customers

Bank of America emails will never ask you to reply to an email with any personal information or data, such as your Social Security number or any other sensitive information.

If you should ever receive an email that appears to be suspicious, simply delete it. To report a suspicious email that uses Bank of America's name, you can forward it to security@bankofamerica.com.

View demo | Learn more | Enroll now

First time signing in? Create a password.

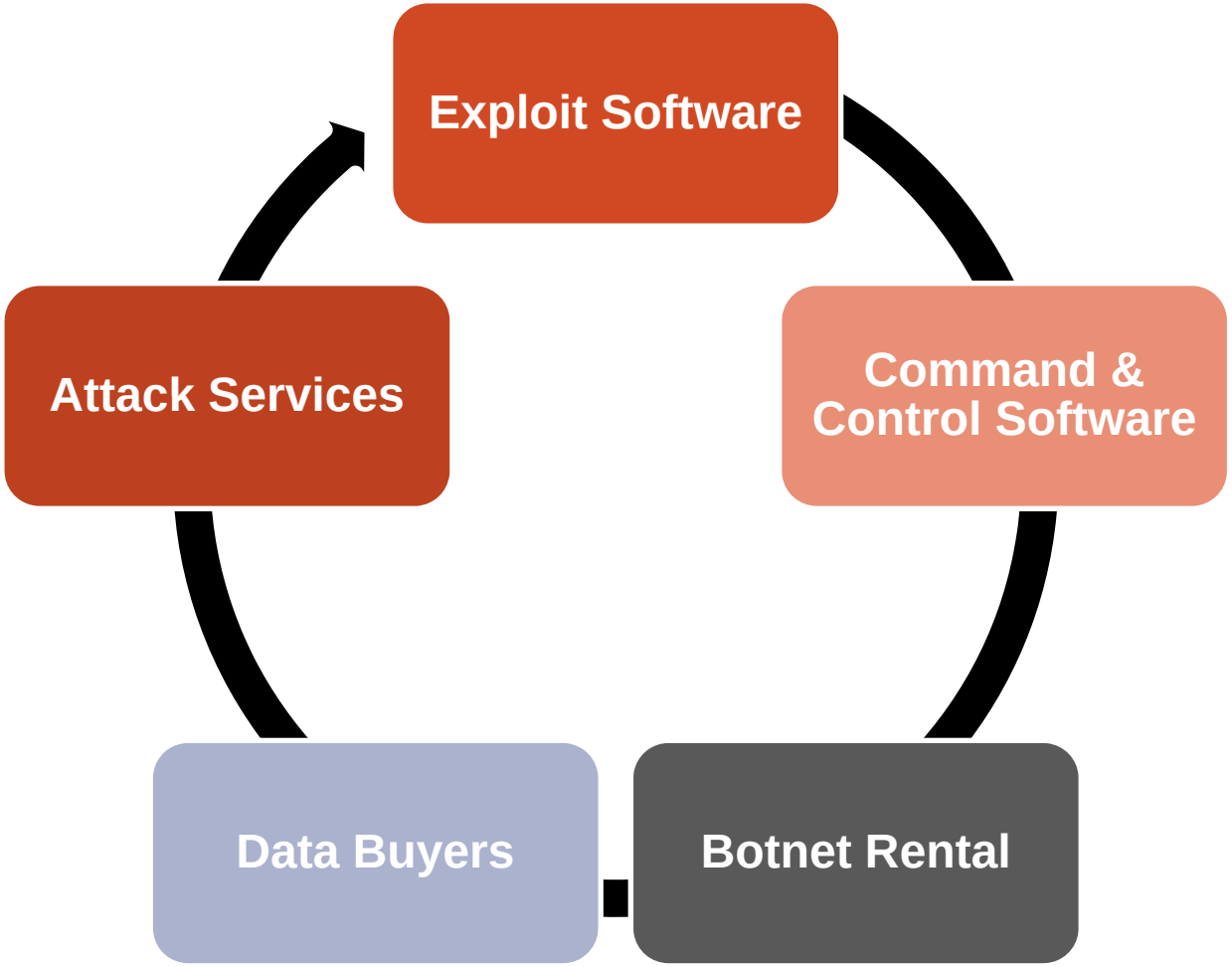
Username:

Password: Sign In

Forgot your password?

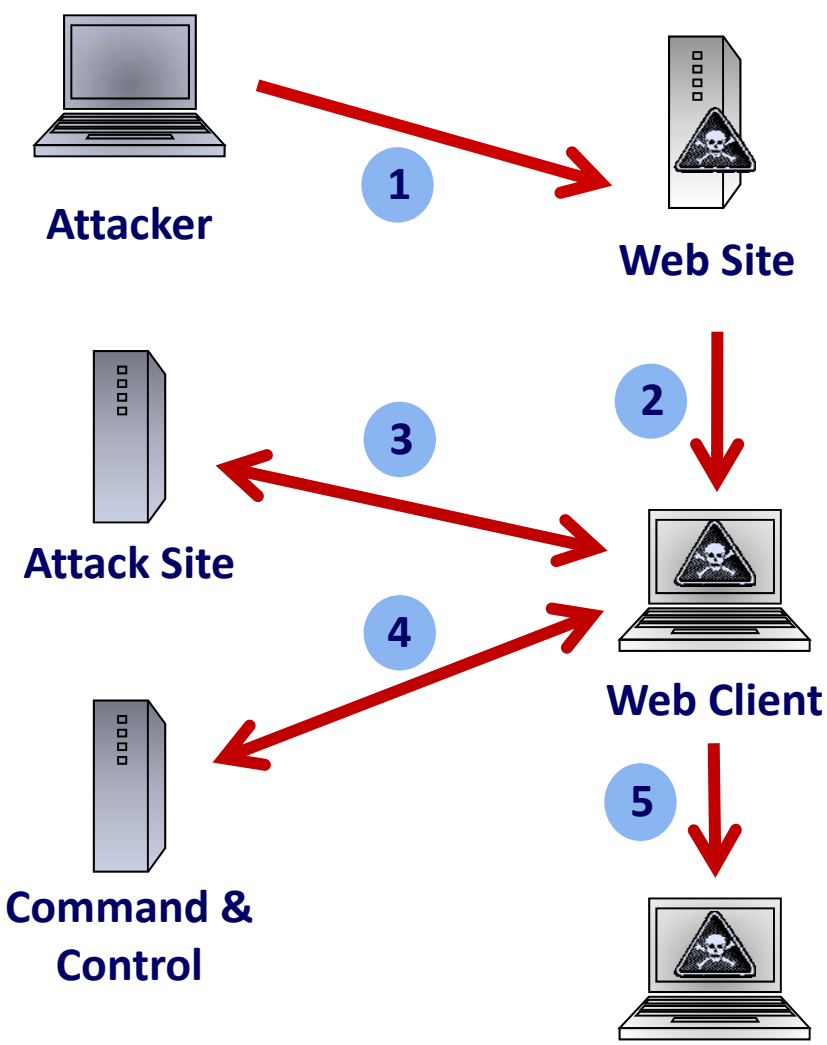
網路犯罪生態系

TippingPoint
IPS-SECURED NETWORKS



入侵電腦流程

TippingPoint
IPS-SECURED NETWORKS



1. Attacker compromises a legitimate web site
2. Client visits legitimate site and is redirected to attacker site
3. Attacker site downloads botnet trojan to client
4. Botnet contacts command and control for instructions
5. Botnet infects other systems on network

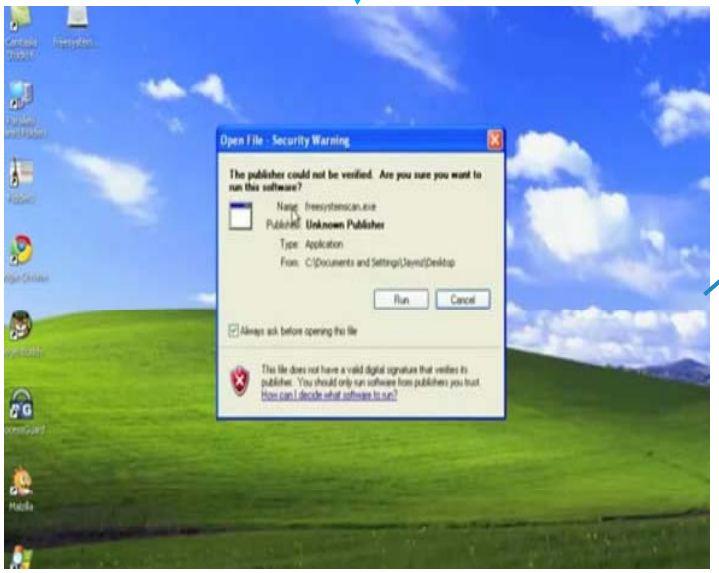
近期攻擊案例 : LizaMoon Malware Attacks

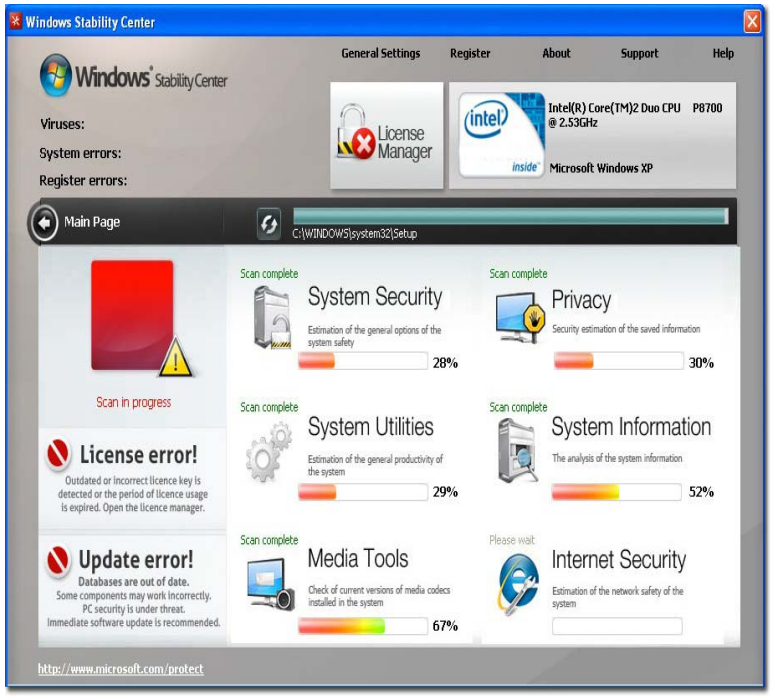
TippingPoint
IPS-SECURED NETWORKS

- First noted on the 29 of March 2011 and was named after the first domain that it was identified on, lizamoon.com. After approx 1 week, the number of impacted URLs ranges between the hundreds of thousands and 1.5 million. Latest statistics show at 4 million + URL being compromised.

Victim web host : www.學校.edu.tw
(host affected by SQL Injection attack)

Redirected to http://lizamoon.com





Windows Stability Center(Fake APP)

社交工程實例--恐嚇手法

你中毒了!要購買防毒軟體

TippingPoint
IPS-SECURED NETWORKS

駭客網上騙賣假殺毒軟體 每日獲利1萬美元

2009年03月25日 09:11 來源：賽迪網

[發表評論] [推薦朋友] [關閉窗口] [列印本稿]

聚焦兩會之醫療

- 成品油稅改後我國首次上調油價 專家:頻調是好事
- 國企收入和稅金多年來首降 電力交通等行業虧損
- 國資委：一年內欲完成合併縮減40-60家中央企業
- 傳百事、統一欲接受匯源 統一:沒有任何入股意向
- 中移動南京公司涉嫌違規收費3千萬 公司:不知情
- 國際油價高漲 全國各地汽柴油批發價格借勢普漲

食品安全喜怒哀樂

網路安全公司Finjan公佈的數據顯示，通過欺騙用戶購買假殺毒軟體，駭客每日可獲利1萬美元。

Finjan稱，通過關鍵詞優化，駭客首先網民吸引到一些網站上，然後提示用戶電腦中毒，建議安裝殺毒軟體。之後，駭客將用戶重新指向銷售假安全軟體的網站，誘騙用戶購買。

據Finjan連續16天的監控數據顯示，有180萬網民被重新定向到假殺毒軟體網站，12%下載並安裝了該軟體，1.79%以50美元的價格購買了該軟體，駭客每日可獲利1萬多美元。

SQL Injection大肆入侵

1,900+ Web Sites Compromised via SQL Injection

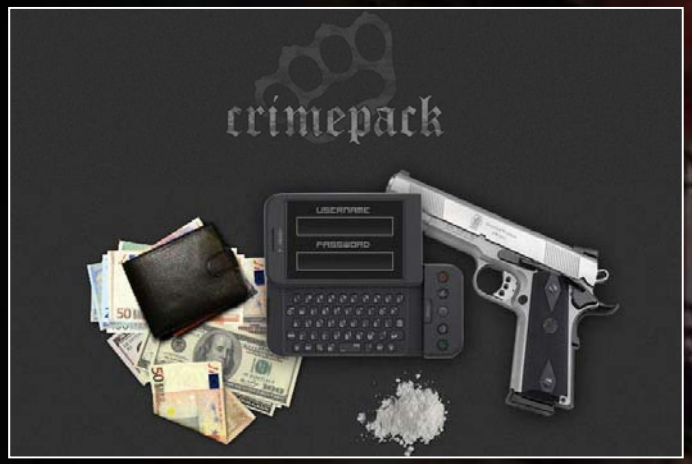
TippingPoint

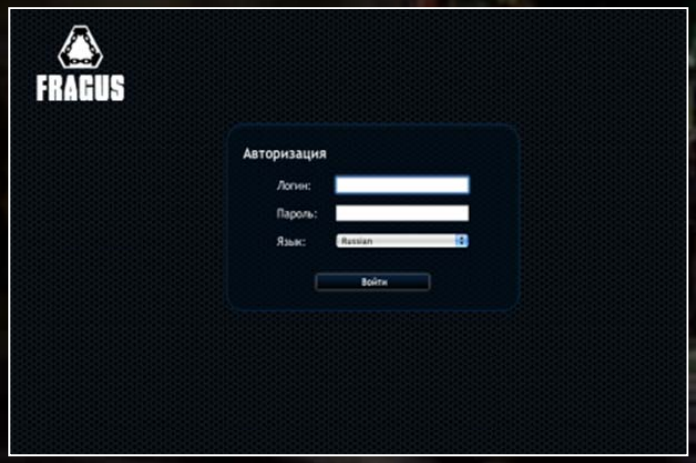
IPS-SECURED NETWORKS

- 將使用者導向惡意站臺
- 惡意站臺試圖利用漏洞入侵使用者電腦
- 偷取個人電腦裡的資料, 或是植入殭屍控制程式

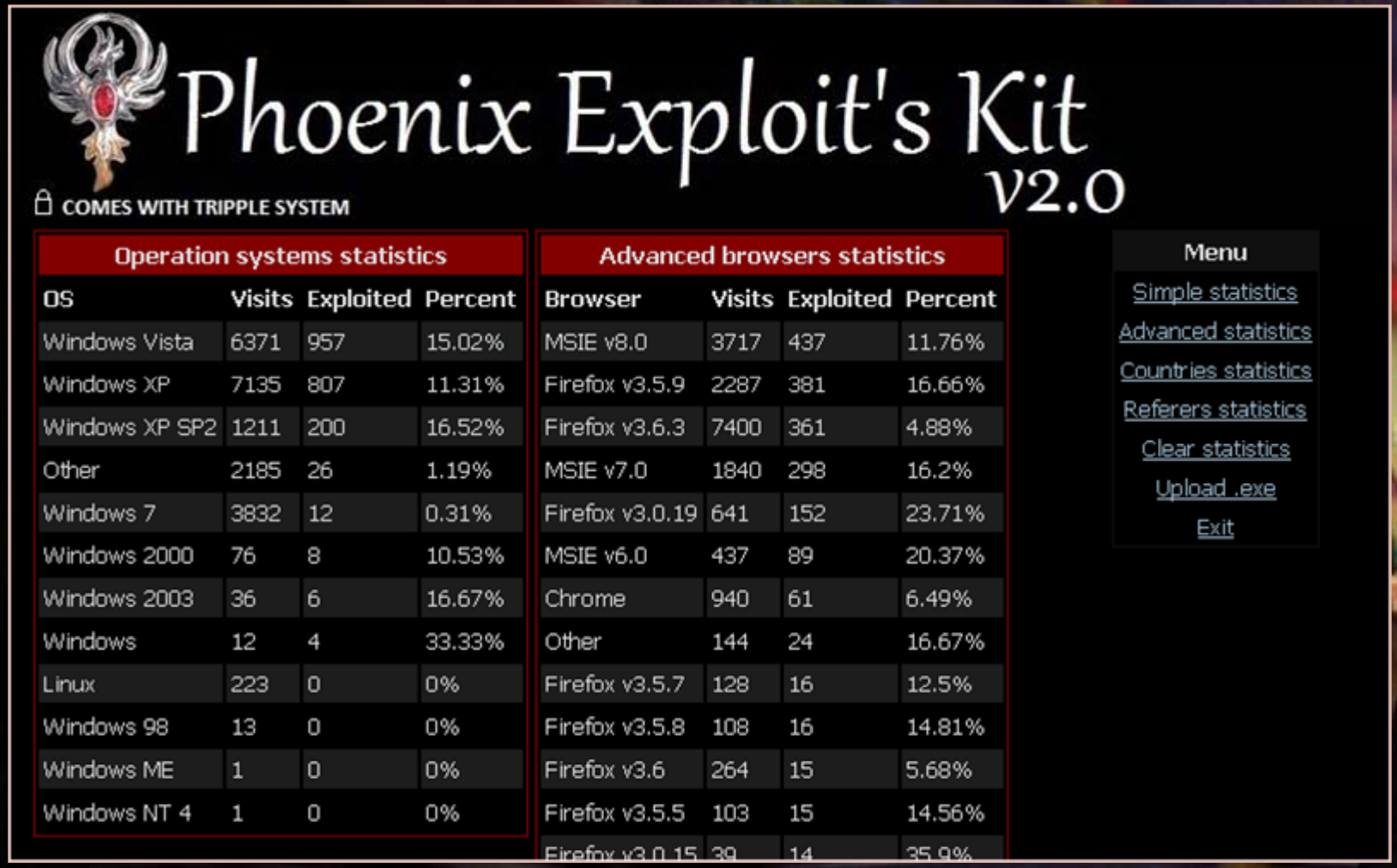
Exploit Toolkits

- Turn-key attack applications are rapidly evolving





Effectiveness of Exploit Toolkits



Phoenix Exploit's Kit v2.0

COMES WITH TRIPPLE SYSTEM

Operation systems statistics

OS	Visits	Exploited	Percent
Windows Vista	6371	957	15.02%
Windows XP	7135	807	11.31%
Windows XP SP2	1211	200	16.52%
Other	2185	26	1.19%
Windows 7	3832	12	0.31%
Windows 2000	76	8	10.53%
Windows 2003	36	6	16.67%
Windows	12	4	33.33%
Linux	223	0	0%
Windows 98	13	0	0%
Windows ME	1	0	0%
Windows NT 4	1	0	0%

Advanced browsers statistics

Browser	Visits	Exploited	Percent
MSIE v8.0	3717	437	11.76%
Firefox v3.5.9	2287	381	16.66%
Firefox v3.6.3	7400	361	4.88%
MSIE v7.0	1840	298	16.2%
Firefox v3.0.19	641	152	23.71%
MSIE v6.0	437	89	20.37%
Chrome	940	61	6.49%
Other	144	24	16.67%
Firefox v3.5.7	128	16	12.5%
Firefox v3.5.8	108	16	14.81%
Firefox v3.6	264	15	5.68%
Firefox v3.5.5	103	15	14.56%
Firefox v3.0.15	39	14	35.9%

Menu

- Simple statistics
- Advanced statistics
- Countries statistics
- Referers statistics
- Clear statistics
- Upload .exe
- Exit

殭屍電腦(Botnet)的用途

TippingPoint
IPS-SECURED NETWORKS

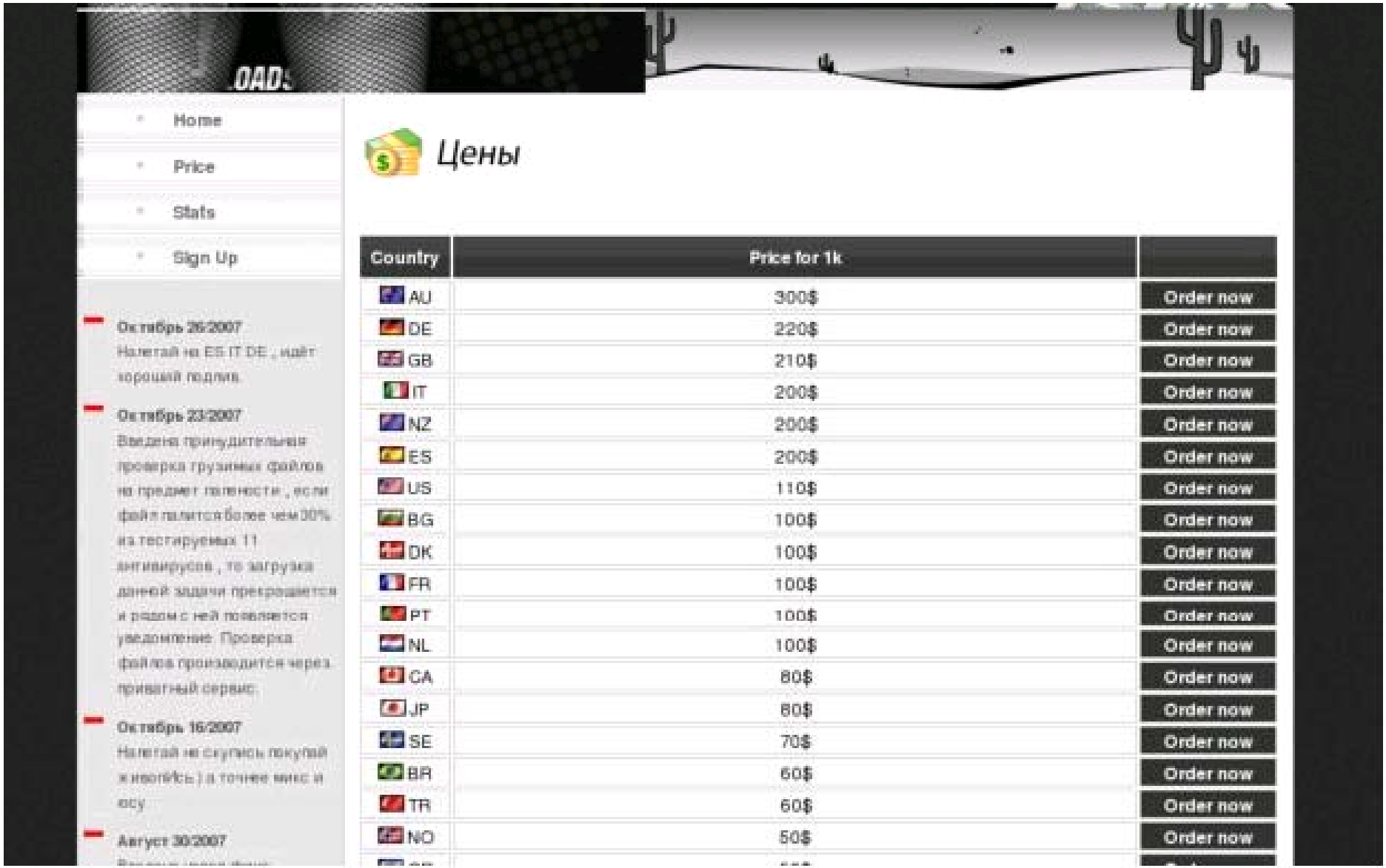
- **Botnet是有組織性的犯罪工具,主要用途包括:**
  - 發送垃圾郵件
  - 執行網路釣魚誘騙
  - 增加廣告點閱次數(click fraud)
  - 發動DDoS攻擊

- **要防止DDoS,企圖用異常流量演算來阻擋是不得已的下策:**
  - 異常流量演算一定有時間上的延誤與誤差值問題
  - 做好漏洞防護工作,避免電腦成為Botnet
  - 對IRC管控

任何人都可以租用Botnet

TippingPoint

IPS-SECURED NETWORKS



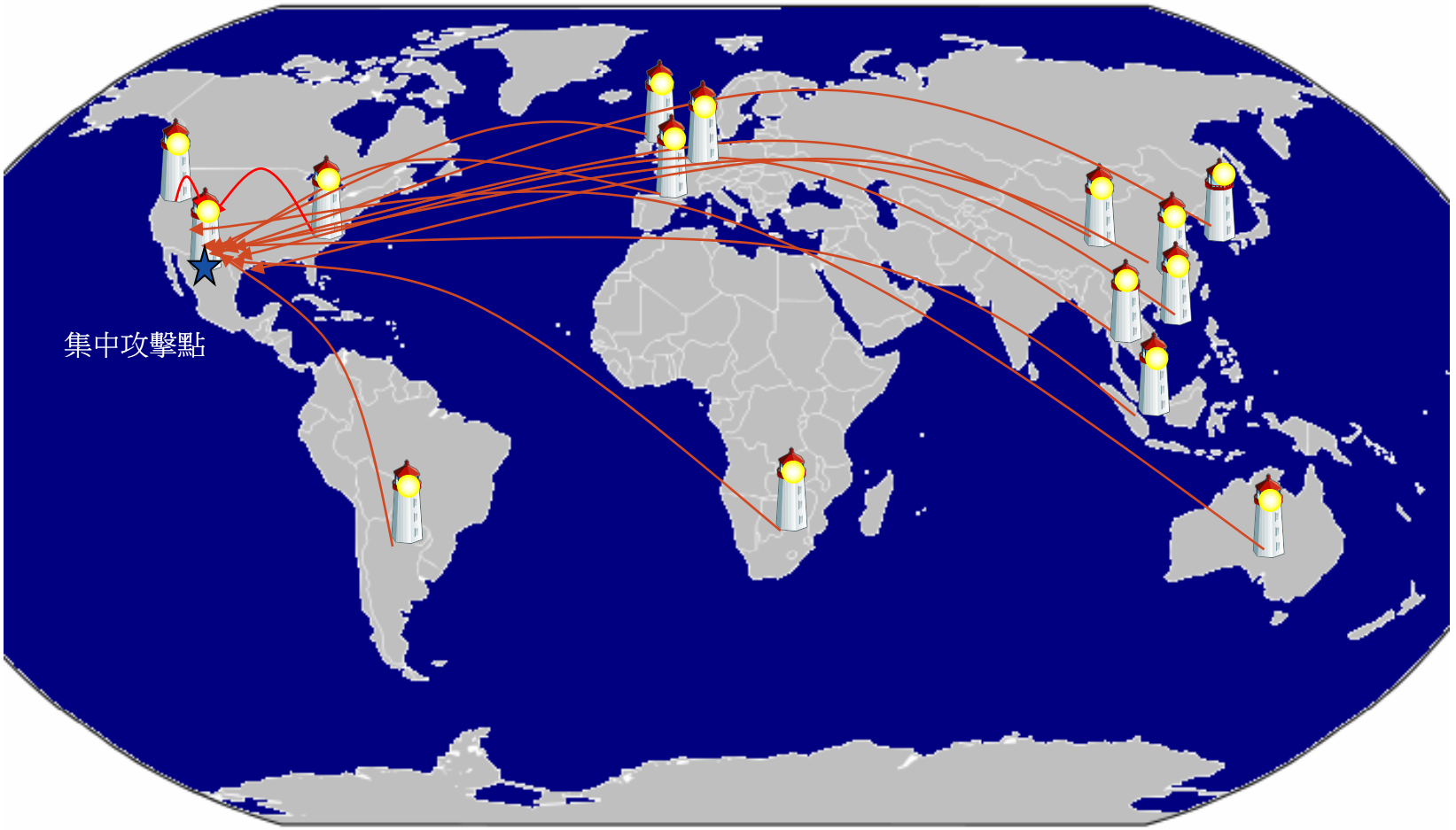
駭客運用殭屍電腦軍團發動攻擊

您的電腦很可能就是當中的一份子

TippingPoint

IPS-SECURED NETWORKS

- 發送垃圾郵件, 詐騙郵件, 夾檔中帶有惡意程式的郵件
- 大量猜測別人的帳號密碼
- 癱瘓他人的網站, 塞爆他人的頻寬



俄羅斯駭客發動網軍癱瘓愛沙尼亞政府網路

許多來自台灣的電腦參予了這次的攻擊

TippingPoint

IPS-SECURED NETWORKS

InfoWorld

Back to article Print this

Russian gov't not behind Estonia DDOS attacks

Analysis throws doubt on whether a single agency alone was involved

By Jeremy Kirk, IDG News Service

June 01, 2007

From alleged poisonings to organized crime, Russia has been getting a lot of bad press lately. But this time the country -- or at least, the government -- may be in the clear.

The string of crippling DDOS (distributed denial-of-service) attacks against Estonia didn't appear to be a coordinated attack by one entity ssia, wrote Jose Nazario, senior security engineer with Arbor Networks, in a commentary.

Estonia, a former satellite of the Soviet Union with a population of 1.3 million, came under int mmercial and government Web sites. The attacks came as Estonia moved a World War II memorial of a statue of a Soviet

Although Russia was quickly accused, Russian re suspicions than facts.

But further analysis throws do rio wrote.

While it is possible to spoof the to Tallin," Estonia's capital, Nazario wrote.

While the Russian government Russian-speaking computer gurus may have joined in.

Several Russian-language Web allow others to rig their computers to join in a DDOS attack, which involves sending massive streams of data to a Web site, causing it to crash. omputer to send data to a Web site.

"We see signs of Russian nationalism at work here, but no Russian government connection," Nazario wrote.

This week has been fairly quiet, said Hillar Aarelaid, chief security officer for Estonia's Computer Emergency Response Team.

"We have seen some attacks, but they are quite easy to handle," Aarelaid said, adding the DDOS attacks remain under investigation.

Critical Infrastructure Attacks

“Estonia… came under intense electronic attacks on April 27, jamming up commercial and government Web sites. – DDOS Attacks”

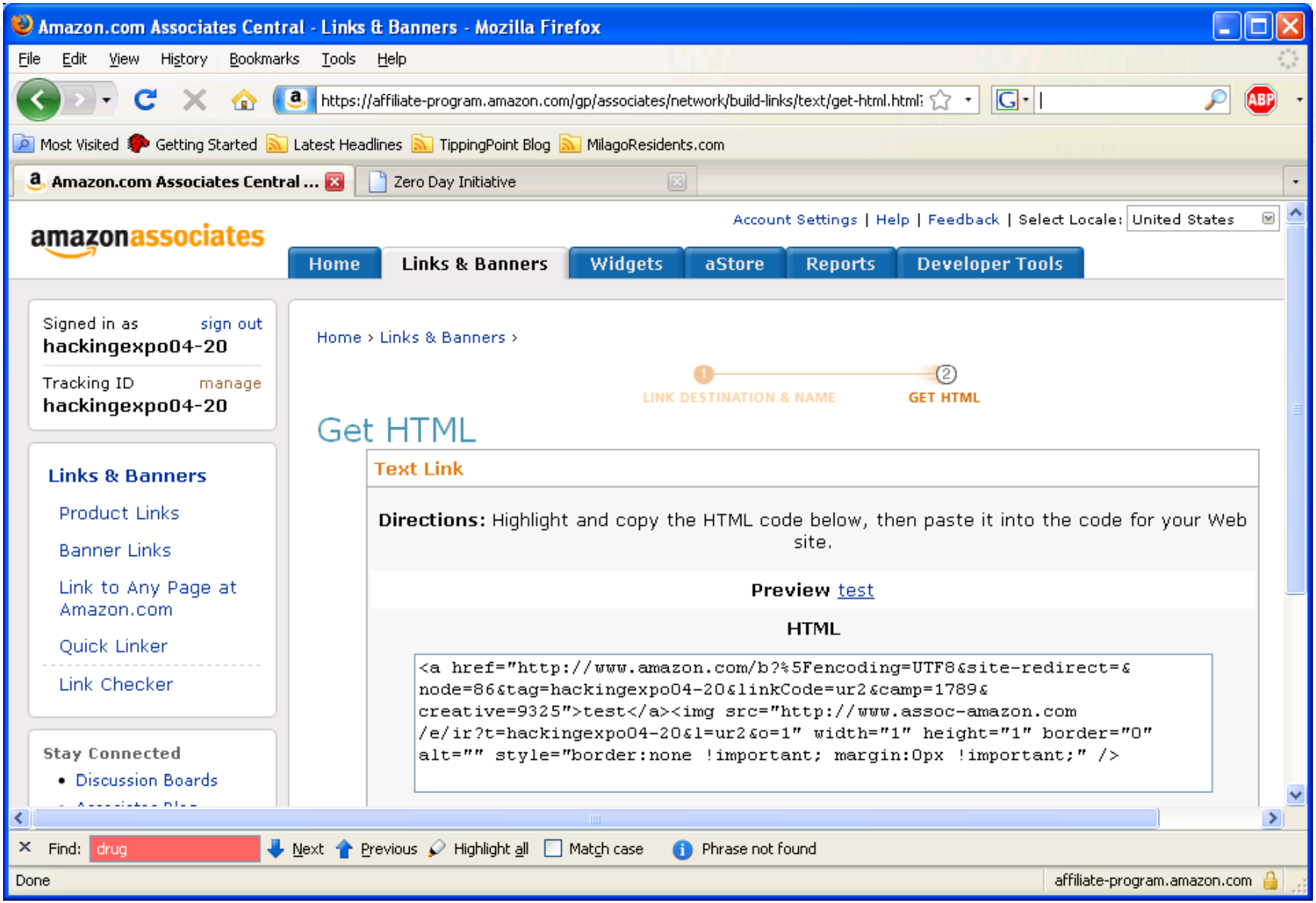
現今的網路犯罪

TippingPoint
IPS-SECURED NETWORKS

- 駭客的目的已經改變
  - 轉向以金錢為目的
- 駭客的目標轉向一般的網民
  - 大範圍的傳播給網路使用者(個人電腦)取代針對少數伺服器的入侵
- 多種手法
  - 零時差攻擊
  - 透過社交工程手法
  - 藉由社群網路傳播
- 最終目的
  - 引誘網民安裝惡意控制軟體(殭屍電腦)
  - 竊取網民電腦裡的資料
  - 騙取金錢

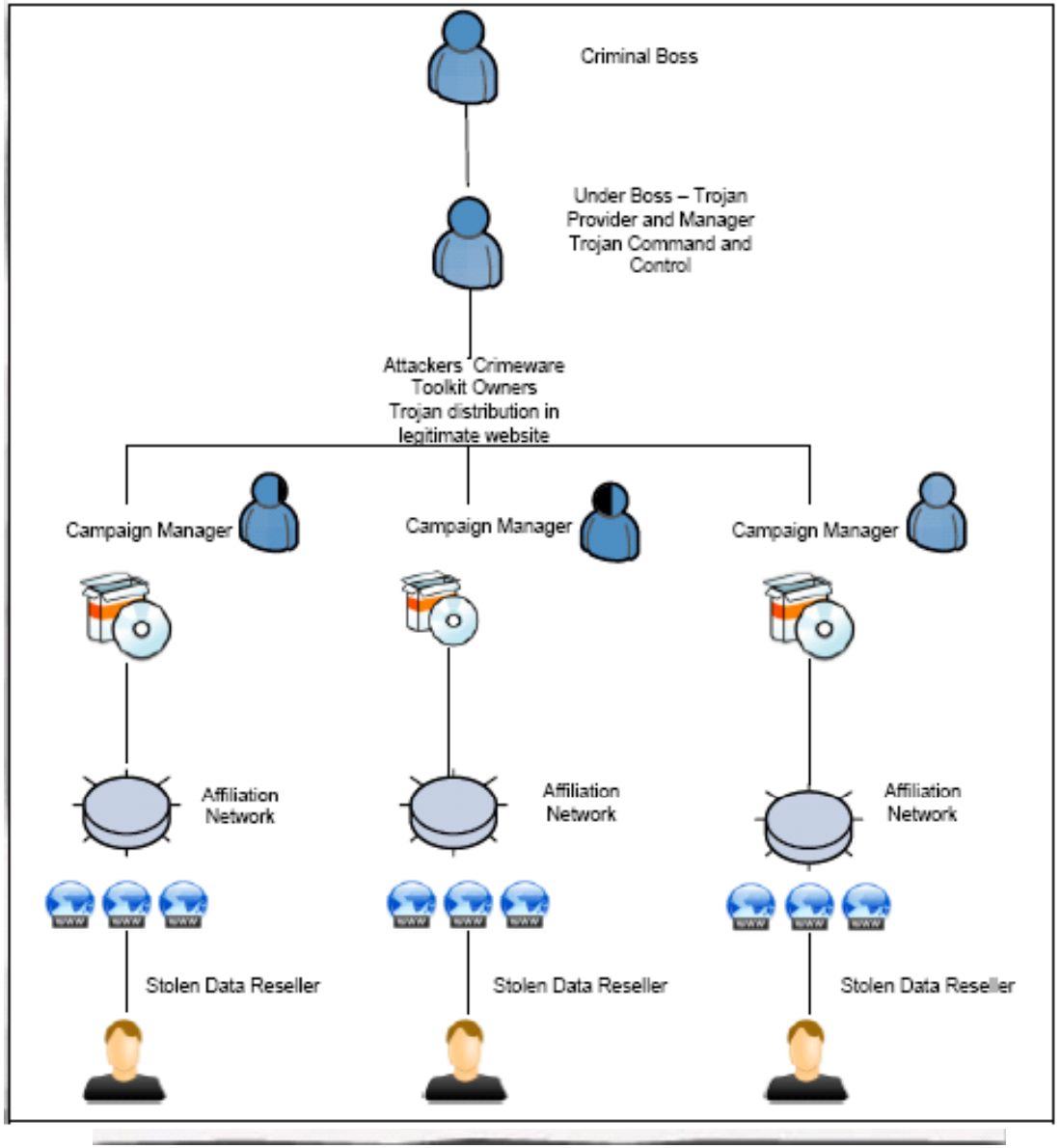
亞馬遜的協銷商業模式

TippingPoint
IPS-SECURED NETWORKS



亞馬遜協銷概念被運用在許多網路犯罪鏈中

TippingPoint
IPS-SECURED NETWORKS




Home
Scan
Settings
Quarantined list
Ignore list
MalwareRemoval BOT
SPYWARE, ADWARE & VIRUSES
Scan & Remove Malware, Spyware, & Unwanted Software from your PC!
Start Scan
Scan your PC for hidden Malware/Spyware
System Status:
Last updated: 1.9.3337.776
Version: 11.3.6
Total no. of scans: 0
Last scan time and result: <No scans>
Reset Statistics
Register Now!
Utilities:
BHO Manager
Full Registry Backup
Add/Remove Prog. Mngr.
Startup.Prog. Manager
Home Page Manager
Scan Scheduler
Quick Links
Quarantined List
Ignore List
Live Updates

看似真實的防毒防駭網站

TippingPoint
IPS-SECURED NETWORKS

Easy Spyware Cleaner

SpyRid

InfeStop

WinIFixer

Advanced XP Defender

Advanced XP Fixer

Malware Protector 2008

Antivirus XP 2008

銷售競賽?

豐富的獎品吸引眾多網友加入犯罪協銷

TippingPoint
IPS-SECURED NETWORKS

TRAFFIC CONVERTER

Contest: My Lexus. Results

VIP points contest finished.

N	Name	Points
Show webmasters...		

N	Name	Points
Hide webmasters...		
1	Webmaster	710
2	Webmaster	673
3	Webmaster	585
4	v-seo-deneg-net	556
5	Webmaster	540

N	Name	Points
Hide webmasters...		
1	Webmaster	466
2	napster	407

Winner:

433

Winners:

一個網路犯罪的統計資料

TippingPoint
IPS-SECURED NETWORKS

- 2009有一群資安專家試圖潛入一個專門在行銷假防毒產品的網路.
- 結果發現16天中,總共有180萬使用者被吸引到這個銷售假防毒產品的網頁.
- 只要成功吸引人到這個網站,社群的成員就可以獲得美金$9.6 cents,也就是說在這16天裡總共發出了$172,000 ($10,800/a day).
- 而安裝假防毒軟體的比例估計為7%-12%之間,也就是共有12萬6千人到21萬6千人執行下載.

Source: Finjan Cybercrime report

駭客入侵駭客

TippingPoint
IPS-SECURED NETWORKS

- 有一個駭客入侵了由另一個駭客所建立的網路犯罪集團資料庫,並將會員的非法收入明細公布在網路上.
- 發現第一名的週收入竟高達美金$158,568.86

Affiliate ID	Affiliate Username	Account Balance (USD)
4928	nenastniy	$158,568.86
56	krab	$105,955.76
2	rstwm	$95,021.16
4748	newforis	$93,260.64
5016	slyers	$85,220.22
3684	ultra	$82,174.54
3750	cosma2k	$78,824.88
5050	dp322	$75,631.26
3886	iamthevip	$61,552.63
4048	dp32	$58,160.20

踢爆最新下載騙術

TippingPoint
IPS-SECURED NETWORKS

Step

1.例如「 http://www.tinydl.com/ 」是一個讓網友分享檔案的網站，進入檔案分享頁面，我們將看到為數不少的連結，如果耐心等待，這裡大部分檔案都可下載，只是要等比較久。若你急著想下載，可能會被圖中的廣告連結吸引。

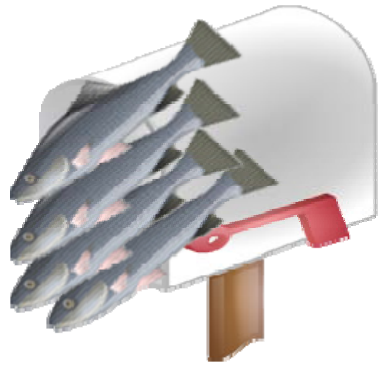
2.哇！好多我需要的東西，網頁上聲稱均可免等待、直接下載。點選速率最快的下載伺服器試試。

3.結果是無法下載！此時網站要你填寫一張表格。您或許會想:反正我用十分鐘信箱，不怕它寄垃圾信。

4.但是您會發現，想要有高速下載的服務是要錢的！但是通常他們的收費超低，宣稱僅支付5～20美金，便可永久、無限制地下載全部資源。雖然大多數人看到要錢就直接退出了，但也是會有心急想抓重要軟體的網友，想說付點小錢趕快抓到檔案要緊。於是就受騙上當了！

5.原來，這類網站都是類似的騙人手法：他會先誘騙你支付少許費用，據說加入會員之後，會給你一套P2P工具，功能與我們常用的eMule並無多少差別，但是會暗藏許多木馬程式，即使你真的能下載到想要的軟體，也可能是被加料下過間諜程式的。因此提醒各位不要因為花費不多而上當受騙喔（下載盜版軟體原本就不應該了）。

何謂「網路釣魚」？



「網路釣魚」，英文為Phishing，根據反網路釣魚工作小組（APWG）所做的定義，「網路釣魚」是利用**偽造電子郵件**與**幾可亂真的仿冒網站**作為誘餌，愚弄使用者洩漏如銀行帳戶密碼、信用卡號碼等個人機密資料的一種駭客手法。

根據調查: 利用知名品牌所建立的信賴感，讓此類詐騙行為成功機率達5%

MSN...越來越受駭客喜歡的詐騙管道

TippingPoint
IPS-SECURED NETWORKS

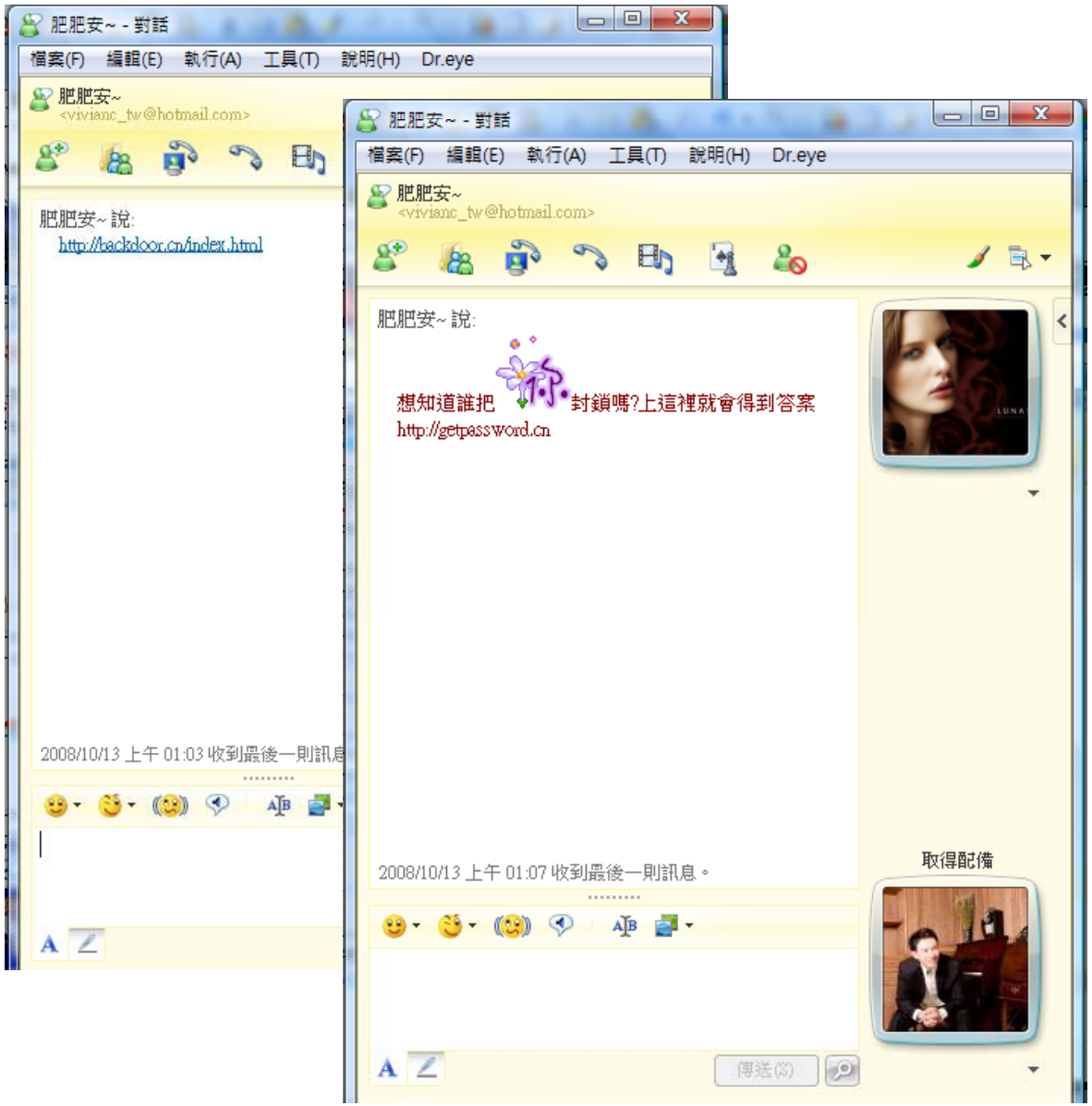
- 對方離線還送來訊息?
- 都是一些連結

→切勿點選

→儘快通知對方進行電腦掃毒並且更換MSN密碼

MSN...越來越受駭客喜歡的詐騙管道(續)

TippingPoint
IPS-SECURED NETWORKS



- 對方在線
- 甚麼都沒說直接給一個連結

→點選前先回一段文字確認

微軟與警政署的防駭提示

TippingPoint
IPS-SECURED NETWORKS

微軟帳號被盜處理協助

TippingPoint
IPS-SECURED NETWORKS

1

微軟線上服務事業群與內政部警政署連合呼籲，若網友不幸遇到詐騙或帳號被駭的情形，可立即撥打內政部反詐騙諮詢專線 165 尋求諮詢，並透過 Windows Live Windows Live 協助中心 http://windowslivehelp.com 尋求線上客服支援。

2

微軟與知名圖文部落客四小折、米滷蛋合作，利用有趣的圖文漫畫，傳遞清楚易懂的網路防身秘技，加強推廣網路安全與防詐知識，致力於保障使用者線上安全，降低網路安全危機，提高網友對網路詐騙手法的警覺性。

3

您還可透過以下資訊協求協助

- **帳號被盜協助** https://windowslivehelp.com/PasswordReset.aspx
- **帳號取回步驟協助** http://explore.live.com/post/110220/PasswordReset
- **網路防詐指南** http://3c.msn.com.tw/messenger/msncentral/feature/2011_BT/default.htm
- **165 全民防騙超連結** http://165.gov.tw/index.aspx

社交網站是容易洩漏個資的地方

Facebook? 非死不可?

TippingPoint

IPS-SECURED NETWORKS

謊稱要送你虛擬貨幣

其實是要得到
你的個人資料

Facebook個資在網路上公開販賣

TippingPoint
IPS-SECURED NETWORKS

網安／驚！駭客兜售150萬筆Facebook帳號

NOWnews 今日新聞 更新日期：2010/04/26 09:42　記者蘇湘雲／綜合報導

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

（看全部文章→）

據外媒報導，VeriSign旗下網路安全情報機制iDefense發現，這顯示平均每300名Facebook用戶中，就有一人的帳號被盜取，150萬筆的Facebook帳號的售價是根據使用者聯絡人名單數量，少於10名友人的1000筆帳號售價為25美元，超過10名友人的1000筆帳號售價為45美元。

而沒有聯絡人的使用者帳號則是另有價值，駭客可用這些帳號來散布惡意軟體，或是擴大該帳號的聯絡人數量後再開價。報導說，犯罪集團還會利用盜來的帳號向該用戶的好友發送信息，謊稱自己在國外遇上困難而需要錢回國，引誘上當。

iDefense並發現，社交網路帳號在黑市中的需求快速成長，因此建議社交網站用戶嚴格限制個人檔案的檢視權，避免與他人分享個人資訊，發現可疑活動應立即檢舉，父母家長也應關心家中孩童使用社交網路的狀況。

以為是在玩網路遊戲,卻不知不覺開啟視訊功能

TippingPoint

IPS-SECURED NETWORKS

請看影片

網路視訊?小心全都錄

TippingPoint
IPS-SECURED NETWORKS

yam 天空新聞 News

新聞 網頁 圖片 搜尋

首頁 | 即時 | 影音 | 專輯 | 政治 | 財經 | 娛樂 | 運動 | 汽車 | 社會 | 兩岸 | 國際

即時 專輯 排行 討論 圖片 影音

情侶MSN赤裸訊愛 駭客全都錄 PK! 此新聞

中廣新聞網／杜大澂 2009-01-14 07:42

調整字級： 小 中 大 特

基隆有一名男子，自稱「網愛駭客」，他涉嫌利用駭客手法入侵網友的MSN和即時通，側錄私密影像，再向被害人恐嚇，警方清查，至少有六名女子受害。

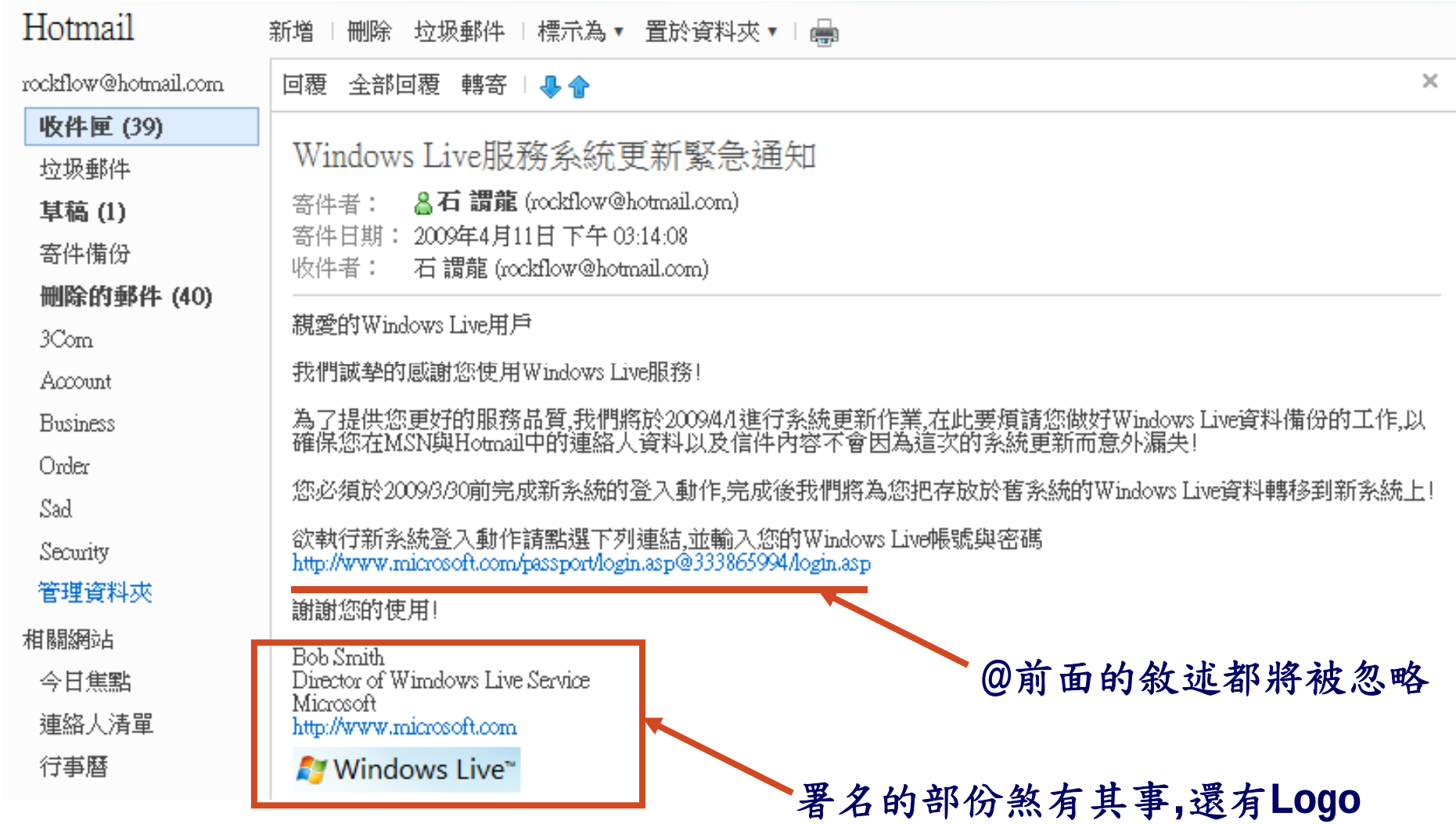
報案的一名小姐指出，她是在和男友透過即時通，傳送私密裸露愛撫的視訊影像，卻發現第三者在線上觀看，緊急關閉視訊之後，對方傳了即時訊息，自稱是「網愛駭客」，已經將視訊檔案側錄，如果不想影片被散佈，必需依照指示再直播一次。

刑事局偵九隊一組是獲報，清查網路資料和通聯紀錄，鎖定嫌犯身分，循線在基隆將徐姓男子逮捕。

警方調查，嫌犯是入侵被害人的網路連線之後，利用HyperCam Video軟體側錄網愛畫面之後，向被害人恐嚇，警方從查扣的電腦主機發現，至少有六名女子受害，警方除了依妨害電腦使用和恐嚇等罪嫌移送法辦，是否還有其他人受害，也將進一步清查。

您曾經收到類似的信件嗎?

TippingPoint
IPS-SECURED NETWORKS

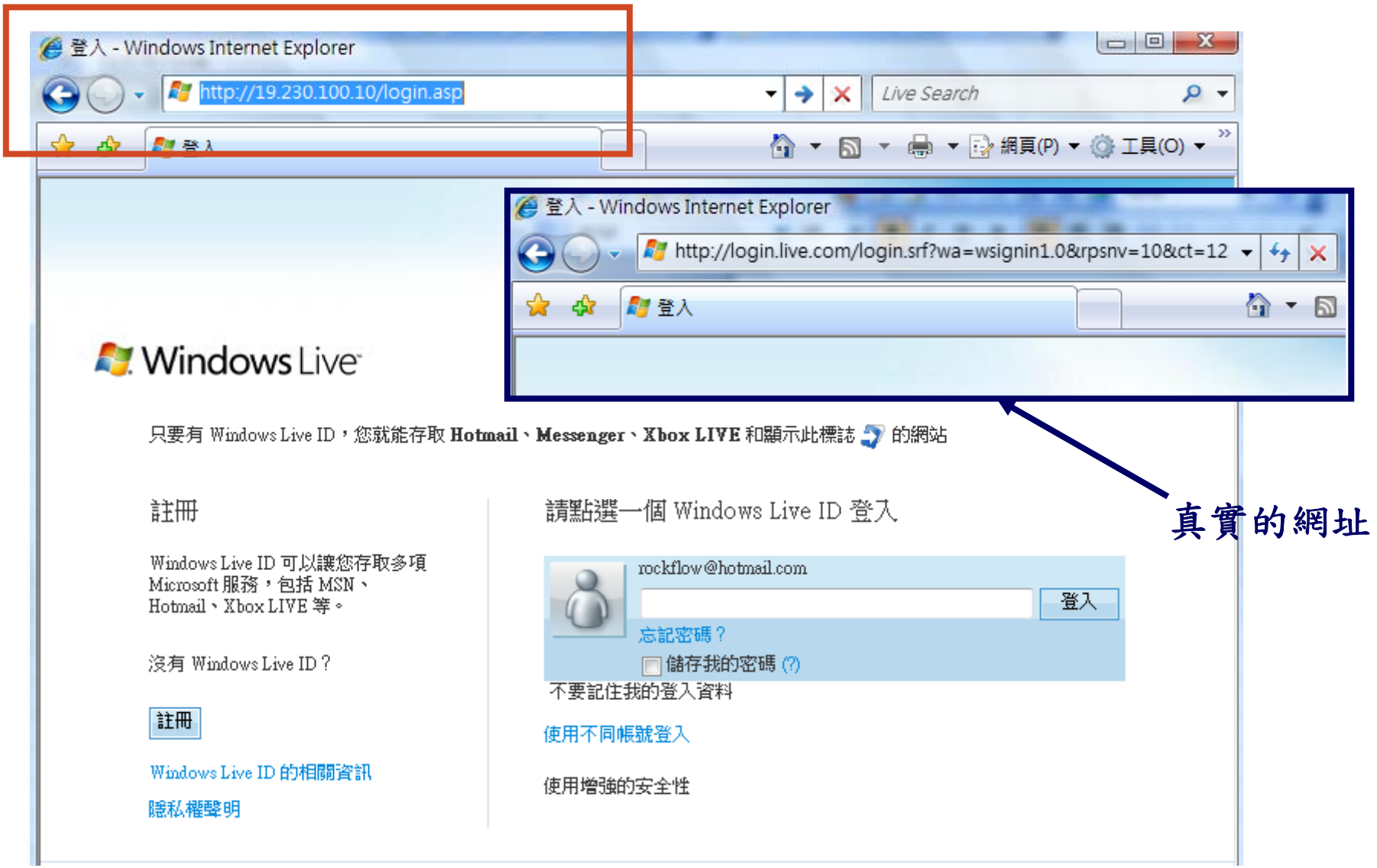


網址列用IP來呈現?

登入畫面幾可亂真

TippingPoint

IPS-SECURED NETWORKS



簡單辨識釣魚信件的方式

TippingPoint
IPS-SECURED NETWORKS

1. 非HTTPS
2. 用IP代替URL網址– this is NOT PayPal!

考驗眼力嗎?釣魚網址註冊的跟真的超級像

TippingPoint
IPS-SECURED NETWORKS

是「l」?還是「1」?

土地銀行 **http://www.landbank.com.tw**

→釣魚網址 **http://www.1andbank.com.tw** ← 竊取網銀帳號密碼

是「o」?還是「0」?

雅虎奇摩拍賣 **http://tw.bid.yahoo.com**

→釣魚網址 **http://tw.bid.yah00.com** ← 竊取拍賣帳號密碼

若是不慎將自己的帳號密碼登入到假網站中,往往會出現錯誤訊息

→因為這是假的網站,沒有資料庫可以比對帳號密碼的正確性

結合Google關鍵字廣告的釣魚網址

TippingPoint
IPS-SECURED NETWORKS

透過Google查詢「拍賣」

竟看到假的Yahoo拍賣網站
tw.bids-yahoo.com

結合Google關鍵字廣告的釣魚網址(續)

TippingPoint
IPS-SECURED NETWORKS

真的Yahoo拍賣

假的Yahoo拍賣

校園網路安全使用手則

電子郵件社交工程手法之防範

注意可疑電子郵件之特徵

TippingPoint
IPS-SECURED NETWORKS

要求輸入並送出個人私密資料的郵件

→任何要求您提供個人姓名、生日、身份證字號、電子郵件帳號與密碼，或其他相關個人資料的電子郵件，無論寄件人是什麼身份，這樣的郵件八九不離十是屬於詐騙信件。若您還是相信這封郵件的合法性，請先複製網站的 URL 後貼上，或是上該公司的網站查清楚他們的連絡資訊。不要直接回覆郵件或按下任何超連結。請即刻連絡該公司的支援部門，確認該封郵件的合法性。

內文含有這樣的描述

→通常那些字句不通順、錯字連篇，或是有類似「這是千真萬確的」或「請將這封信轉寄給您所有的朋友」句子的電子郵件，都應該要多加留意。即使不是惡意郵件，常常也是以訛傳訛的內容。

電子郵件社交工程手法之防範

注意可疑電子郵件之特徵(續)

TippingPoint
IPS-SECURED NETWORKS

- 過於聳動的主旨或是緊急處置要求

→吸引您來開啟

- 不正常的發信時間

→半夜兩點同事居然寄信來?

- 陌生人或少往來對象來信

→很久沒連繫的朋友?除非是發喜帖吧!

- 認識的人來信但主旨或內容與其習性不符

→老王只愛打麻將,居然寄MP3來?

電子郵件社交工程手法之防範

調整收信程式的安全性

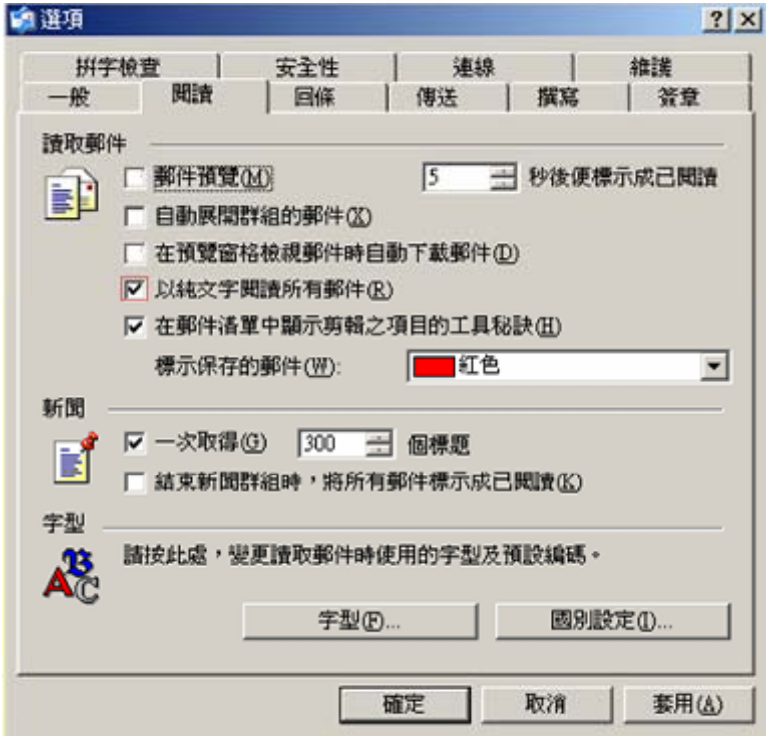
TippingPoint

IPS-SECURED NETWORKS

- 關閉郵件預覽功能
- 關閉在預覽窗格檢視時自動下載郵件
- 勾選以純文字閱讀所有郵件

以Outlook Express為例:

選項→閱讀



- 關閉郵件預覽窗格

以Outlook Express為例:

檢視→版面配置→預覽窗格

電子郵件社交工程手法之防範

調整收信程式的安全性(續)

TippingPoint
IPS-SECURED NETWORKS

- 點選受限制的網站區域
- 勾選在其它應用程式試圖以我的名義傳送電子郵件時警告我

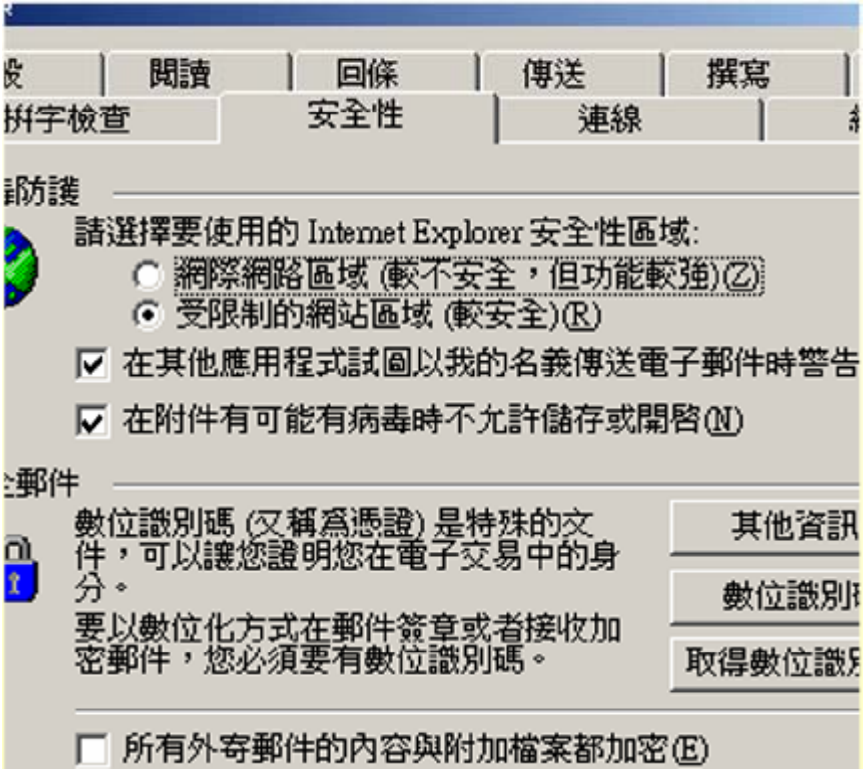
→避免在不知情的狀況下傳送郵件

→駭客會利用入侵成功的電腦代為發送惡意郵件

- 勾選在附件有可能有病毒時不允許儲存或開啟

以Outlook Express為例:

選項→安全性



電子郵件社交工程手法之防範

養成良好的使用習慣

TippingPoint
IPS-SECURED NETWORKS

- 非必要閱讀之郵件逕行刪除

→非公務與教學必要的郵件

- 檢查寄件者與郵件地址的真實性

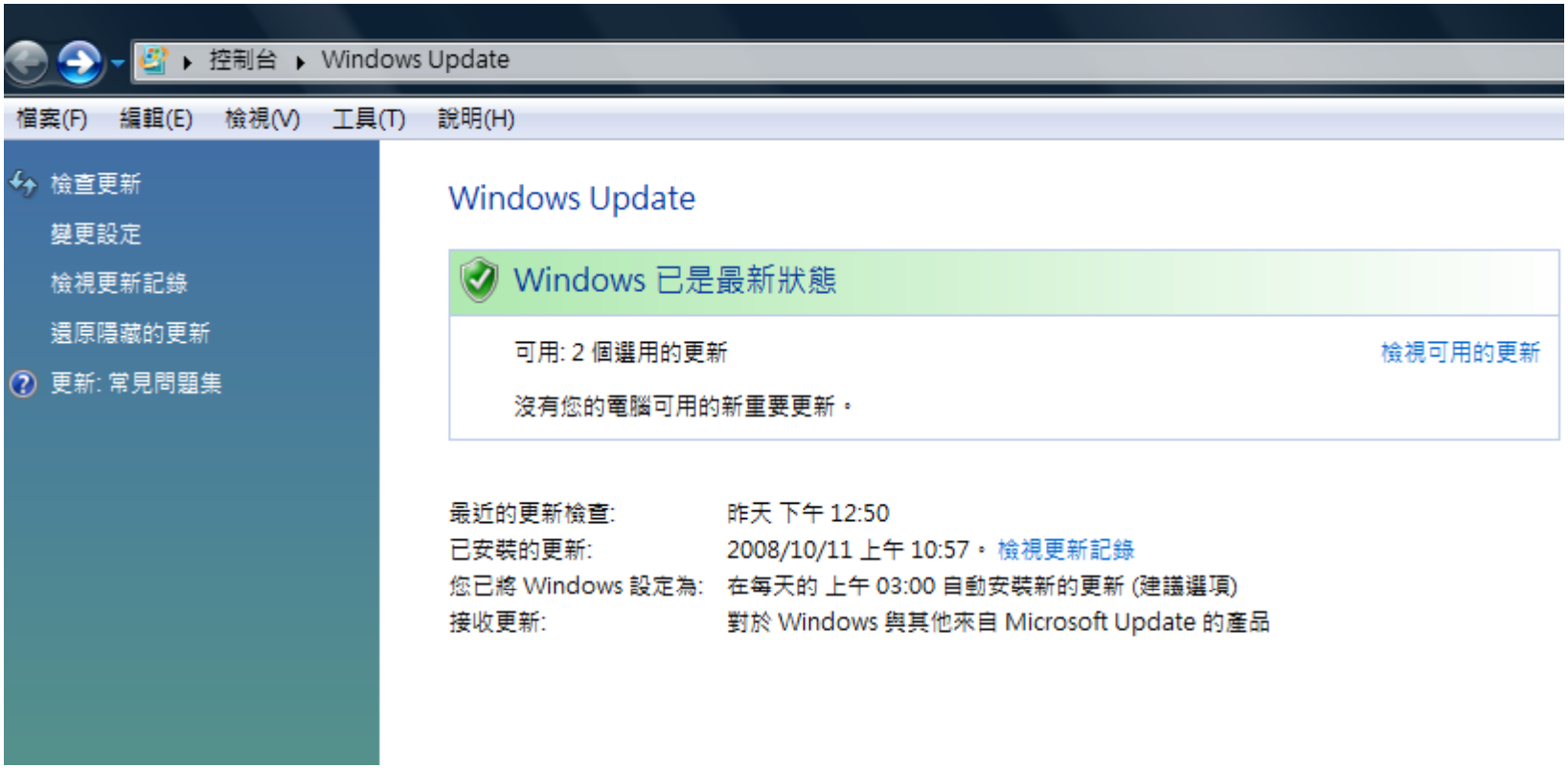
→直接在寄件者處按滑鼠左鍵兩次

- 開啟郵件內含之超連結時先確認連線網址之網域名稱(Domain Name)是否足以識別？若為數字IP之網址勿輕易開啟

→http://www.microsoft.com/passport/login.asp@333865994/login.asp

隨時更新系統與防毒軟體

TippingPoint
IPS-SECURED NETWORKS



- 漏洞修補是資安防護最重要的工作→駭客無法將植入惡意程式(ex:木馬)
- 別讓自己的電腦變成殭屍Botnet→駭客不能藉由您的電腦轉發惡意郵件
- 不僅是Windows,還有各種應用程式(ex: Adobe)

善用警政署提供的資源

TippingPoint
IPS-SECURED NETWORKS

免費防毒軟體與免費線上掃毒服務資源列表
http://www.cib.gov.tw/interview/service01_2.aspx?no=36

免費電腦健康檢查程式**NPASCAN v1.7** 附件下載：
下載處**1.** http://www.police.org.tw/NPASCAN_1.7.zip
下載處**2.** **http://www.npa.gov.tw/NPAGip/wSite/public/Attachment/f1234227146655.zip**

還有甚麼值得注意的地方?

TippingPoint
IPS-SECURED NETWORKS

- 將常用的網站,特別是需要登入帳號密碼的網站(網銀,拍賣,電子郵件...)加入我的最愛

→避免使用搜尋引擎來搜尋網址
→避免不必要的輸入錯誤
→避免從電子郵件中的連結直接點選

- 常更新密碼

→不要通用一個密碼
→使用滑鼠點選的螢幕虛擬鍵盤
更可以避免側錄風險

TippingPoint

Q & A

感謝您的耐心聽講與指導

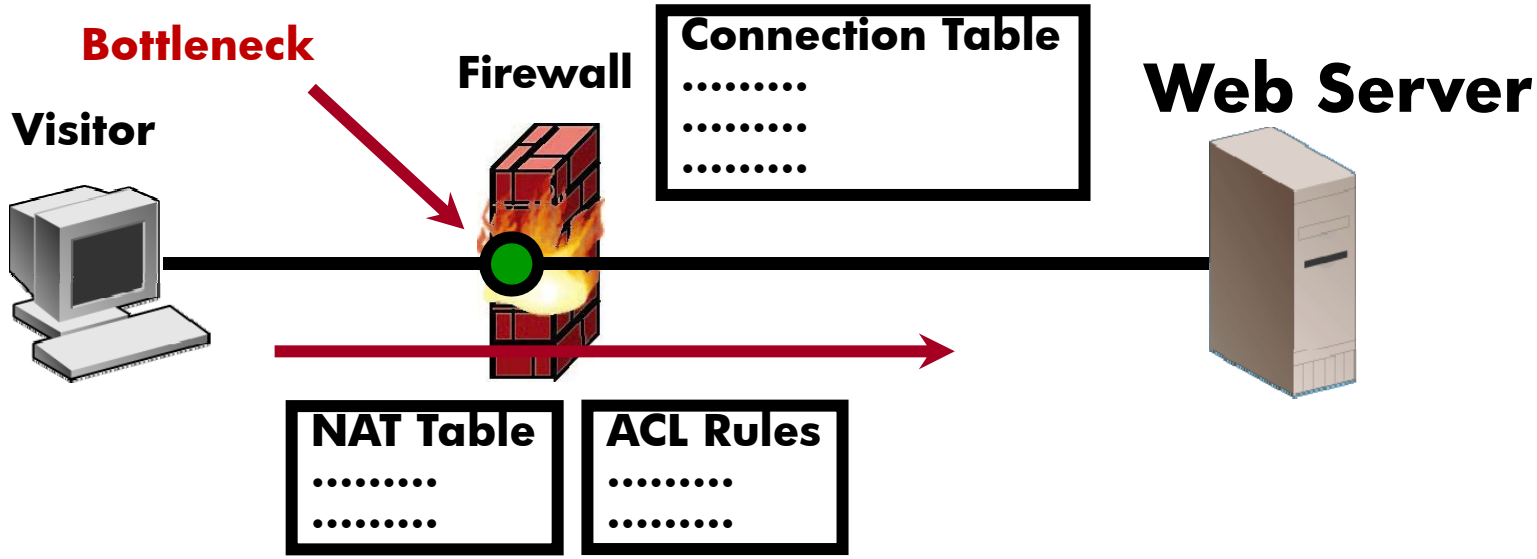
石謂龍 Robin Shih rshih@tippingpoint.com 0935784086

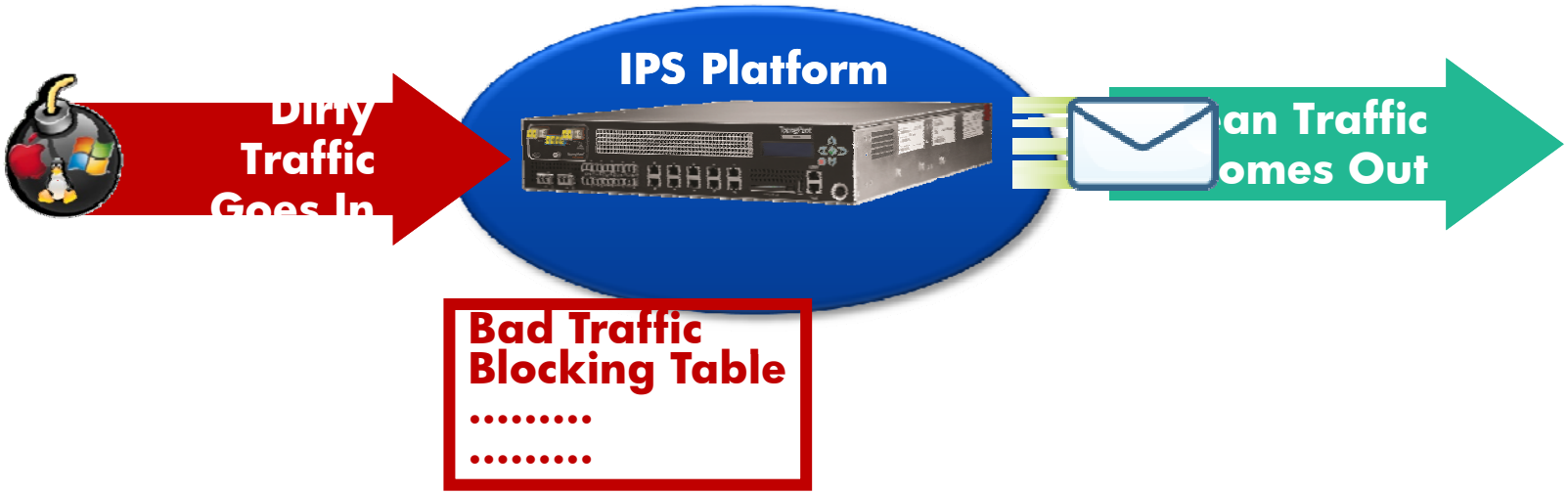
IPS-SECURED NETWORKS

IPS V.S. Firewall

TippingPoint
IPS-SECURED NETWORKS

巨量TCP Session佔據Firewall的資源導致網路緩慢

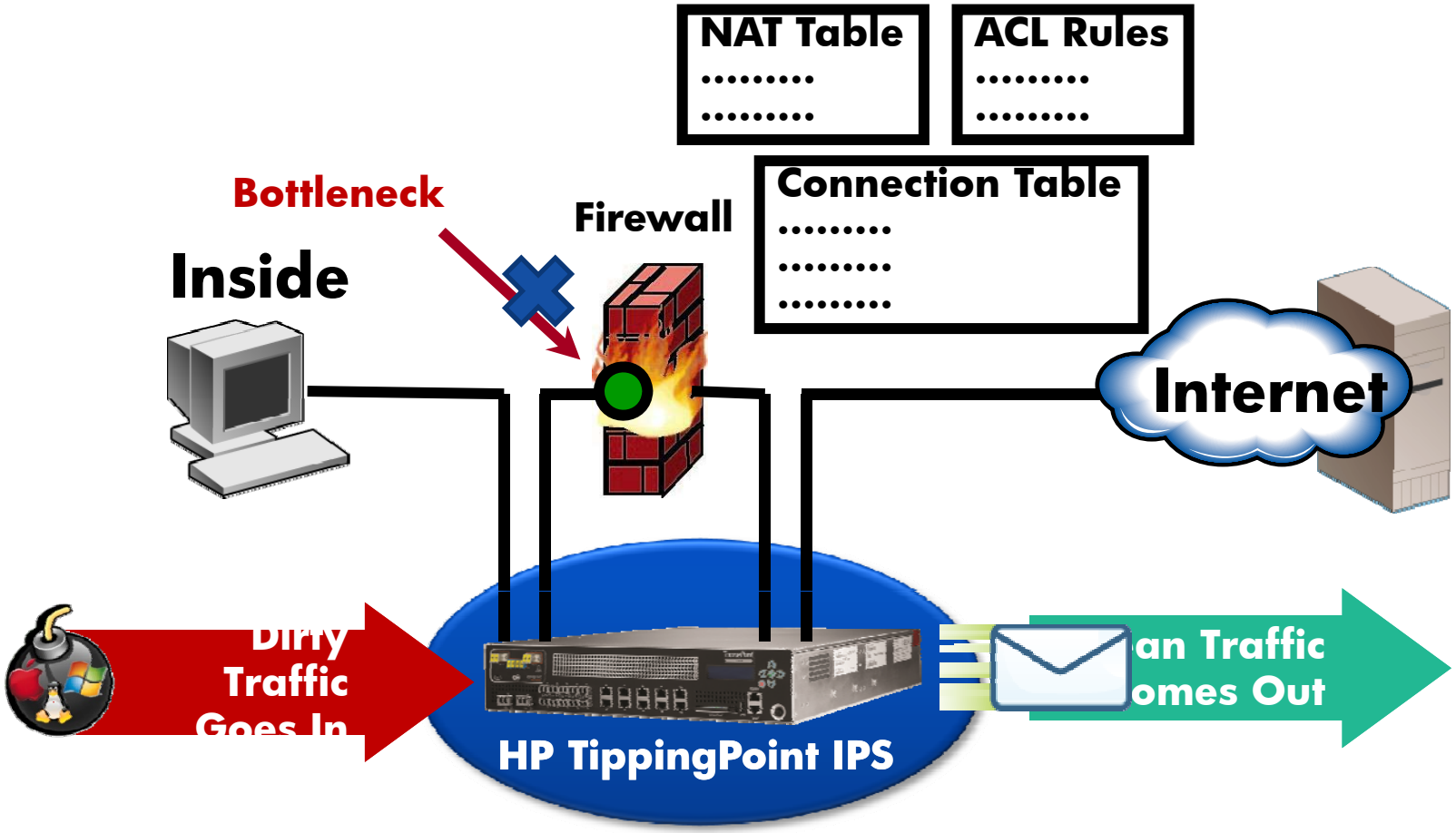




IPS co-work with Firewall

TippingPoint

IPS-SECURED NETWORKS



網路防護架構

TippingPoint

IPS-SECURED NETWORKS

- Blocks threats attacking applications and operating systems
- Network-embedded and standalone devices
- Endpoint management
- Protection for physical, virtual,
  and cloud environments