中華電信
Chunghwa Telecom

社交工程演練
說明會

報告人

中華電信 數據通信分公司

Refresh your life

大綱1/2

- 公文依據、廠商交付報告
- 何謂社交工程?
- 社交工程演練目的
- 駭客入侵過程各階段
  - 1.帳號蒐集階段(社交工程演練)
  - 2.弱密碼試探階段
  - 3.誘騙階段(社交工程演練)
  - 4.資訊蒐集階段(臥底長達數年)
  - 5.破壞階段

大綱2/2

❖防制作法

- 1. 收信軟體關閉自動化預覽
  - HTML預覽(關閉)
  - 自動下載圖片(關閉)
- 2.使用純文字模式檢查信件
  - 警覺性判斷
    - 人(我認識寄件者嗎?)
    - 事、時(跟我近期工作內容有關嗎?)
    - 地(URL有奇怪的IP或網域)
- 3.附檔安全檢查(請強烈懷疑同事寄的檔案是否有毒?)

❖結語

公文依據

- 行政院國家資通安全會報所公佈的
  - 國家資通安全通報應變作業綱要

5.2.2 防範惡意電子郵件社交工程演練

（一）演練目的：提高「資通安全處理小組」及其所屬機關(構)對社交工程攻擊防制認知。

（二）演練時間：每年不定期至少辦理 2 次，由資通安全處理小組自行規劃及執行，惟須於每年 4 月底前辦理第 1 次演練，並於 9 月底前辦理第 2 次演練。

（三）一般說明：

1. 演練對象由資通安全處理小組自行決定，惟主管機關及所屬機關(構)具有公務電子郵件人員，須 1/4(含)以上參與演練。
2. 演練實施前須訂定演練計畫，簽奉機關資安長核定。
3. 完成演練作業後，機關應召開「檢討會議」，檢討辦理情形及演練結果；演練報告須經機關資安長核定，並於每次演練完成後 1 個月內主動送本會報政府資通安全組備查。

修正

3. 完成演練作業後，須由機關資安長召開「檢討會議」，檢討辦理情形及演

附件二：電子郵件社交工程演練未達基準檢討與改善計畫

機關(單位名稱) 電子郵件社交工程演練未達基準檢討與改善計畫

一、 演練結果概述：

(說明及比較分析去年度演練結果)

二、 未達基準原因檢討：

(瞭解歸納同仁開啟演練信件原因以為預防)

三、 改善策略及作為：

(含本部要求辦理之教育訓練、對開啟人員口頭告誡等各項措施，以及機關(單位)自訂之改善策略及作為，如對重點對象(連續 2 次演練均開啟、開啟多封演練信件)之加強措施等)

四、 改善辦理情形：

(說明前項相關改善策略及作為之辦理情形)

五、 結語：

廠商交付報告(1/7)

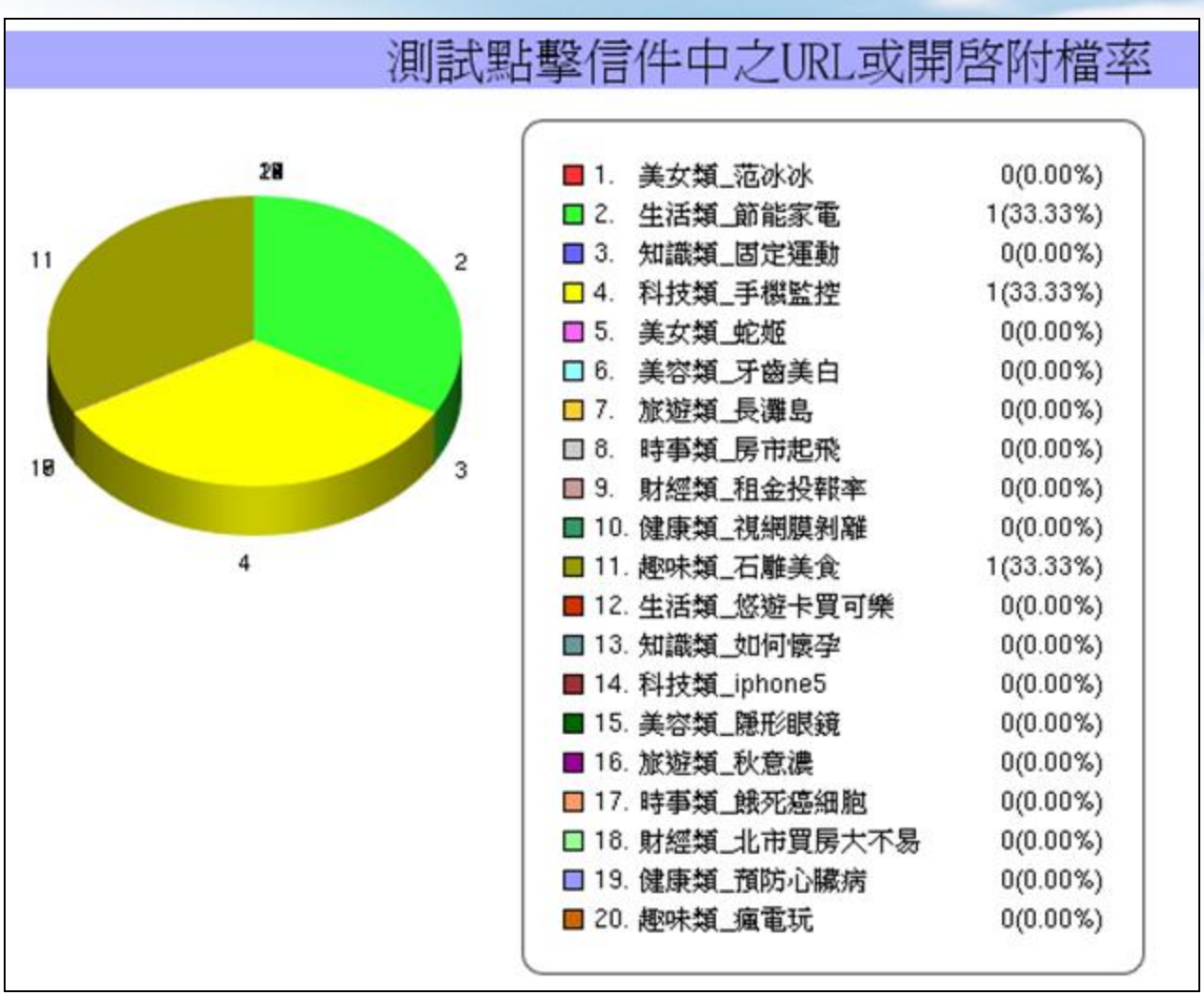
信件類型	連線方式	點擊人數	分類點擊人數
生活類_節能家電	開啟信件	1	2
	點擊信件中之 URL 或開啟附檔	1	
知識類_固定運動	開啟信件	4	4
	點擊信件中之 URL 或開啟附檔	0	
科技類_手機監控	開啟信件	2	3
	點擊信件中之 URL 或開啟附檔	1	
美女類_蛇姬	開啟信件	1	1
	點擊信件中之 URL 或開啟附檔	0	
美容類_牙齒美白	開啟信件	2	2
	點擊信件中之 URL 或開啟附檔	0	
旅遊類_長灘島	開啟信件	1	1
	點擊信件中之 URL 或開啟附檔	0	
時事類_房市起飛	開啟信件	4	4
	點擊信件中之 URL 或開啟附檔	0	

廠商交付報告(2/7)

測試開啓信件率

1.	美女類_范冰冰	0(0.00%)
2.	生活類_節能家電	1(4.17%)
3.	知識類_固定運動	4(16.67%)
4.	科技類_手機監控	2(8.33%)
5.	美女類_蛇姬	1(4.17%)
6.	美容類_牙齒美白	2(8.33%)
7.	旅遊類_長灘島	1(4.17%)
8.	時事類_房市起飛	4(16.67%)
9.	財經類_租金投報率	2(8.33%)
10.	健康類_視網膜剝離	2(8.33%)
11.	趣味類_石雕美食	5(20.83%)
12.	生活類_悠遊卡買可樂	0(0.00%)
13.	知識類_如何懷孕	0(0.00%)
14.	科技類_iphone5	0(0.00%)
15.	美容類_隱形眼鏡	0(0.00%)
16.	旅遊類_秋意濃	0(0.00%)
17.	時事類_餓死癌細胞	0(0.00%)
18.	財經類_北市買房大不易	0(0.00%)
19.	健康類_預防心臟病	0(0.00%)
20.	趣味類_瘋電玩	0(0.00%)

廠商交付報告(3/7)


測試點擊信件中之URL或開啓附檔率
11
2
10
3
4
1. 美女類_范冰冰 0(0.00%)
2. 生活類_節能家電 1(33.33%)
3. 知識類_固定運動 0(0.00%)
4. 科技類_手機監控 1(33.33%)
5. 美女類_蛇姬 0(0.00%)
6. 美容類_牙齒美白 0(0.00%)
7. 旅遊類_長灘島 0(0.00%)
8. 時事類_房市起飛 0(0.00%)
9. 財經類_租金投報率 0(0.00%)
10. 健康類_視網膜剝離 0(0.00%)
11. 趣味類_石雕美食 1(33.33%)
12. 生活類_悠遊卡買可樂 0(0.00%)
13. 知識類_如何懷孕 0(0.00%)
14. 科技類_iphone5 0(0.00%)
15. 美容類_隱形眼鏡 0(0.00%)
16. 旅遊類_秋意濃 0(0.00%)
17. 時事類_餓死癌細胞 0(0.00%)
18. 財經類_北市買房大不易 0(0.00%)
19. 健康類_預防心臟病 0(0.00%)
20. 趣味類_瘋電玩 0(0.00%)

廠商交付報告(4/7)

單位	單位人數	連線方式	點擊人數	單位點擊人數	單位點擊比例	佔全部點擊比例
人文社會學科	1	開啟信件	0	0	0%	0%
		點擊信件中之 URL 或開啟附檔	0			
人文社會學院	1	開啟信件	0	0	0%	0%
		點擊信件中之 URL 或開啟附檔	0			
人事室	5	開啟信件	1	1	20%	7.14%
		點擊信件中之 URL 或開啟附檔	0			
工商業設計系	1	開啟信件	0	0	0%	0%
		點擊信件中之 URL 或開啟附檔	0			
工程學院	3	開啟信件	0	0	0%	0%
		點擊信件中之 URL 或開啟附檔	0			

廠商交付報告(5/7)

七、TOP10 點擊使用者及其次數

七月

名次	單位	姓名	email	點擊次數
1	總務處			17
2	台灣創意母體			7
3	管理學院			7
4	化工系			7
5	機械系			2
6	人事室			1
7	總務處			1
8	建築系			1
9	教務處			1
10	電機系			1

廠商交付報告(6/7)

十一、　附錄：各單位開啟及點擊清單

七月

人事室測試結果統計(102 年 07 月)

郵件帳號	姓名	職稱	連線方式	連線次數	開啟信件數
[redacted]	[redacted]	[redacted]	開啟信件	1	1
			點擊信件中之 URL 或開啟附檔	0	

化工系測試結果統計(102 年 07 月)

郵件帳號	姓名	職稱	連線方式	連線次數	開啟信件數
[redacted]	[redacted]	[redacted]	開啟信件	7	6
			點擊信件中之 URL 或開啟附檔	0	

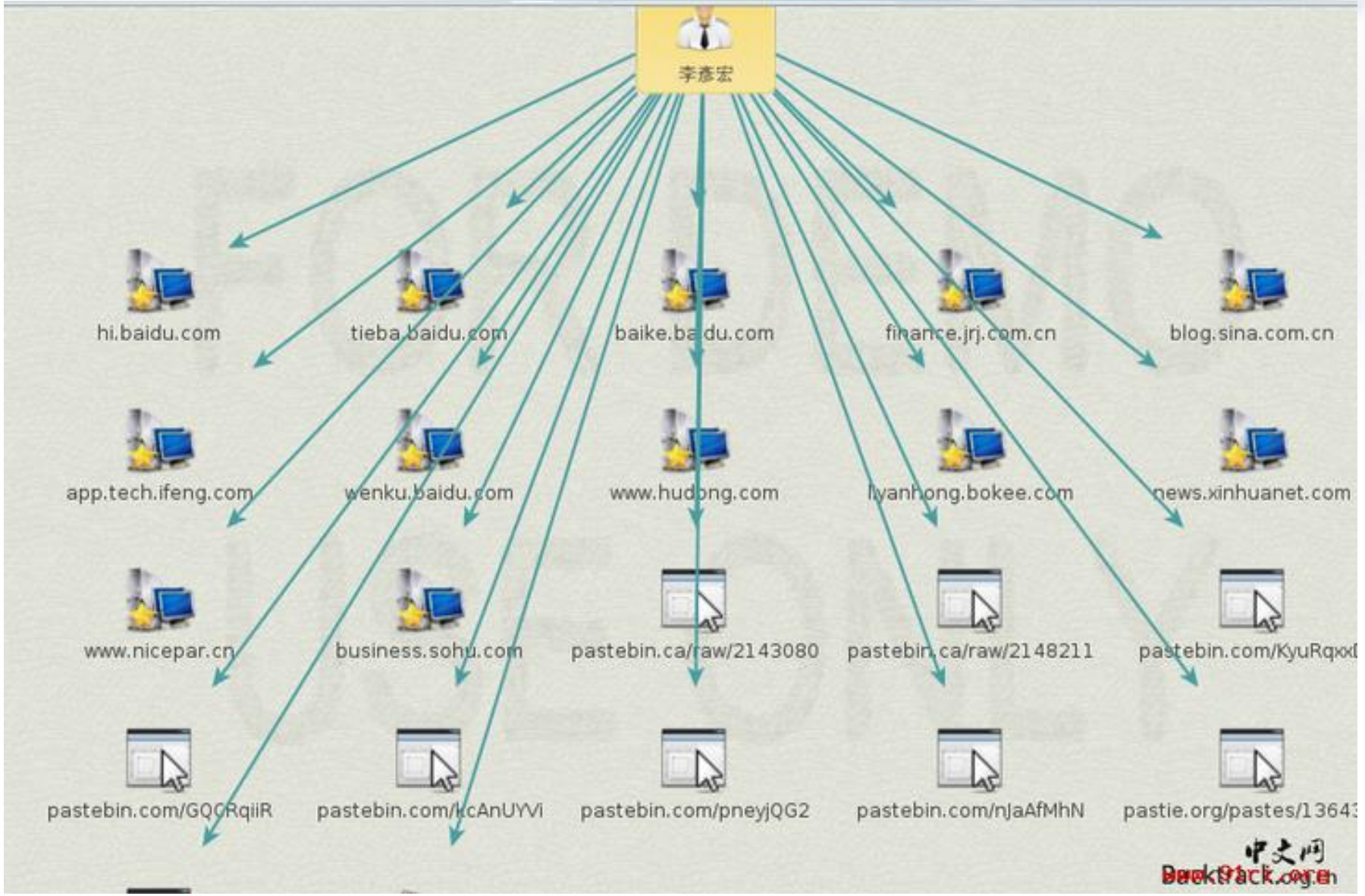
廠商交付報告(7/7)

十、建議改善方案

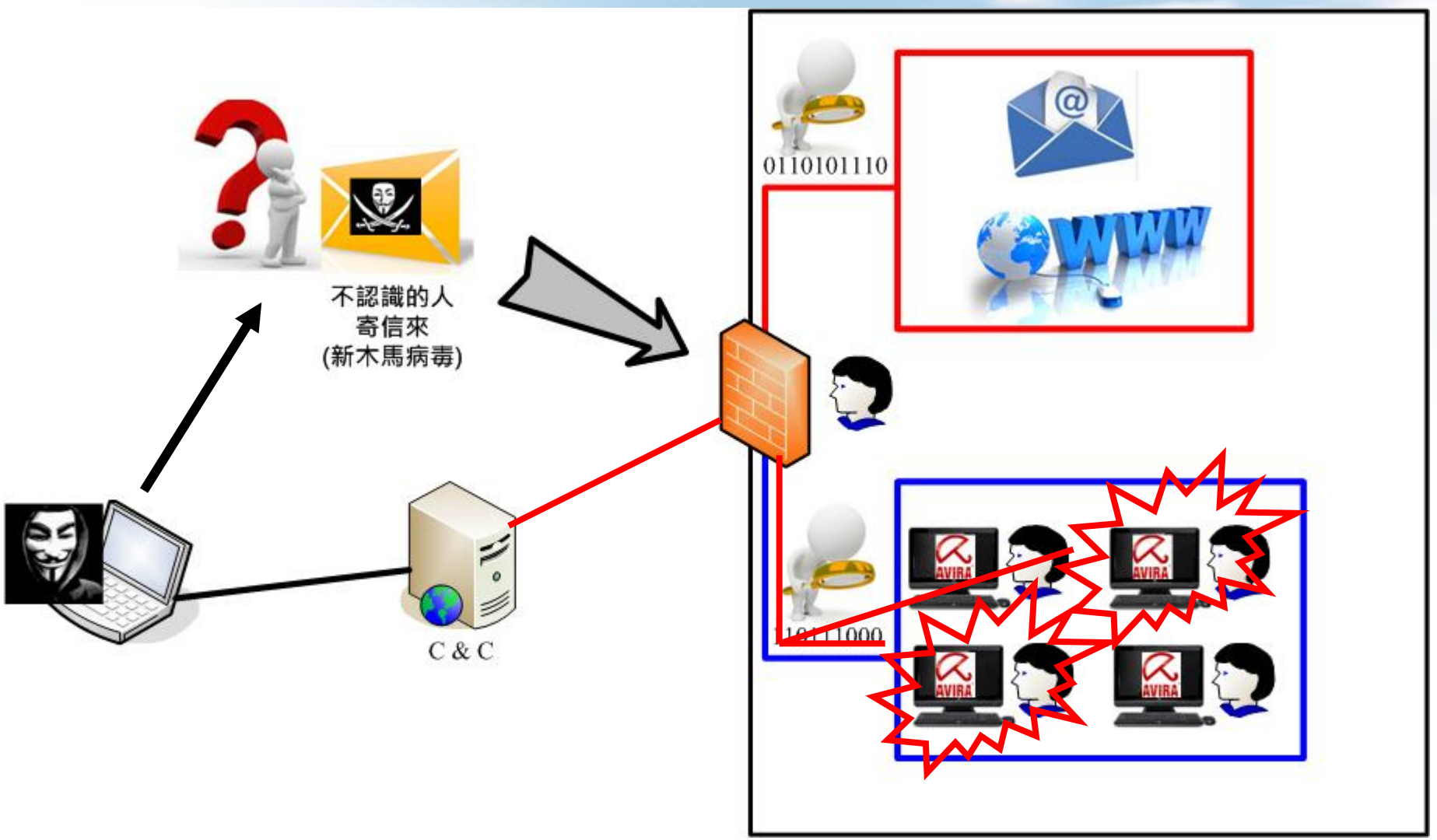
- 針對貴校本次演練結果
  - 七月份開啟信件比例：7.86%、有點擊信件中之 URL 或開啟附檔 人數比例：2.14%，已符合教育部演練標準(開啟信件比例須≦10%，點擊信件中之 URL 或開啟附檔比例須≦6%)。
  - 九月份開啟信件比例：9.29%、有點擊信件中之 URL 或開啟附檔 人數比例：2.14%，已符合教育部演練標準(開啟信件比例須≦10%，點擊信件中之 URL 或開啟附檔比例須≦6%)。
  - 整體開啟信件及點擊次數較前次 5 月份演練低(前次開啟信件比例 46.98%、有點擊信件中之 URL 或開啟附檔 人數比例：14.26%)，顯示貴校受測人員資安意識有顯著提升，但現階段常見之 APT 或社交工程釣魚攻擊仍有受駭之可能，仍建議可持續要求人員遵守資安規範，以人為本要求遵守組織內資安制度規範，循序漸進，以滿足符合教育部之規定演練標準。
  - **人員面：針對有點擊人員，仍建議採行以下防護措施建議，並提升人員資安防範意識，以防護 APT 攻擊，**並建議未來可選擇不同社交工程演練方式以不同樣本設計原理及檢測方式，交互測試，進一步提升人員防範意識。

何謂社交工程?

(補充)網路情報與偵察應用工具:Maltego



演練目的(測試單位人員收信時的警覺心，每半年1次)



入侵各階段:1.帳號蒐集階段

- 目的:找出目標帳號
- 方法:
  - 演練：客戶提供名單(部門、姓名、職稱、公務電郵)
  - 無名單則使用工具:theHarvester (Kali Linux)

    theharvester -d mail.npust.edu.tw -b all -l 300

    -d:目標網域

    -b:搜尋引擎

    -l:結果數目上限 (預設100)

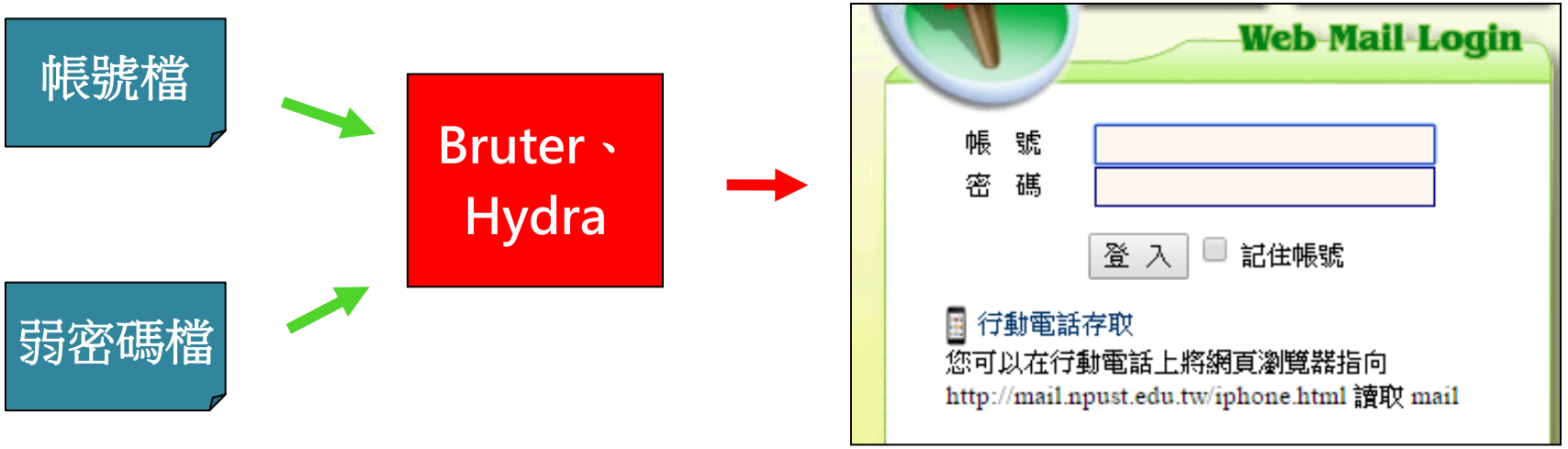
產出 電子郵件帳號檔案

產出 帳號檔案

入侵各階段:2.密碼試探階段

- 目的:找出具有弱密碼的帳號
  - 公開常用的密碼也屬於
    - 1qaz@WSX3edc
    - P@sw0rd
    - iphone6、2015...

- 方法:
  - Google查詢常用密碼,產出弱密碼檔案
  - 使用密碼暴力破解軟體:Bruter、Hydra



2014年 145個 弱密碼

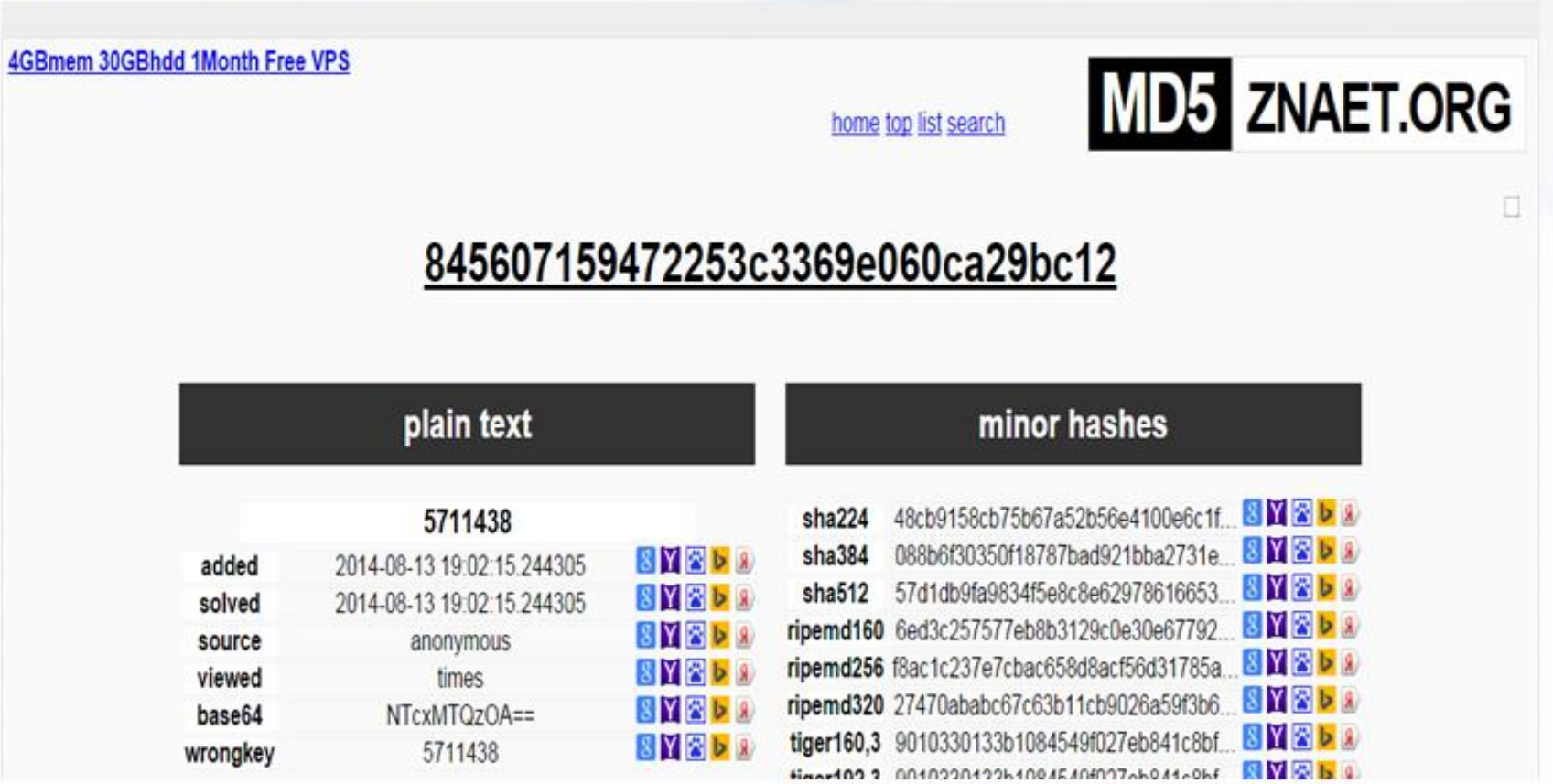
%username%	1234qwer	baseball	job	samsung
0	123qwe	bitch	jordan	secret
1111	1q2w3e	buster	jordan	sex
1234	1q2w3e4r	career	joshua	shadow
12345	1qaz@WSX	charlie	killer	snoopy1
102030	1qaz2wsx	chocolate	letmein	soccer
111111	2wsx3edc	computer	link	summer
112233	8uhb7ygv	connect	liverpool	sunshine
121212	aaaaaa	daniel	lkjhmnbv	superman
123123	abc	daniel	macromedia	test
123321	abc123	devil	maggie	test123
123456	abcd1234	dragon	master	the
123456	abcdef	dreamweaver	matrix	thomas
123654	admin	duck	michael	tigger
222222	administrator	eagles	michelle	toor
555555	adobe1	fdsa	monkey	trustno1
654321	adobe123	football	nicole	welcome
654321	adobeadobe	freedom	nimda	whatever
666666	alexander	fu*k	p@ssw0rd	work
753951	andrea	fuck	password	yankees
1234567	andrew	fuckyou	password1	zxcvbnm
1234567	andrew	ginger	pepper	
7777777	angel	god	photoshop	
9876543	asdasd	hannah	poiulkjh	
11111111	asdfasdf	ilove	princess	
12345678	asdfgh	iloveyou	purple	
123123123	asdfghj	internet	qazwsx	
123456789	asdfghjkl	jennifer	qwerty	
987654321	asdfzxcv	jennifer	qwertyuiop	
1234567890	azerty	jessica	root	
0okm9ijn	b*tch	jesus	root123	

加密後的數字,仍有破解風險

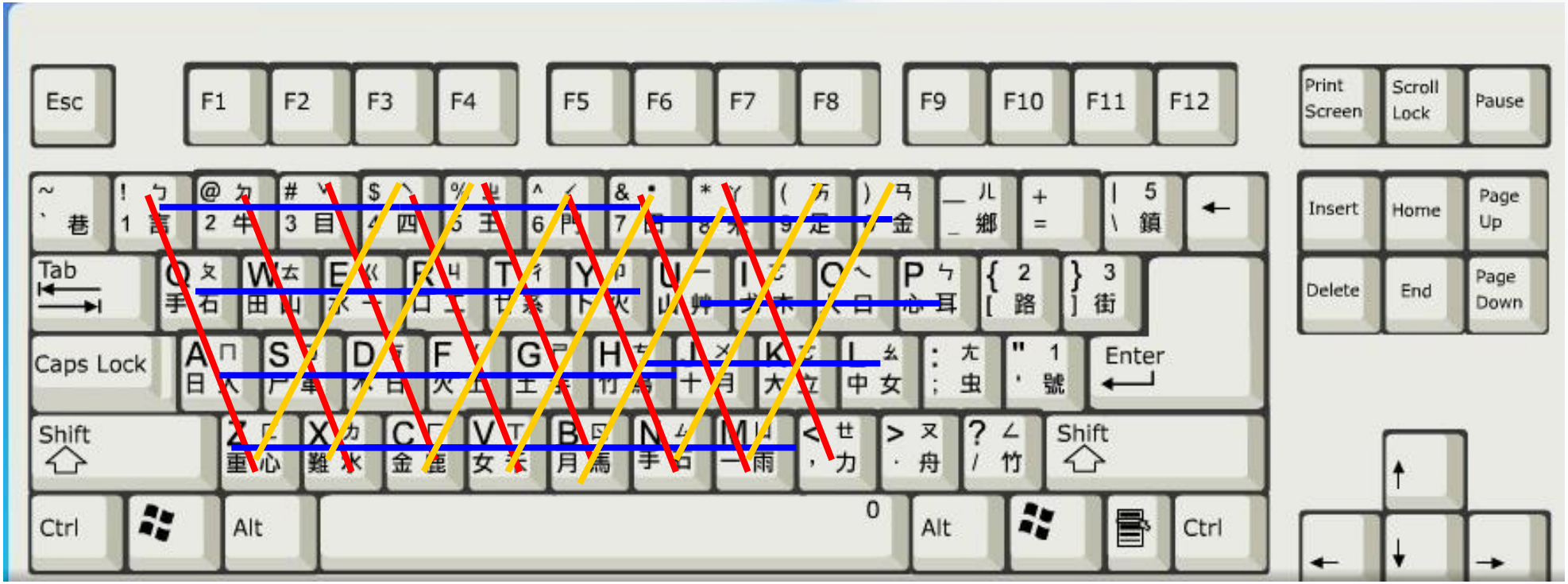
```
{

$m_pass=md5($_POST['system_pass']);
if($_POST['system_user']=="admin" && $m_pass=="845607159472253c3369e060ca29bc12")
{       $admin_check="ture";                }
```

斷裡面是否有符合的資料

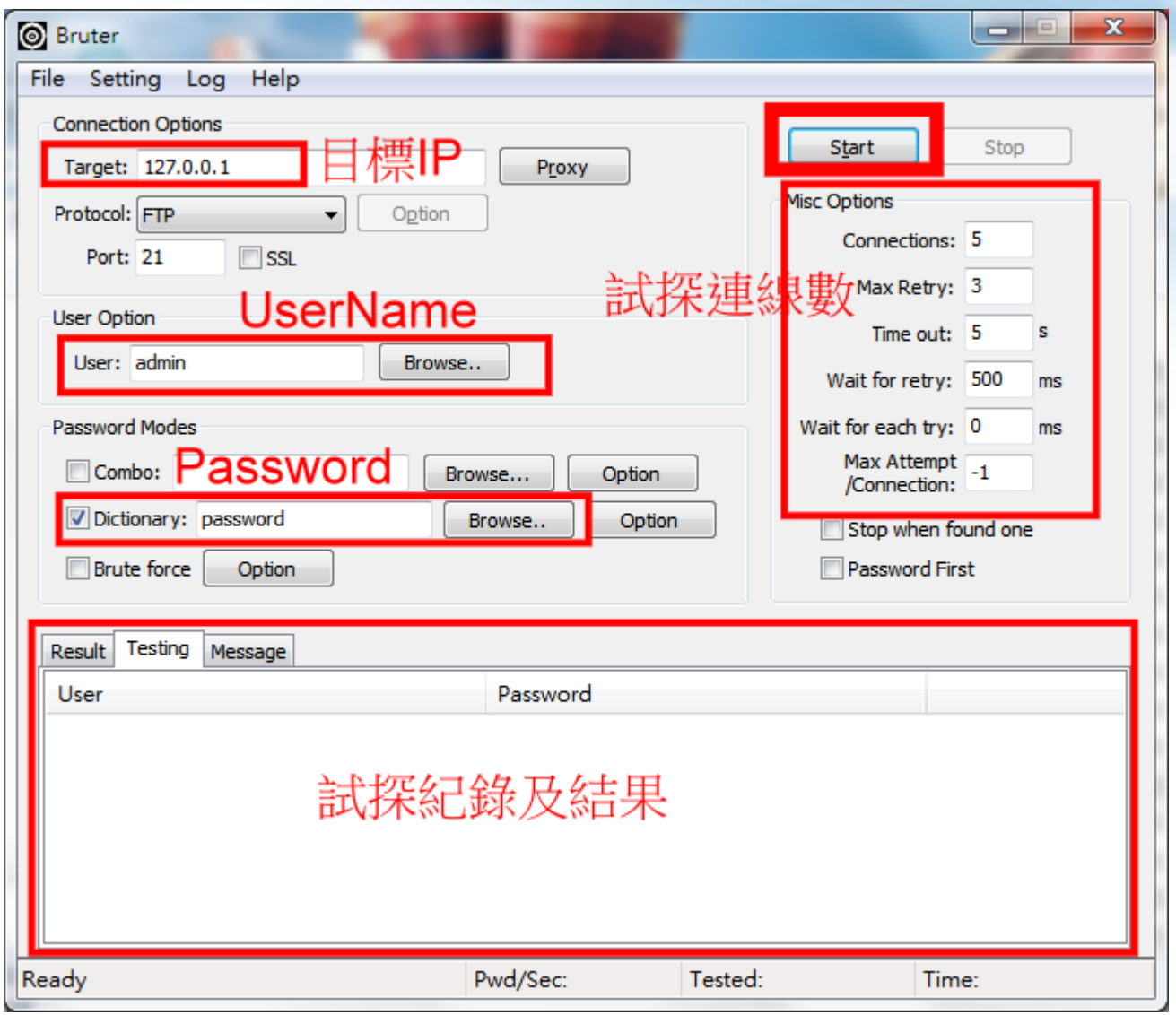
Google搜尋(密碼)845607159472253c3369e060ca29bc12
得到5711438明文

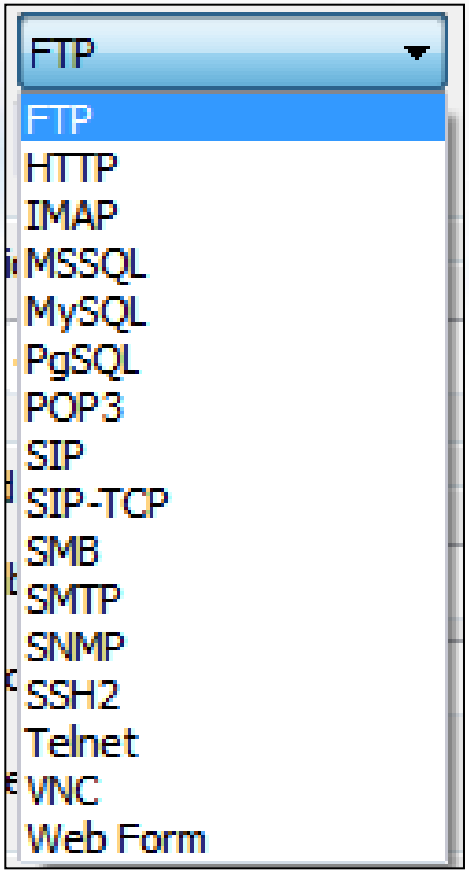


鍵盤按鍵順序的密碼,勿使用



(補充)Bruter畫面


Bruter
File Setting Log Help
Connection Options
Target: 127.0.0.1
目標IP
Proxy
Protocol: FTP
Option
Port: 21
SSL
User Option
UserName
User: admin
Browse..
Password Modes
Combo:
Password
Browse...
Option
Dictionary: password
Browse..
Option
Brute force
Option
Start
Stop
Misc Options
Connections: 5
試探連線數
Max Retry: 3
Time out: 5 s
Wait for retry: 500 ms
Wait for each try: 0 ms
Max Attempt /Connection: -1
Stop when found one
Password First
Result
Testing
Message
User
Password
試探紀錄及結果
Ready
Pwd/Sec:
Tested:
Time:


FTP
FTP
HTTP
IMAP
MSSQL
MySQL
PgSQL
POP3
SIP
SIP-TCP
SMB
SMTP
SNMP
SSH2
Telnet
VNC
Web Form

入侵各階段:3.誘騙階段

- **目的:製作吸引點閱的郵件內容，且不被懷疑是廣告郵件**
- **方法:**
  - **郵件內容:**依各年齡層、各類主題及結合時事來製作
    - 美女、美容、健康養生、財經、時事、科技、生活、旅遊、知識...等類
  - **寄送方式:**10日內分散寄送5封,每人收到信件的時間與順序不同
    - 寄件人隨機多組來配置
      - 小可<news123@msn.com>
      - 怡君<gigacircle@msn.com>
      - Gaston_Wang<Gaston@gmail.com>
      - 東森新聞雲<ettoday@gmail.com>

      ……

國外媒體曝光iPhone 6超薄概念機 - 郵件 (HTML)

寄件者: 卡堤諾 <ck101@gmail.com>
寄件日期: 2014/1/22 (週三) 上午 10:13
收件者: [redacted]
副本:
主旨: 國外媒體曝光iPhone 6超薄概念機

訊息 iPhone 6超薄概念機.doc (35 KB)

國外媒體曝光 iPhone 6 超薄概念機

去年蘋果秋季新品發佈會上 iPad Air 如約而至，全新的命名方式令人喜出望外，首次出現 Macbook Air 之外的 Air 設備。

而之前國外媒體就曝光了有關 iPhone Air 的設計概念圖。從它的設計思路中我們可以看到薄如刀片的 iPhone 6。

iPhone Air 的設計除了超薄之外還首次加入了無邊框大屏設計。整個機身外形採用了一種水滴設計樣式，顯得非常的輕薄。

同時 Home 鍵部位繼承了 iPhone5s 的指紋識別技術，具備指紋掃瞄功能，同時 Nano Sim 卡的位置被移到了機身左側的下方。

而機身採用的是全金屬材質，配備的是 5 英吋的無邊框螢幕，解析度達到 2K 級別。

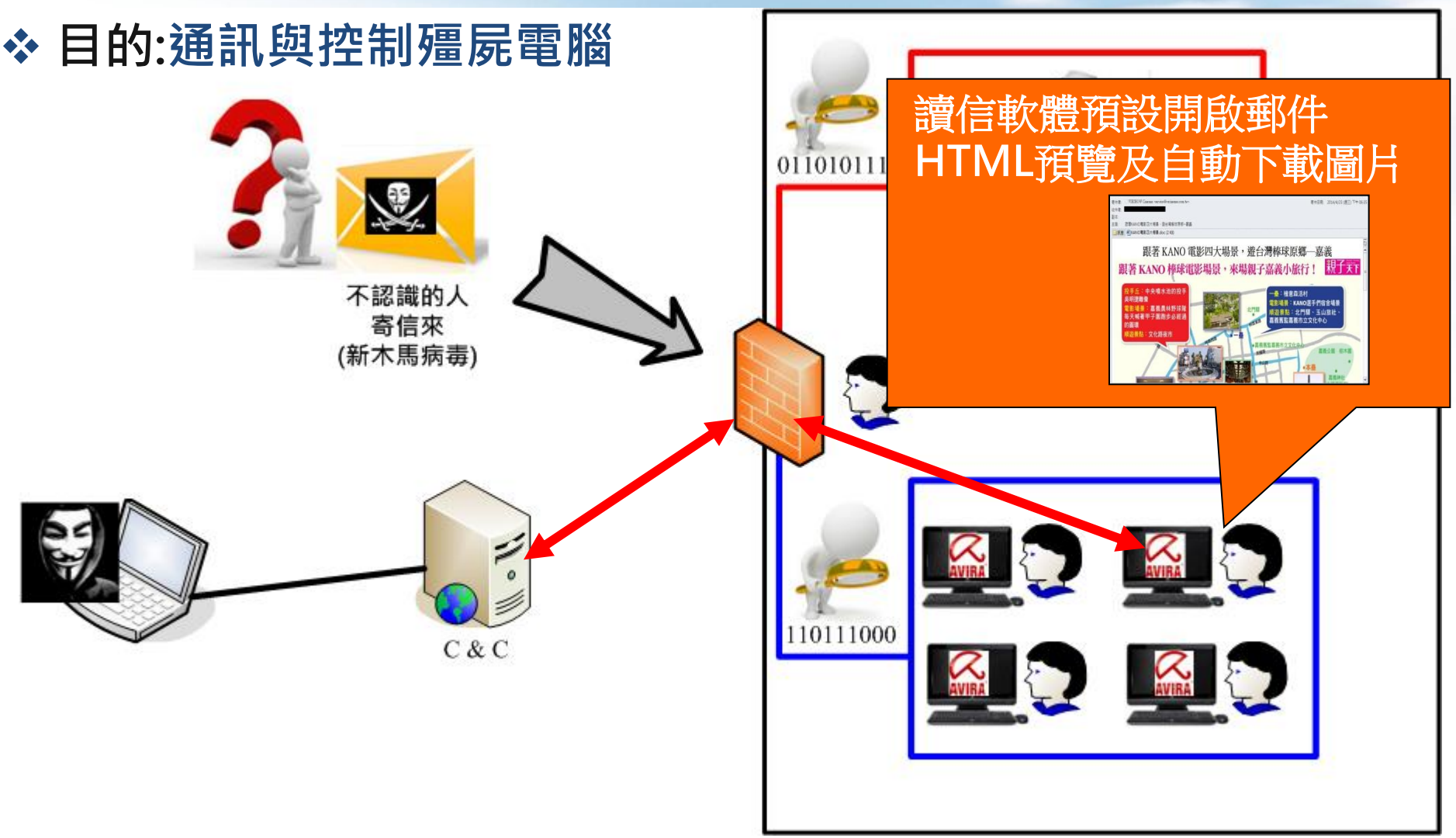
更多 iPhone 6 介紹影片

卡堤諾

下午 02:11
2014/1/24

入侵各階段:4.資訊蒐集階段

- 目的:通訊與控制殭屍電腦



(補充)報到畫面

A	B	C	D	E	F	G	H	I
電子郵件帳號	單位名稱	單位名稱2	職稱	姓名	測試名稱	點選開啟時間	動作名稱	IP Address
c	公所				有無eTag收費方式懶人包	2014/4/28 11:33	開啟信件	1
v	處				讓熱量消耗快一點！5大招擁有	2014/4/28 11:47	開啟信件	6
r	處				讓熱量消耗快一點！5大招擁有	2014/4/28 13:57	開啟附檔	2
p	處				好文分享-兩岸服貿協議真的「	2014/4/28 14:40	開啟附檔	2
p	處				好文分享-兩岸服貿協議真的「	2014/4/28 14:41	開啟附檔	2
d	處				好文分享-兩岸服貿協議真的「	2014/4/28 14:50	開啟附檔	2
fl	局				有無eTag收費方式懶人包	2014/4/28 14:58	開啟信件	6
e	處				跟著KANO電影四大場景，遊台	2014/4/28 15:37	開啟附檔	2
n	處				讓熱量消耗快一點！5大招擁有	2014/4/28 17:18	開啟信件	1
n	處				讓熱量消耗快一點！5大招擁有	2014/4/28 17:18	開啟附檔	1
j(	處				有無eTag收費方式懶人包	2014/4/29 01:23	開啟信件	1
p	局				跟著KANO電影四大場景，遊台	2014/4/29 08:31	開啟信件	2
d	處				讓熱量消耗快一點！5大招擁有	2014/4/30 14:54	開啟附檔	1
c	處				讓熱量消耗快一點！5大招擁有	2014/4/30 18:03	開啟附檔	2
c	處				讓熱量消耗快一點！5大招擁有	2014/4/30 18:04	開啟附檔	2

微軟Outlook郵件預設(不安全)

寄件者: 熊大 <bearbig98@gmail.com>
收件者: [redacted]
副本:
主旨: 國外媒體曝光iPhone 6超薄概念機
訊息 | iPhone 6超薄概念機.doc (1 KB)

附件預覽開啟

國外媒體曝光 iPhone 6 超薄概念機

去年蘋果秋季新品發佈會上 iPad Air 如約而至，全新的命名方式令人喜出望外，首次出現 Macbook Air 之外的 Air 設備。

而之前國外媒體就曝光了有關 iPhone Air 的設計概念圖。從它的設計思路中我們可以看到薄如刀片的 iPhone 6。

iPhone Air 的設計除了超薄之外還首次加入了無邊框大屏設計。整個機身外形採用了一種水滴設計樣式，顯得非常的輕薄。

同時 Home 鍵部位繼承了 iPhone5s 的指紋識別技術，具備指紋掃瞄功能，同時 Nano Sim 卡的位置被移到了機身左側的下方。

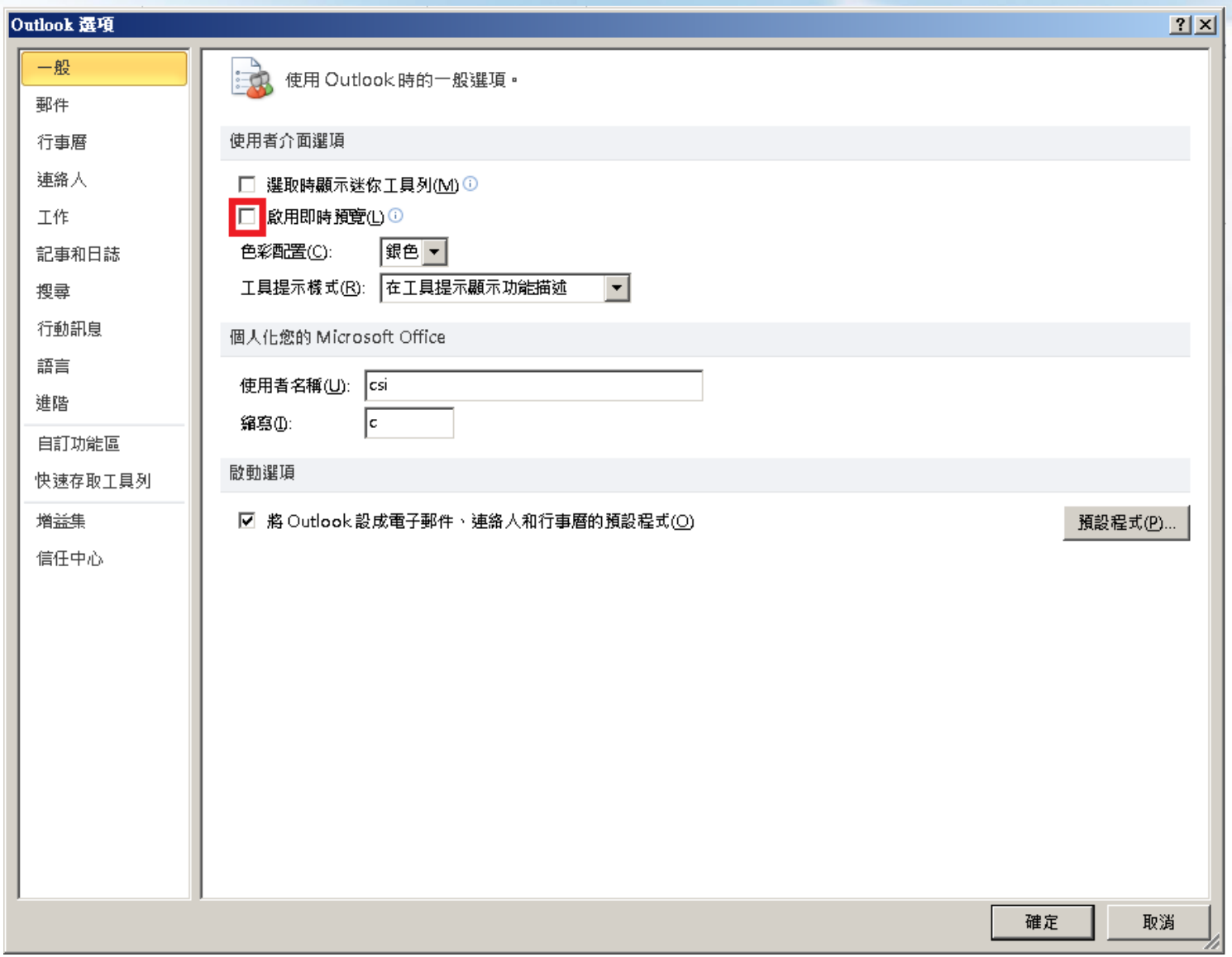
而機身採用的是全金屬材質，配備的是 5 英吋的無邊框螢幕，解析度達到 2K 級別。

更多 iPhone 6 介紹影片

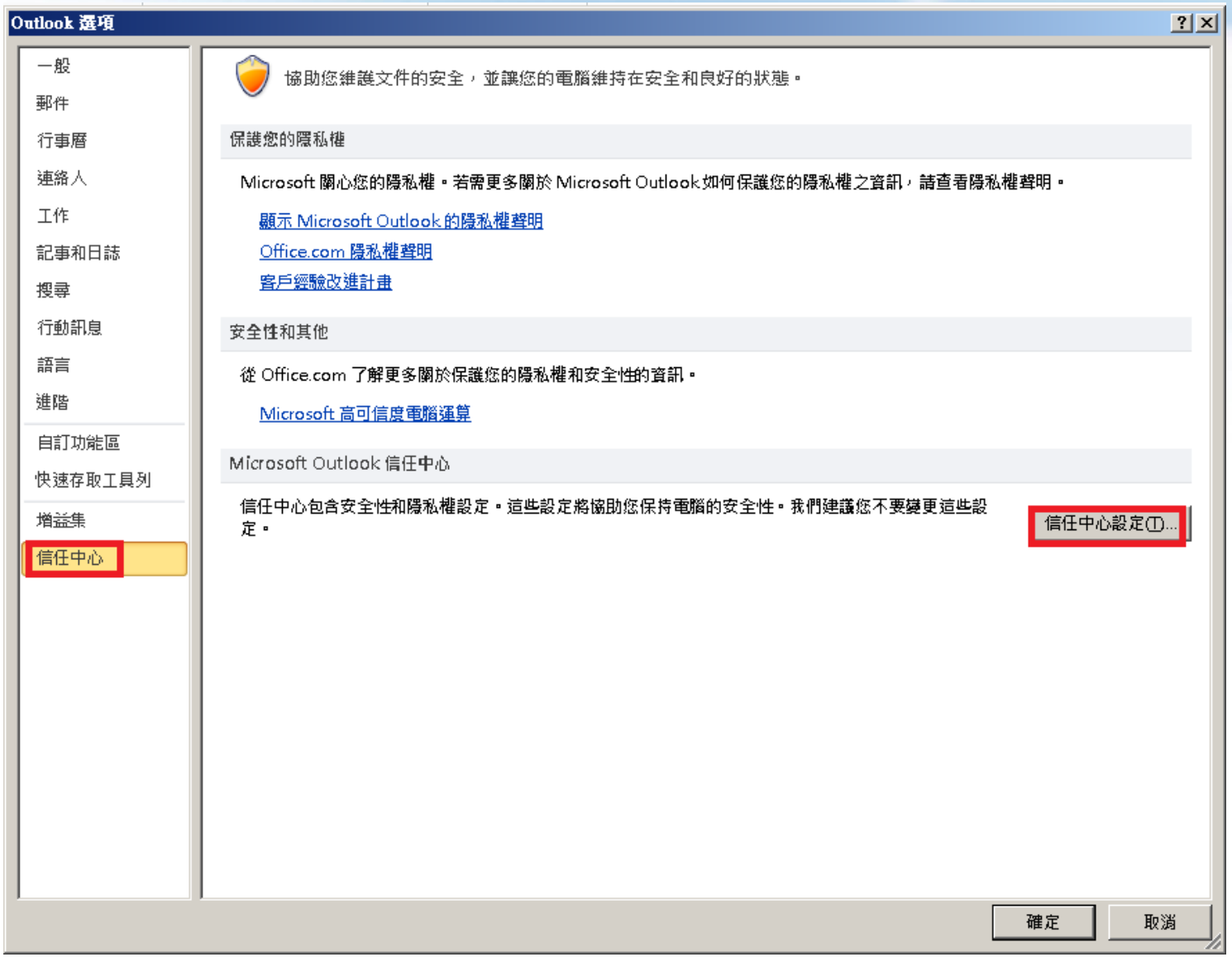
以html格式呈現

自動下載及顯示圖片

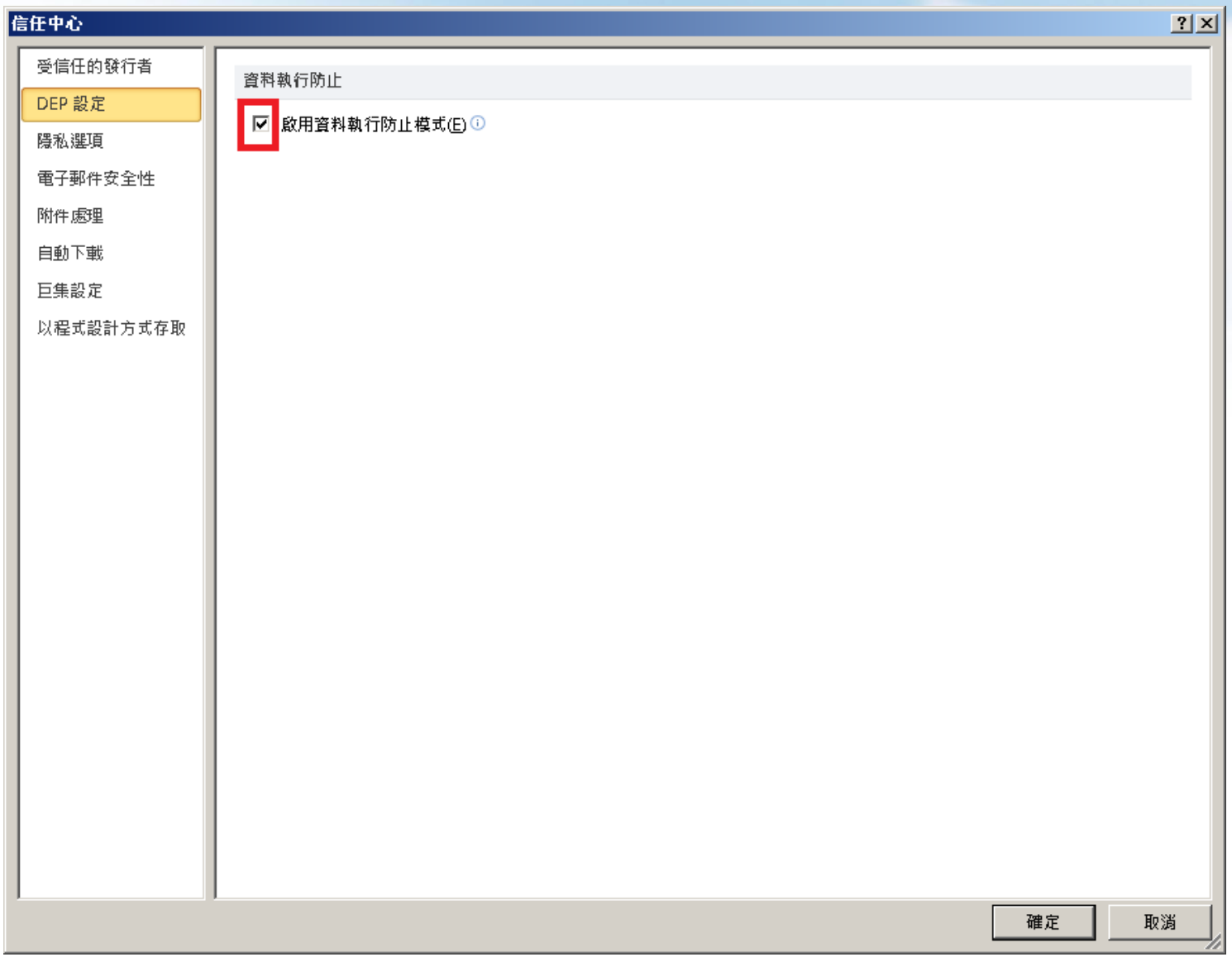
防制作法:關閉自動化預覽(Outlook) (1/7)



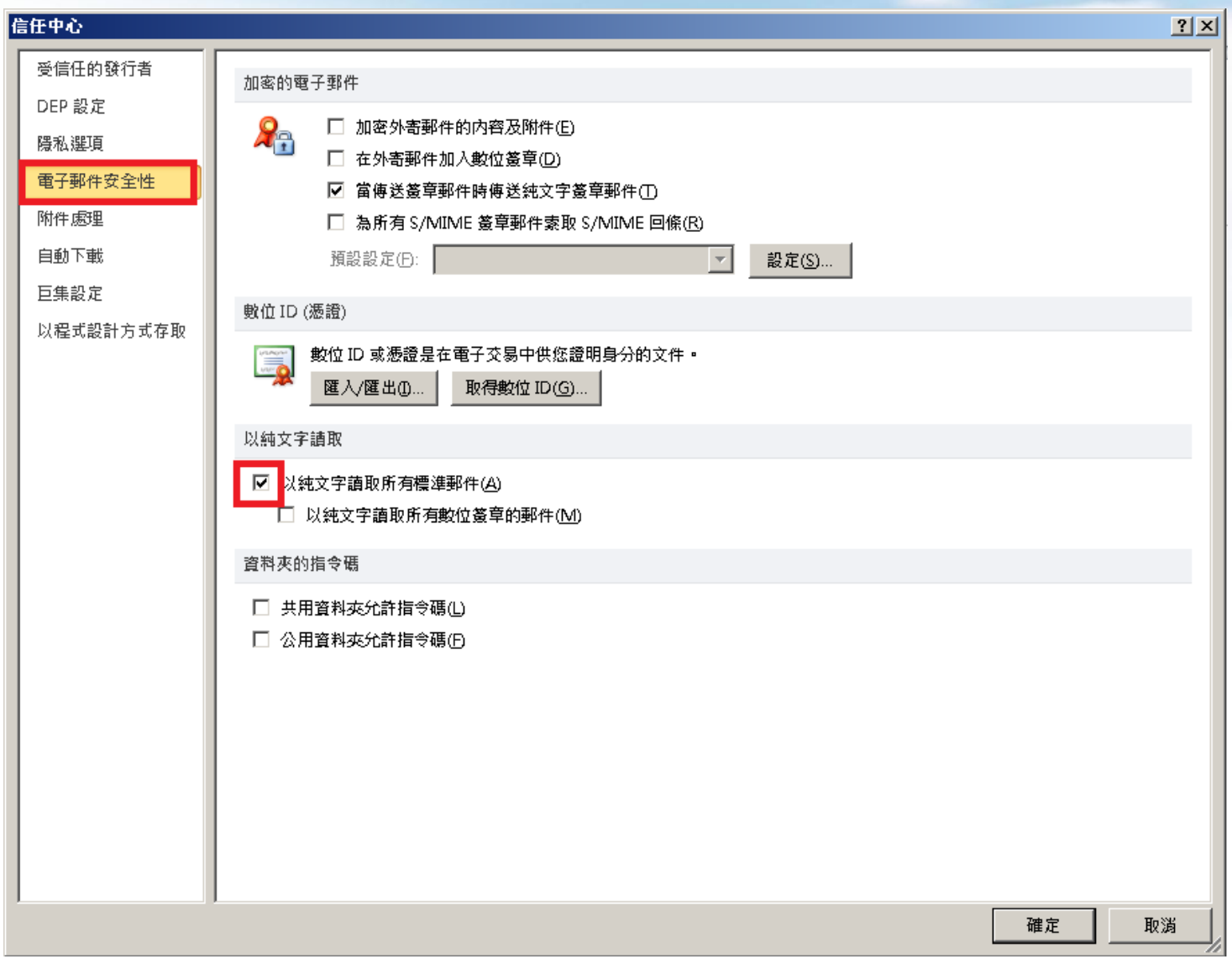
防制作法:關閉自動化預覽(Outlook) (2/7)



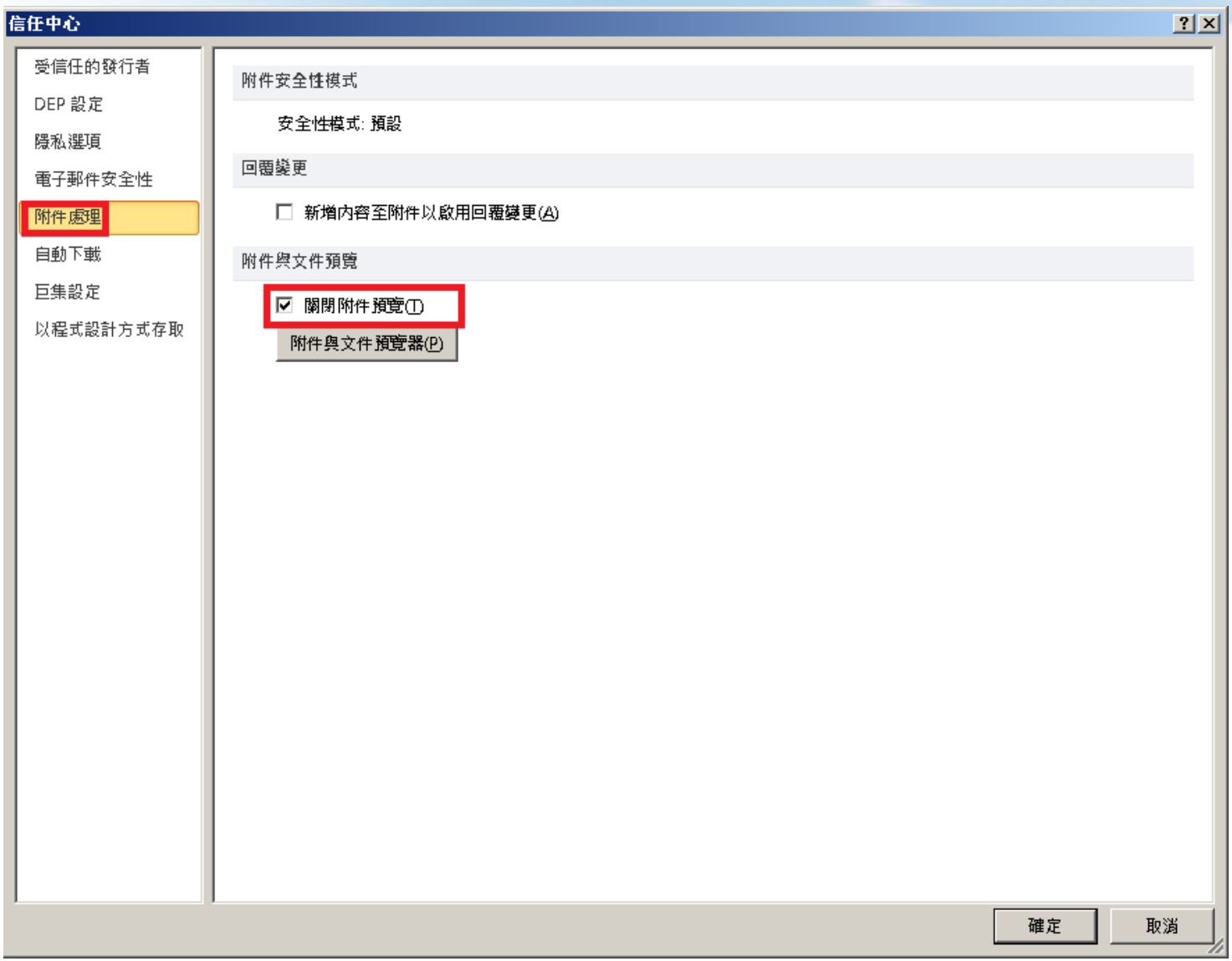
防制作法:關閉自動化預覽(Outlook) (3/7)



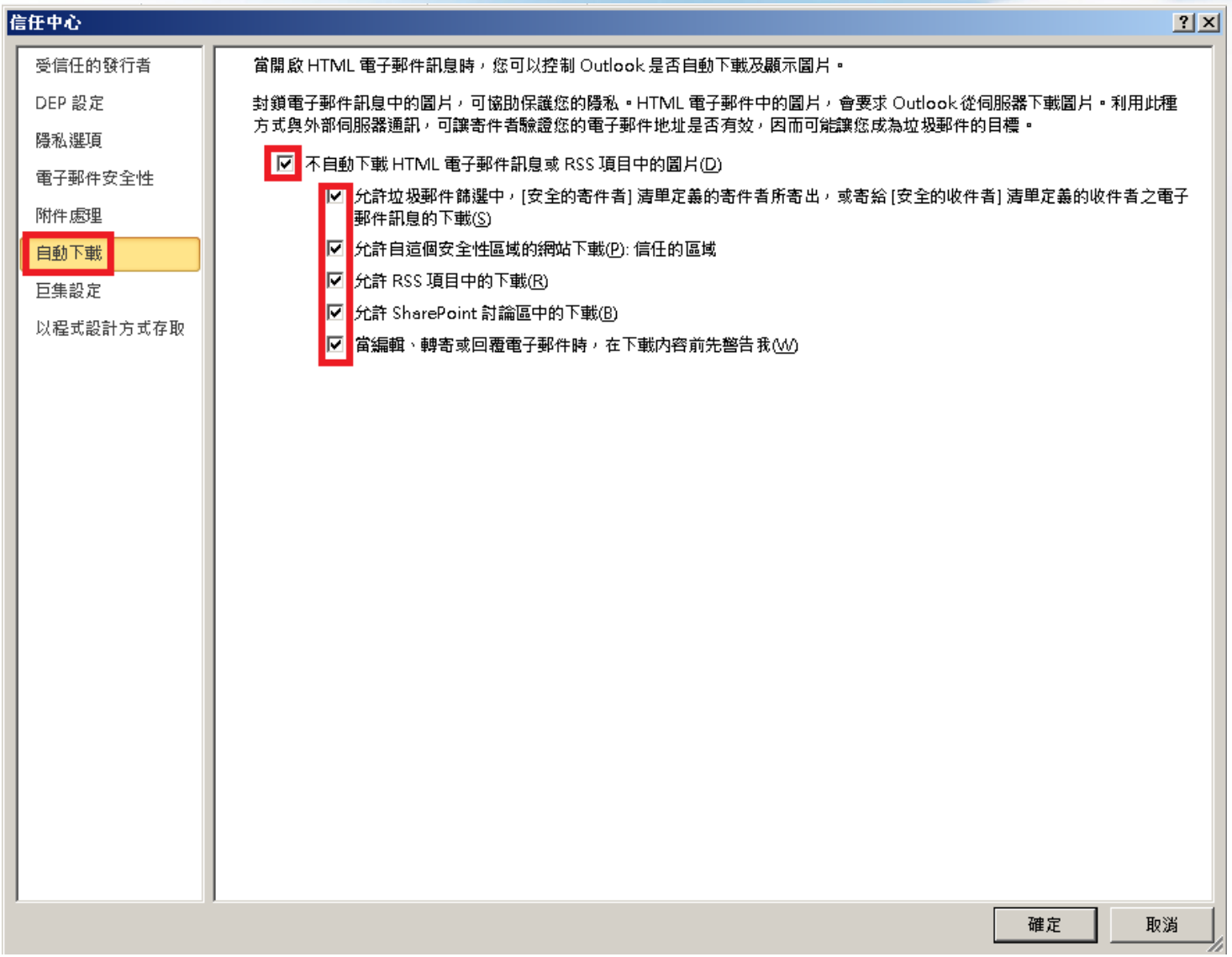
防制作法:關閉自動化預覽(Outlook) (4/7)



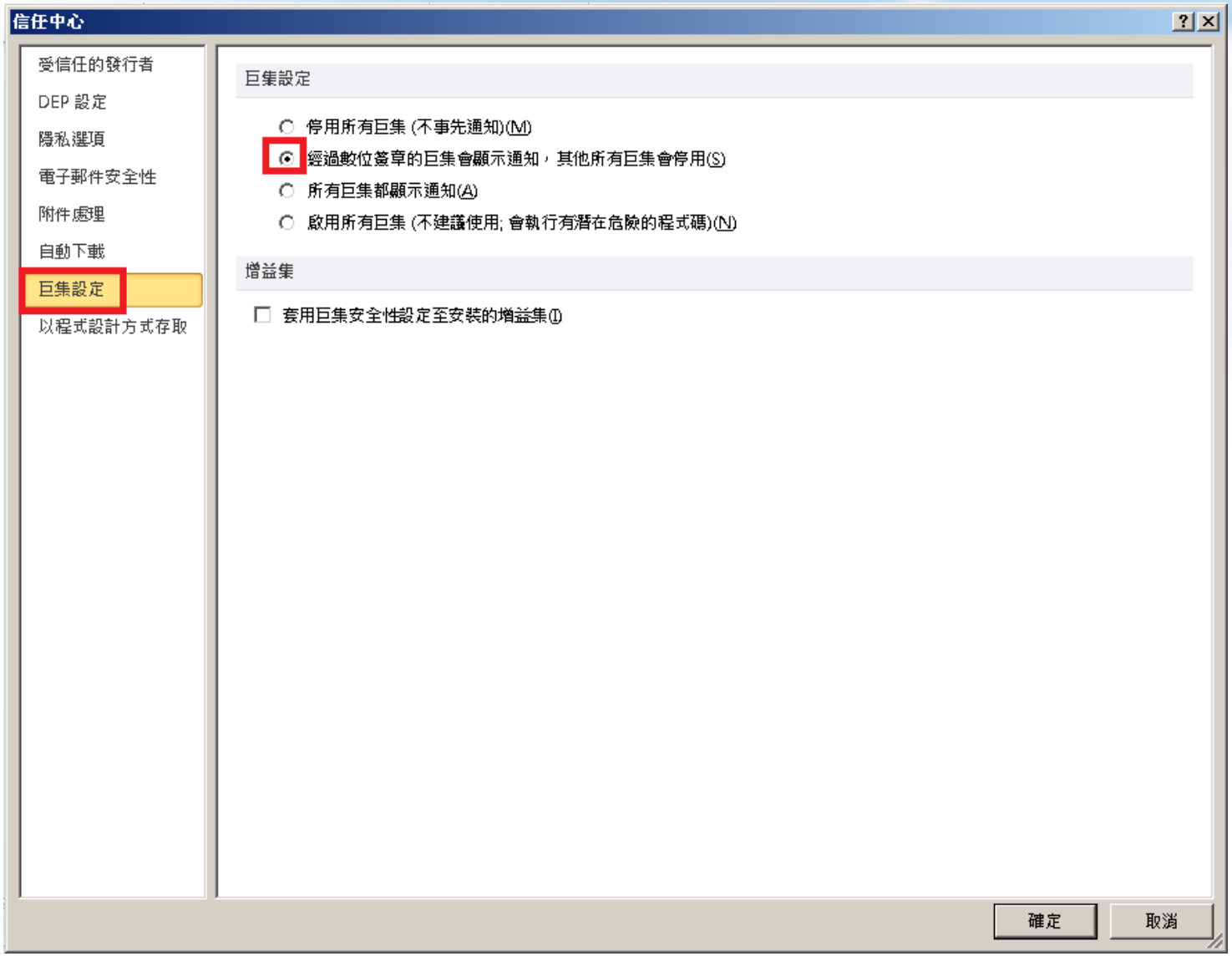
防制作法:關閉自動化預覽(Outlook) (5/7)



防制作法:關閉自動化預覽(Outlook) (6/7)



防制作法:關閉自動化預覽(Outlook) (7/7)



人工方式警覺性判斷:微軟Outlook 純文字預覽

原形畢露

此郵件已轉換為純文字。

寄件者: 熊大 <bearbig98@gmail.com>

收件者: [redacted]

副本:

主旨: 國外媒體曝光iPhone 6超薄概念機

附件: iPhone 6超薄概念機.doc (1 KB)

人:他是誰?這電郵不屬於我認識的人.

國外媒體曝光 iPhone 6 超薄概念機

事、時:內容跟我近期工作沒關係.

去年蘋果秋季新品發佈會上 iPad Air 如約而至，全新的命名方式令人喜出望外，首次出現 Macbook Air 之外的 Air 設備。

而之前國外媒體就曝光了有關 iPhone Air 的設計概念圖。從它的設計思路中我們可以看到薄如刀片的 iPhone 6。

iPhone Air 的設計除了超薄之外還首次加入了無邊框大屏設計。整個機身外形採用了一種水滴設計樣式，顯得非常的輕薄。

同時 Home 鍵部位繼承了 iPhone5s 的指紋識別技術，具備指紋掃瞄功能，同時 Nano Sim 卡的位置被移到了機身左側的下方。

而機身採用的是全金屬材質，配備的是 5 英吋的無邊框螢幕，解析度達到 2K 級別。

地:為何會連到其他網站?

更多 iPhone 6 介紹影片 <http://technology.hinet.net/TestClick.php?code=0b1e74949948283b6d1b593b2a712965&type=504>

<http://tw.news.yahoo.com/%E7%BE%8E%E7%A0%94%E7%99%BC%E8%90%AC%E8%83%BD%E6%A9%9F%E5%99%A8%E4%BA%BA-%E5%A4%96%EE8%80%85-094600502.html>

<http://technology.hinet.net/image/tmp504.jpg>

<http://tw.news.yahoo.com/%E7%BE%8E%E7%A0%94%E7%99%BC%E8%90%AC%E8%83%BD%E6%A9%9F%E5%99%A8%E4%BA%BA-%E5%A4%96%EE8%80%85-094600502.html>

Mail 2000郵件預設(不安全)

(4) 欲讀取信件，在信件列表中點選欲讀取的信件標題，點選一下可預覽信件內文，快速點選兩下則可開啟信件內文於新視窗。

- 切換純文字與 HTML

為降低惡意信件的風險，使用者可至個人化設定中，將預設讀信方式設為「純文字」，確定安全後再點選 HTML 頁簽檢視豐富的圖文內容。

防制作法:安全預覽設定(1/2) (Mail 2000)

在「使用環境」中，提供五大項設定：

(1) **一般**

- 語言：可依習慣設介面語言。
- 信件資訊顯示模式：設定閱讀信件時，預設顯示資訊。
- 登入顯示頁面：設定登入顯示頁面。
- 連線失效時間：設定多久未動作後自動登出。
- 時區：設定您所在地的時區。

(2) **郵件**

- 讀信模式：可依習慣選擇讀信模式，有上下分割、左右分割、整頁模式。
- 信件自動預覽：選擇是否於進入收信匣或其他信件匣時，自動預覽信件。
- 去除Javascript：讀信時除去信件內的Javascript，降低惡意信件的危害。
- 預設讀信方式：預設以 HTML或純文字方式閱讀信件內容。
- 封鎖外部圖檔：設定讀信時是否封鎖信件內的外部圖檔，避免可能造成的安全上顧慮。
- 本系統提供三種封鎖方式與封鎖條件：
  - 全部封鎖：本系統會為您封鎖全部信件匣的圖片。
  - 只封鎖廣告信匣：本系統只為您封鎖在廣告信匣裡的圖片，其他信匣不封鎖。
  - 不封鎖：本系統不會為您封鎖任何信匣中的任何圖片。
  - 已讀信件不封鎖：本系統將不封鎖您已讀取之信件的圖片。

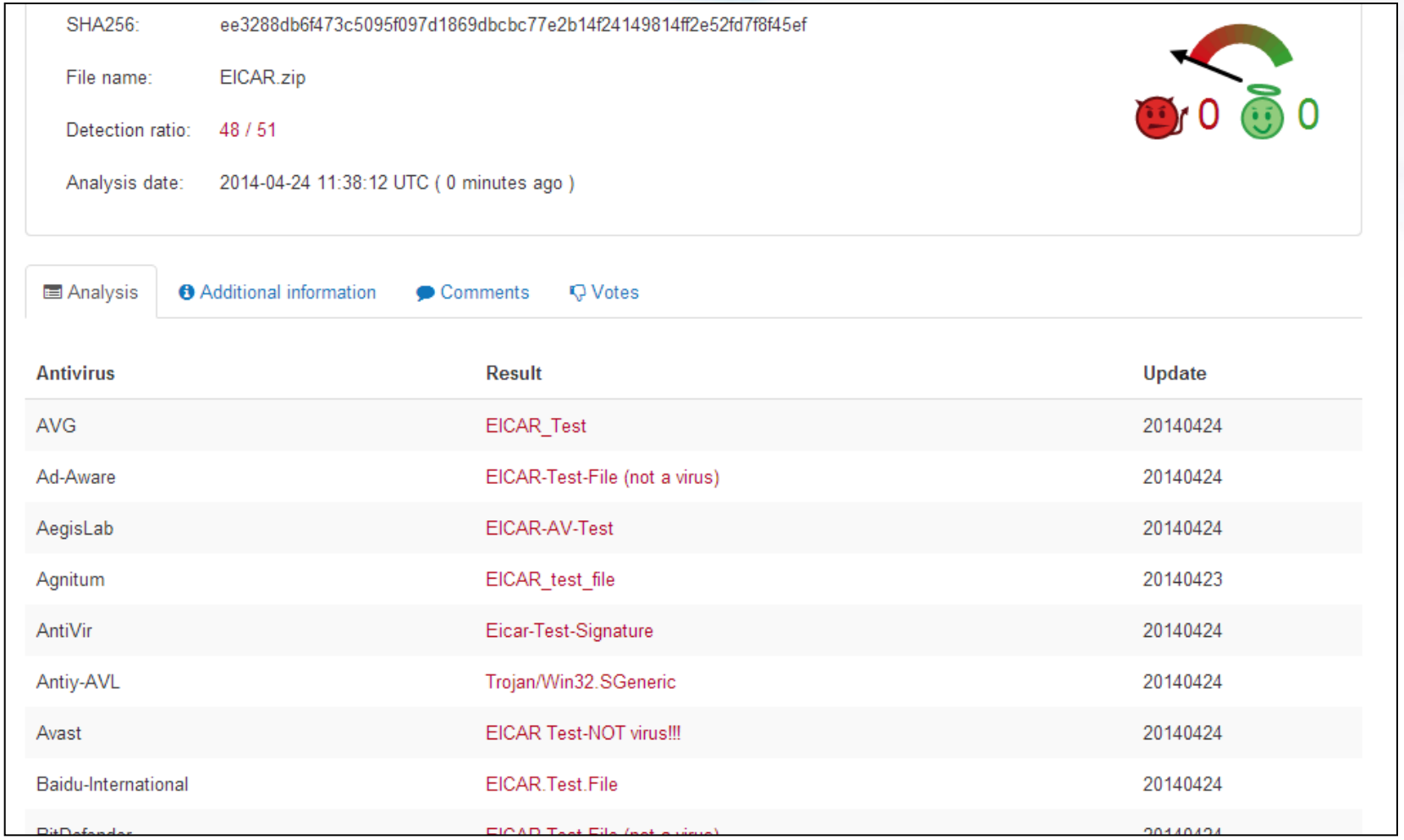
防制作法:安全預覽設定(2/2) ((Mail 2000)

附檔安全檢查1:VirusTotal 免費掃毒網站(1/2)

- https://www.virustotal.com/

附檔安全檢查1:VirusTotal 免費掃毒網站 (2/2)

- https://www.virustotal.com/



SHA256: ee3288db6f473c5095f097d1869dbcbc77e2b14f24149814ff2e52fd7f8f45ef

File name: EICAR.zip

Detection ratio: 48 / 51

Analysis date: 2014-04-24 11:38:12 UTC (0 minutes ago)

0 0

Analysis | Additional information | Comments | Votes

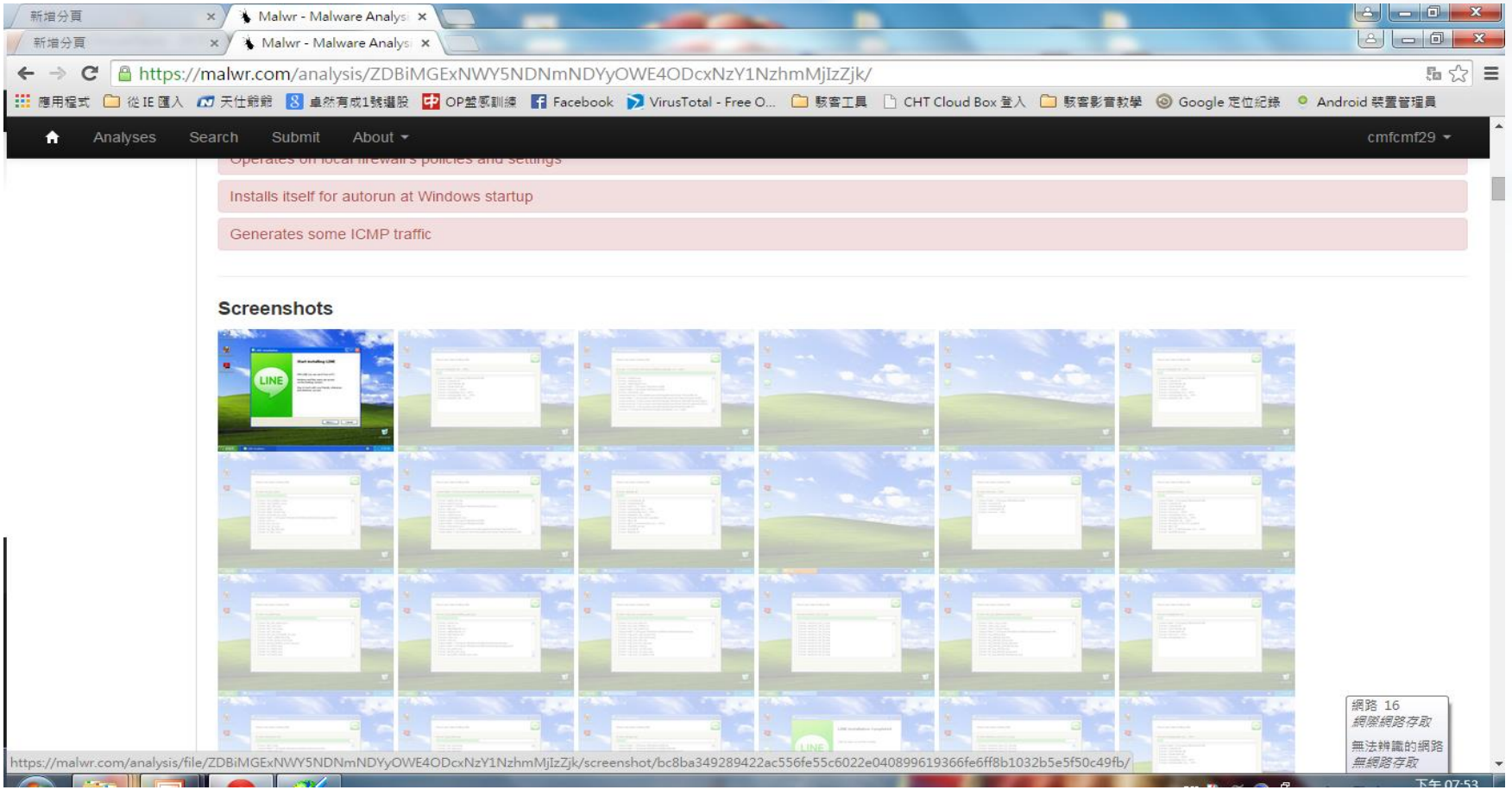
Antivirus	Result	Update
AVG	EICAR_Test	20140424
Ad-Aware	EICAR-Test-File (not a virus)	20140424
AegisLab	EICAR-AV-Test	20140424
Agnitum	EICAR_test_file	20140423
AntiVir	Eicar-Test-Signature	20140424
Antiy-AVL	Trojan/Win32.SGeneric	20140424
Avast	EICAR Test-NOT virus!!!	20140424
Baidu-International	EICAR.Test.File	20140424

附檔安全檢查2:雲端沙箱

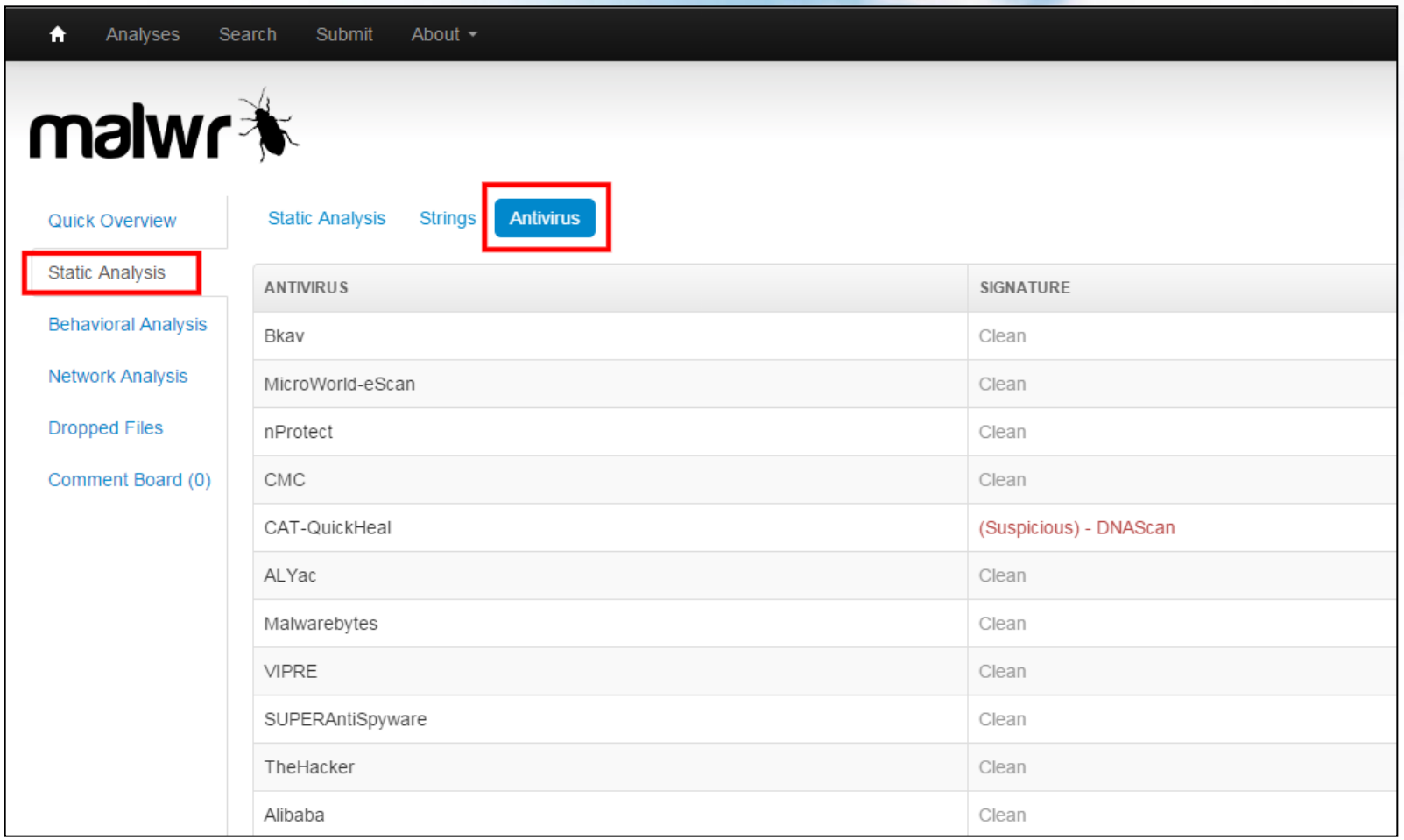
- https://malwr.com/

Line安裝程式 malwr分析(1/2)

- https://malwr.com/analysis/ZDBiMGExNWY5NDNmNDYyOWE4ODcxNzY1NzhmMjIzZjk/



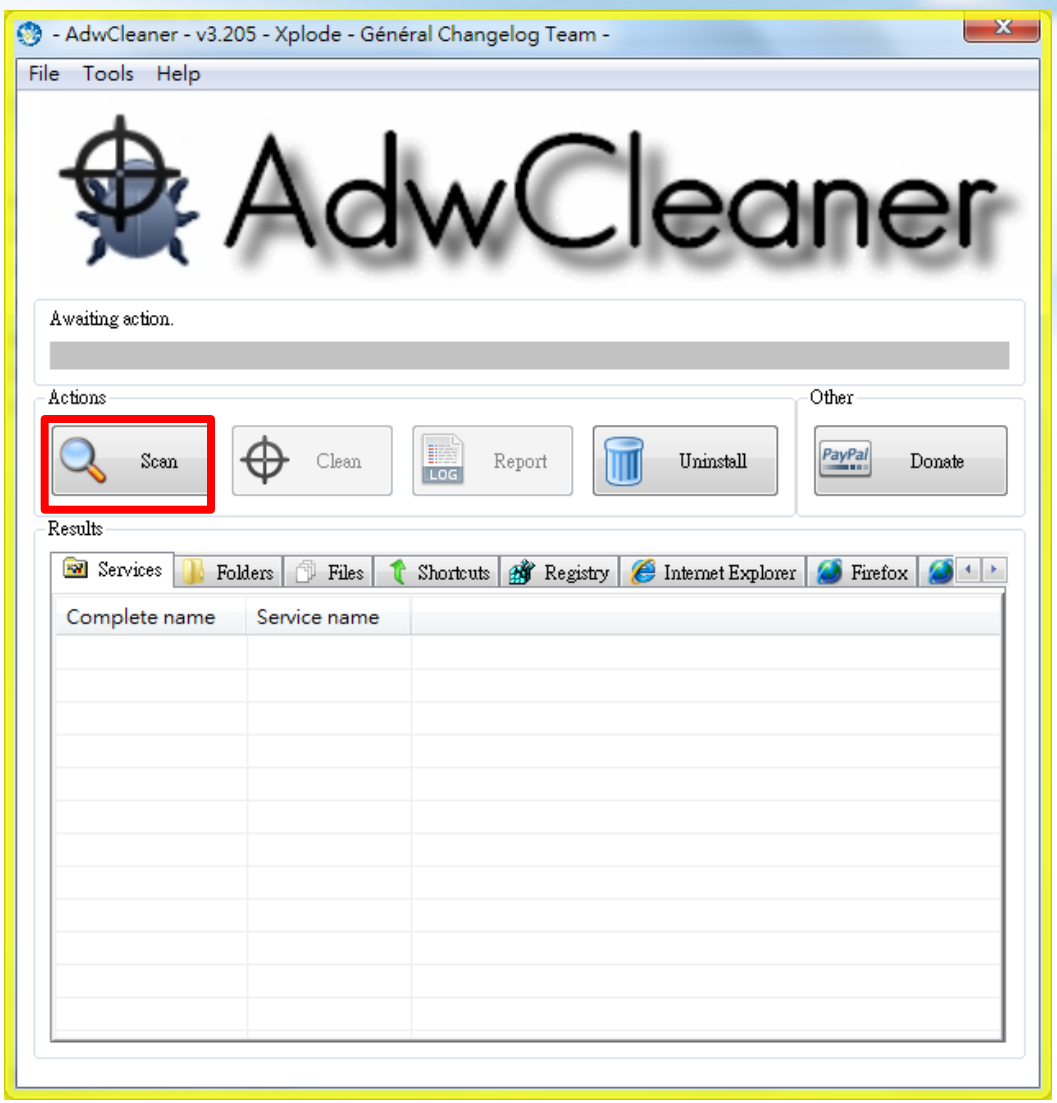
Line安裝程式 malwr分析 (2/2)



adwcleaner.exe首頁綁架移除程式(1/9)

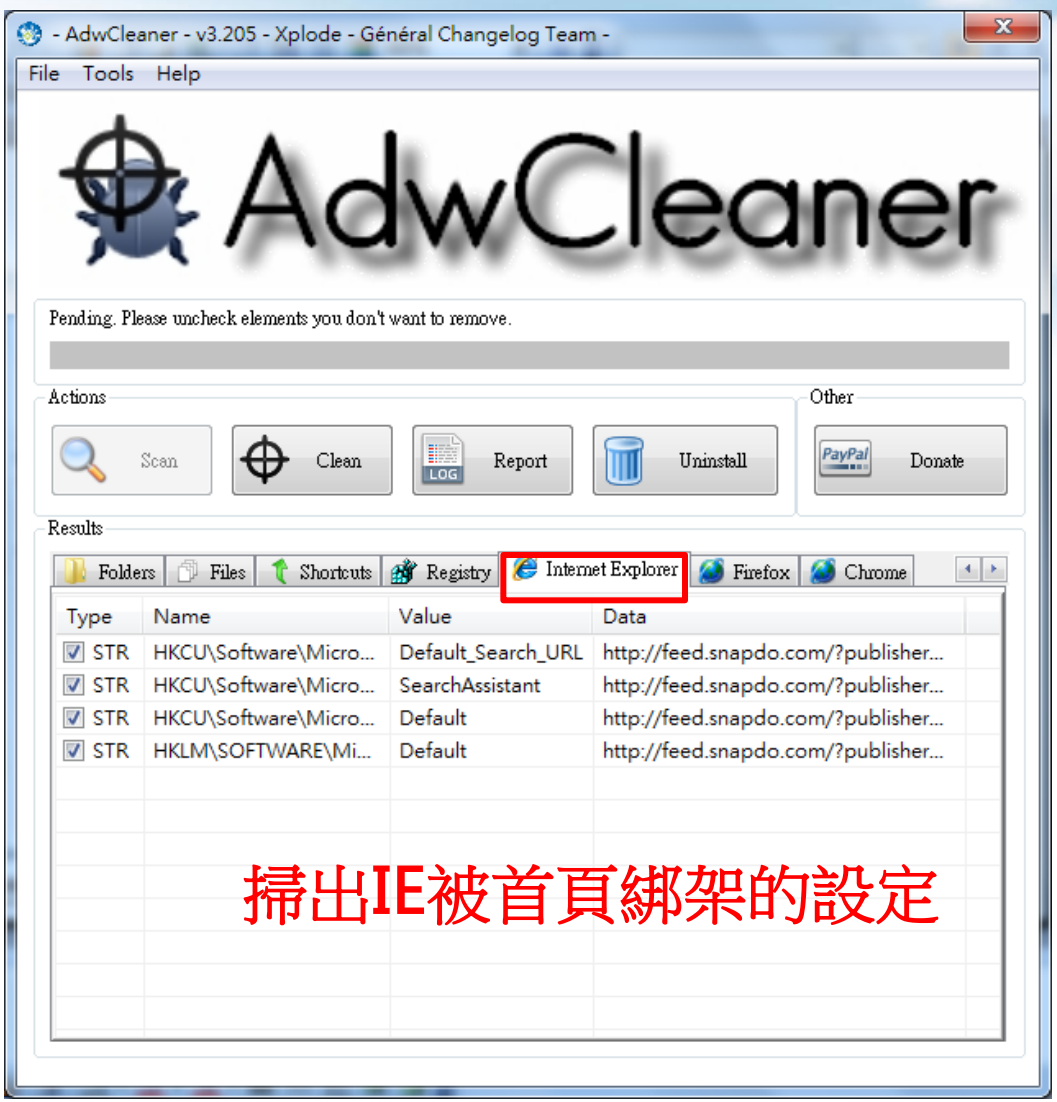
請用
系統管理員
權限來執行

點選Scan

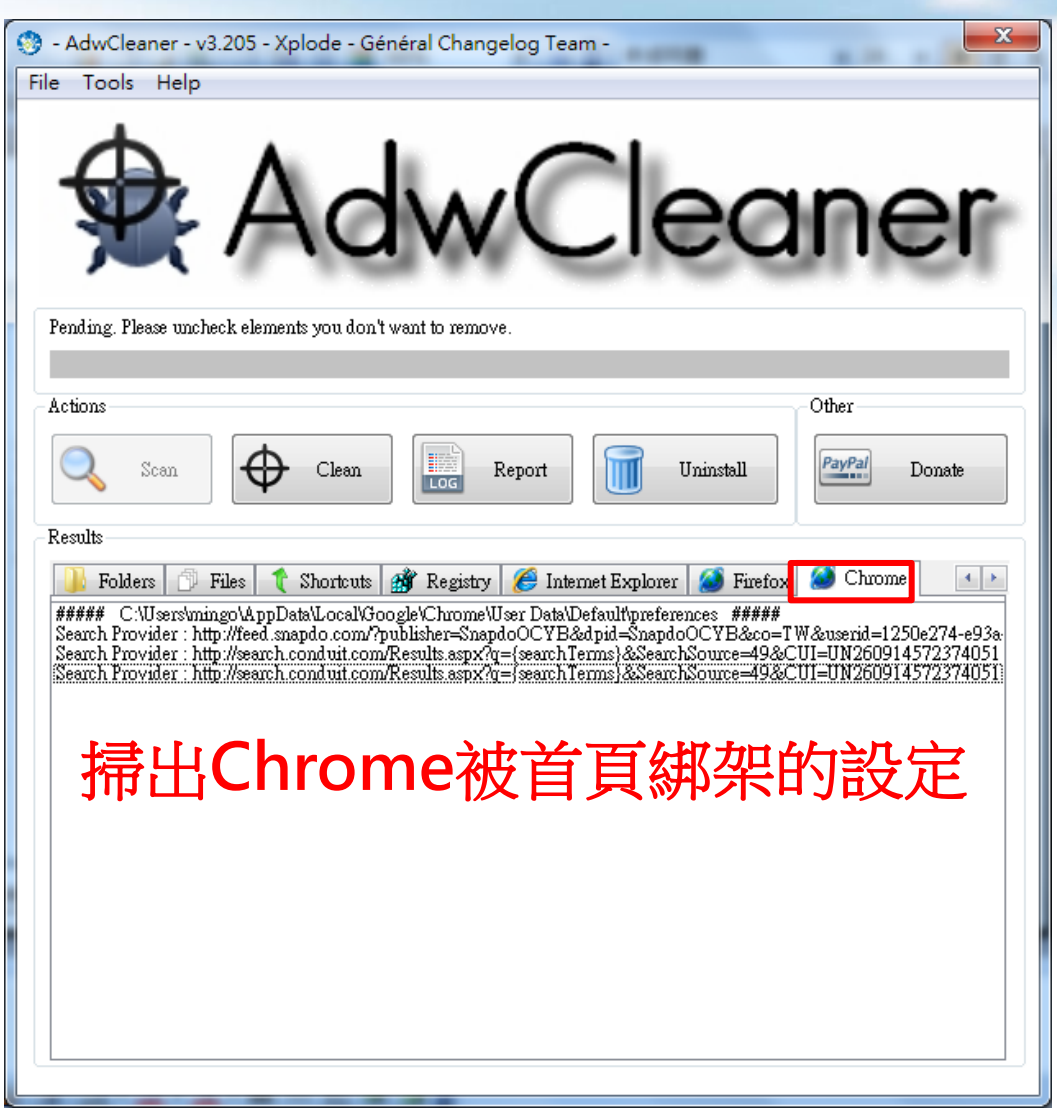


adwcleaner.exe首頁綁架移除程式(2/9)

adwcleaner.exe首頁綁架移除程式(3/9)



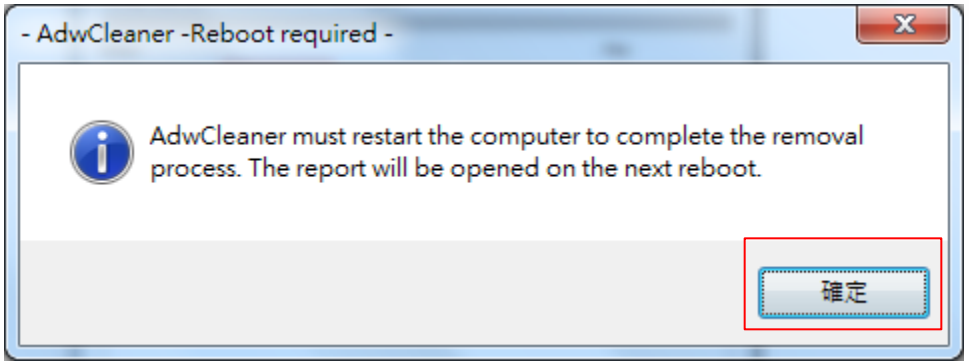
adwcleaner.exe首頁綁架移除程式(4/9)



adwcleaner.exe首頁綁架移除程式(5/9)

adwcleaner.exe首頁綁架移除程式(6/9)

因更動到系統設定,需重新開機



adwcleaner.exe首頁綁架移除程式(7/9)

```
# AdwCleaner v3.205 - Report created 30/04/2014 at 22:48:17
# Updated 28/04/2014 by Xplode
# Operating System : Windows 7 Home Premium Service Pack 1 (64 bits)
# Username : mingo - OP79
# Running from : D:\                                \adwcleaner.exe
# Option : Clean

***** [ Services ] *****


***** [ Files / Folders ] *****

Folder Deleted : C:\Users      .android
Folder Deleted : C:\Users      AppData\Local\genienext
Folder Deleted : C:\Users      AppData\Local\Mobogenie
Folder Deleted : C:\Users      AppData\Local\NativeMessaging
Folder Deleted : C:\Users      AppData\Local\PackageAware
Folder Deleted : C:\Users      AppData\LocalLow\DataMngr
Folder Deleted : C:\Users      AppData\Roaming\newnext.me
Folder Deleted : C:\Users      Documents\Mobogenie
File Deleted : C:\Users        emonprocess.txt

***** [ Shortcuts ] *****


***** [ Registry ] *****

Value Deleted : HKCU\Software\Microsoft\Windows\CurrentVersion\Run [NextLive]
Key Deleted : HKLM\SOFTWARE\Classes\VideoDownloadConverter_4z.SkinLauncherSettings
Key Deleted : HKLM\SOFTWARE\Classes\VideoDownloadConverter_4z.SkinLauncherSettings.1
```

開機後,會跟你報告,刪了那些資料

adwcleaner.exe首頁綁架移除程式(8/9)

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

```
-\\ Internet Explorer v11.0.9600.17041

Setting Restored : HKCU\Software\Microsoft\Internet Explorer\Search [Default_Search_URL]
Setting Restored : HKCU\Software\Microsoft\Internet Explorer\Search [SearchAssistant]
Setting Restored : HKCU\Software\Microsoft\Internet Explorer\SearchUrl [Default]
Setting Restored : HKLM\SOFTWARE\Microsoft\Internet Explorer\SearchUrl [Default]

-\\ Mozilla Firefox v

-\\ Google Chrome v34.0.1847.131

[ File : C:\Users\      \AppData\Local\Google\Chrome\User Data\Default\preferences ]

Deleted [Search Provider] : hxxp://feed.snapdo.com/?publisher=SnapdoOCYB&dpid=SnapdoOCYB&co=TW&userid=1250e2
Deleted [Search Provider] : hxxp://search.conduit.com/Results.aspx?q={searchTerms}&SearchSource=49&CUI=UN260
Deleted [Search Provider] : hxxp://search.conduit.com/Results.aspx?q={searchTerms}&SearchSource=49&CUI=UN260

**************************

AdwCleaner[R0].txt - [25941 octets] - [19/10/2013 13:08:52]
AdwCleaner[R10].txt - [6083 octets] - [30/04/2014 22:42:25]
AdwCleaner[R1].txt - [26123 octets] - [19/10/2013 13:20:53]
AdwCleaner[R2].txt - [1175 octets] - [19/10/2013 14:46:22]
AdwCleaner[R3].txt - [3335 octets] - [09/02/2014 17:59:49]
AdwCleaner[R4].txt - [1326 octets] - [10/02/2014 19:21:31]
AdwCleaner[R5].txt - [1446 octets] - [11/02/2014 19:30:03]
AdwCleaner[R6].txt - [1621 octets] - [15/02/2014 19:52:37]
AdwCleaner[R7].txt - [1567 octets] - [15/02/2014 19:56:42]
AdwCleaner[R8].txt - [1502 octets] - [15/02/2014 20:09:07]
AdwCleaner[R9].txt - [1806 octets] - [16/02/2014 06:50:32]
```

開機後,會跟你報告,修正那些設定

adwcleaner.exe 首頁綁架移除程式(9/9)

強化社群軟體安全性的參考連結

- 10 個強化Facebook帳號安全秘技，降低帳號被盜用的風險
  - http://free.com.tw/10-tips-for-improving-facebook-security/
- 8 個線上服務「兩步驟驗證」設定說明，確保帳戶免於威脅
  - http://free.com.tw/how-to-set-two-factor-authentication-up/
- 免費找資源
  - http://free.com.tw/

智慧財產權的參考連結

- 台灣創用 CC 計畫
  - http://creativecommons.org.tw
- 創用 CC 官方網站
  - http://creativecommons.org
- 教育部創用 CC 資源網
  - http://isp.moe.edu.tw/ccedu/
- 20 個免費下載創用 CC 授權音樂的網站彙整
  - http://free.com.tw/creative-common-music-download/

報告完畢 恭請指教

敬請指教！