賽門鐵克報告-Trojan.Taidoor: Targeting Think Tanks

目錄

一、 行政摘要 2

二、 序論 2

三、 技術說明 3

1. 電子郵件 3

2. 附檔 6

3. Dropper 8

4. payload 8

5. C&C 伺服器 9

6. 變種 11

7. 活動模式 13

8. 攻擊者概況 13

四、 總結 14

五、 資料來源 14

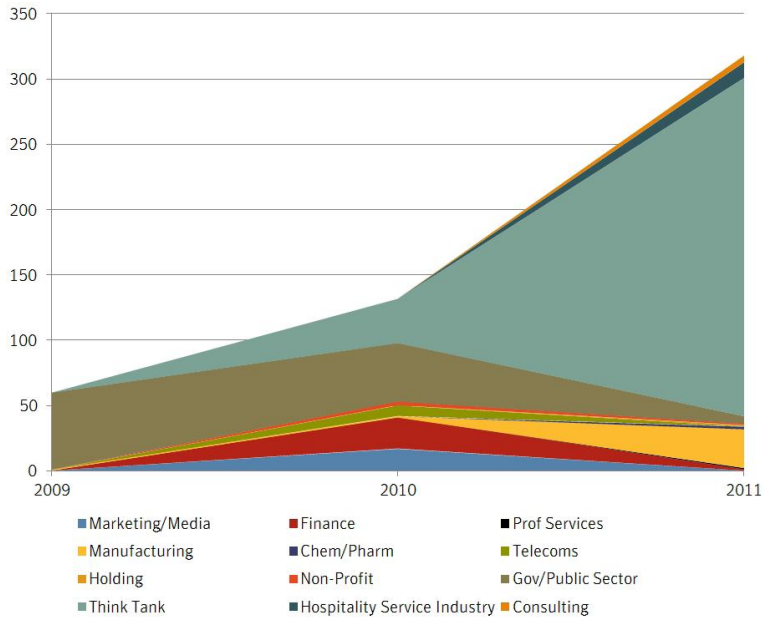
一、 行政摘要

過去三年來 Trojan.Taidoor 普遍使用在具有針對性的攻擊上面，尤其是在 2011 年 5 月過後，其攻擊活動大幅增加，其目前的主要目標為與美國和台灣國家安全事務上有關的私人企業和具有影響力的國際智囊團，在這些組織中的服務部門的設施也有可能成為目標之一，也就是作為攻擊主要對象的攻擊傳播媒介。

Trojan.Taidoor 的歷史可追溯到 2008 年 3 月與其使用的電子郵件攻擊手法則是在 2009 年 5 月，目前已經確認的主要有 14 個版本與 3 個獨立的 families，此威脅正不斷因應攻擊者的需求不斷發展中。

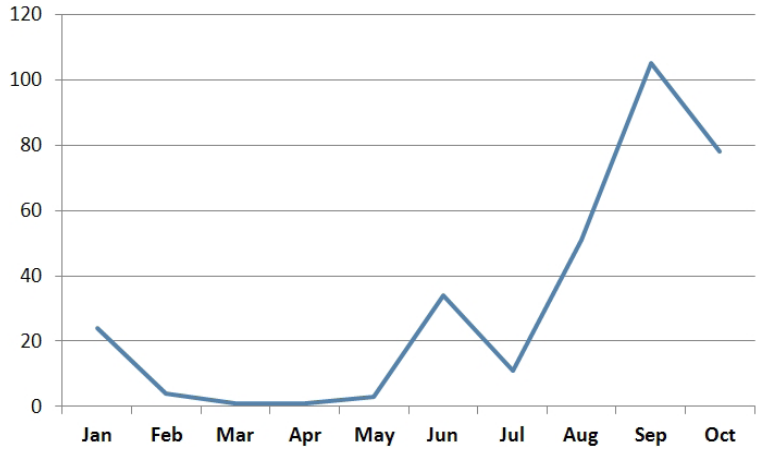
二、 序論

自從 2009 年開始，許多政府組織與私人企業成為 Taidoor 的攻擊目標，但在 2011 年之後，其攻擊重點逐漸轉向與台灣利益一致的國際智囊團、製造業和國防供應商，圖一說明過去三年來 Taidoor 對於各企業的攻擊目標轉移過程。



圖一、2009~2011 各行業被 Taidoor 攻擊的目標數

美國在 2011 年曾參與有關台灣空軍武力升級的會議，同一時間 Taidoor 開始針對那些在南亞和東南亞政策與軍事策略上具有專長的個人、團體或是有影響力的智囊團進行攻擊，雖然這並不是第一次對智囊團進行攻擊，但是這些持續且大量的攻擊使其更加顯著。從圖二來看的話，可以發現在 2011 年這一年當中，5 月~10 月的攻擊特別顯著，而台灣在 2011 年 9 月 18~20 日所舉辦的美台國防工業會議正剛好處於其攻擊的最高峰。



圖二、Trojan.Taidoor 目標電子郵件攻擊數量圖

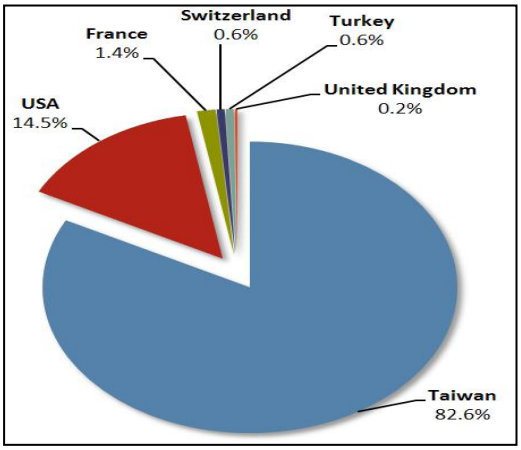
雖然這些年來 Taidoor 的攻擊目標一直在轉變，但是其手法卻仍保持一致，目前已知的攻擊媒介主要都是透過電子郵件並附加惡意程式，而這些惡意程式主要都是針對一些已公開的系統或軟體漏洞，這也就是說並沒有像是 Zero-day 或是 RSA 等高度精密的攻擊方式出現。因此其攻擊手法主要偏向於持續對那些使用過期或未更新補丁的使用者寄發大量與重複的電子郵件，藉此來破壞目標組織的網路。

此檔其它的部分將會更詳細地介紹這些攻擊，從 Taidoor 的攻擊階段一一做說明。從製作具有針對性的電子郵件開始，到其附檔與附檔的組成要素：Taidoor 的 dropper 和負責與 C&C 伺服器溝通的內嵌和加密的後門木馬程式，在這還會將 C&C 伺服器的功能揭示出來，包含觀察到的那些受害的第三方伺服器轉變為攻擊者通訊基礎設施的一部分和分析過程中所捕捉到的攻擊者與受害電腦之間的互動。

三、 技術說明

1. 電子郵件

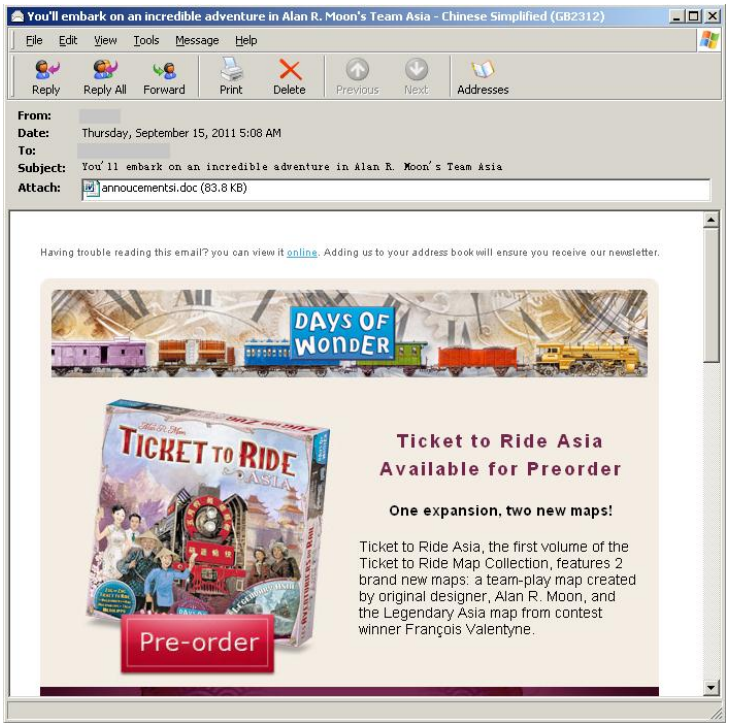
這主要是 Taidoor 進行攻擊的主要關鍵要素，根據圖三可得知目前寄發這些具有針對性攻擊電子郵件的電子郵件伺服器絕大部分來自台灣和美國，但是其原產國還是取決於攻擊的目標，像是來自法國的郵件中就會包含有關巴黎 G20 的資訊，而來自土耳其的電子郵件就會出現與目標同為主耳其電子郵件的地址。



圖三、Taidoor 電子郵件原始的郵件伺服器國家

這些具有針對性攻擊的電子郵件其內容是專門製作出來以誘騙目標點擊的，主要會將這些電子郵件寄發給目標或是目標組織中的其他人員，寄發給其他人員主要是目前最近的攻擊手法之一，主要是因為目標在難以誘騙的情況下，如果透過其他價值的低的目標藉此在組織當中當作立足點的話，就有機會向真正的目標進行攻擊。

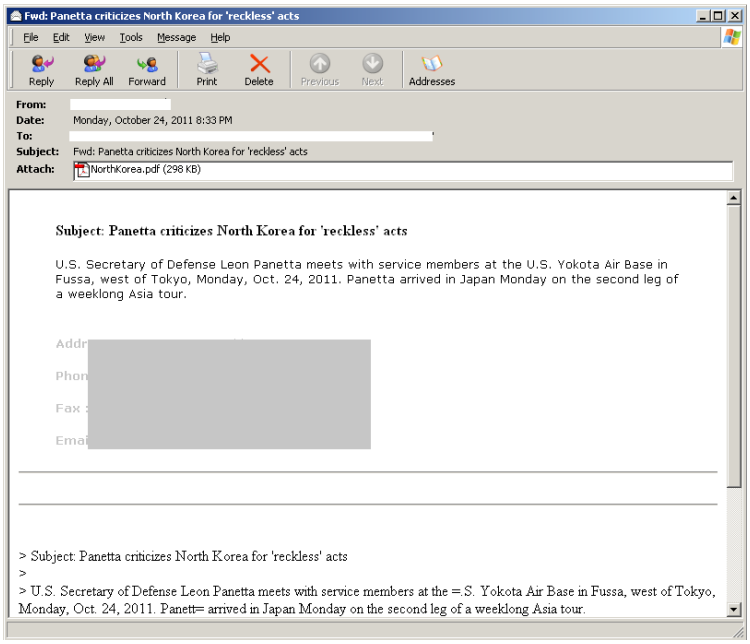
目前 Taidoor 主要有兩種內容型態，第一種是比較簡單的，對於目標的研究背景只需要少數或甚至不用瞭解，其內容通常為一個引人注意的主題、有趣的圖片、簡短的資訊或是一個熱門的話題，藉此誘騙使用者打開附檔，像是圖 4。



圖四、一般的 Taidoor 電子郵件

第二種型態則是需要對目標的研究主題做些研究，因此在這方面的準備是比較多的，在電子郵件上需要包含與目標相關的內容，主題、內文和附檔資訊都可能誘騙使用者閱讀，而這通常是與目標相關的政策或是會議，特別是寄件人的電子郵件也將被改成讓目標錯認為來自某會議或是在其領域中有信譽的來源、認可的名字或是同事。

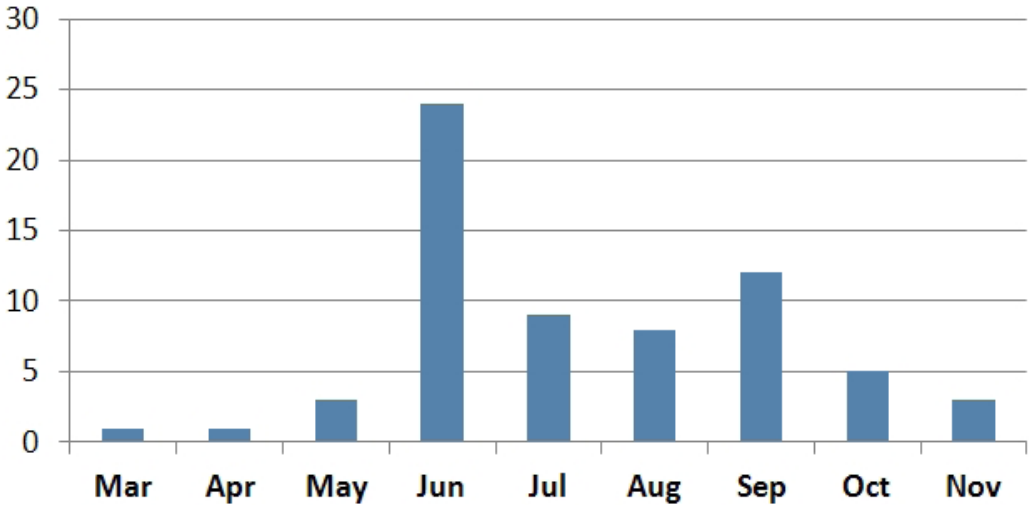
這舉出一個在 2011 年 10 月 24 所寄發的具有針對性的攻擊電子郵件如圖五，在這一天當中目標電子郵件主要寄發給分別在 3 個不同組織的 25 個個體，使用的是相同的惡意附檔，但主題與內容卻是不一樣的。



圖五、具有針對性的 Taidoor 電子郵件

在這 25 封電子郵件當中，有 22 封主要透過台灣的電子郵件伺服器所寄出，其目標主要是美國一些對於國際有影響力的智囊團，這些目標主要都是對於東南亞軍事策略和政策上專精的專家，而這就是典型的 Taidoor 攻擊手法，不管是不是真正感興趣的攻擊目標，但是這些稍加有關聯的目標也可提供有用的資訊或是作為攻擊真正目標的墊腳石。

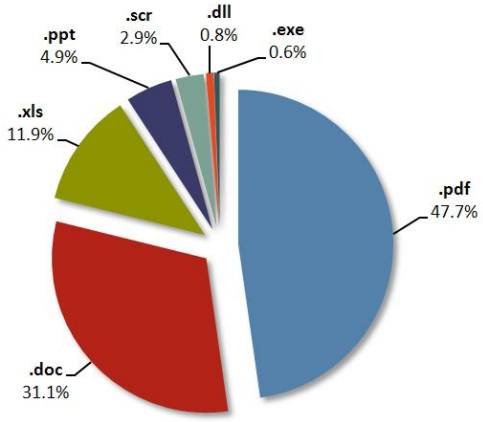
對於真正感興趣的攻擊目標可從檢查電子郵件寄發的頻率來看，以下用 X 先生舉例說明，我們可以從圖六發現到 X 先生從 2011 年 6 月開始往後推算的幾個月內，其具有針對性攻擊的電子郵件數量明顯大幅增加，而這持久的 Taidoor 攻擊也顯示出此目標比較難以誘騙與具有較高利益的價值考量。



圖六、以 X 先生為攻擊目標所寄發的電子郵件數量

2. 附檔

上述所提到的案例附檔為惡意的 PDF 檔案，但是這並不表示 Taidoor 只會利用 PDF 而已，所使用的附檔型態包含 Microsoft 的 PowerPoint、Word、Excel 和一些可執行檔與 DLL 如圖七。



圖七、附檔型態的普及程度

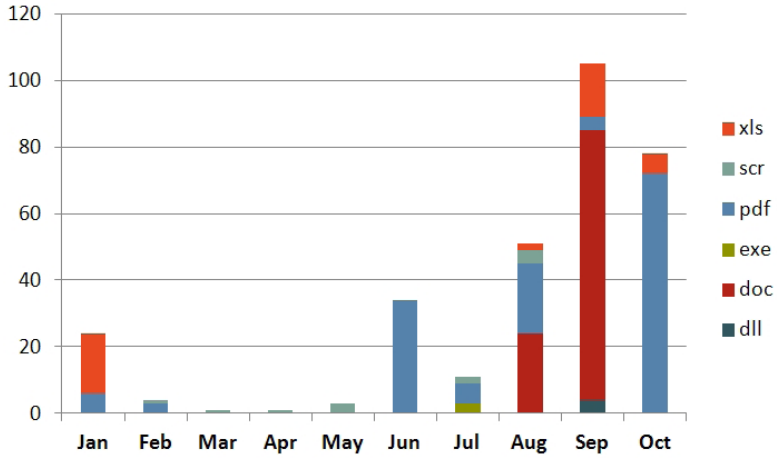
雖然在最近的攻擊中，主要是以 Word 和 PDF 為最流行的攻擊媒介，不過這幾年來由於漏洞不斷增加，因此附檔的格式也越來越廣，這也表明了 Taidoor 會隨著這些漏洞持續更新，且不是害怕嘗試新的攻擊而是透過這些已知漏洞進行攻擊效果較為顯著。

- Microsoft PowerPoint Malformed Record Remote Code Execution Vulnerability (BID 18382)
- Microsoft Word Malformed Data Structures Code Execution Vulnerability (BID 21518)
- Adobe Acrobat and Reader Multiple Arbitrary Code Execution and Security Vulnerabilities (BID 27641)
- Microsoft PowerPoint Sound Data (CVE-2009-1129) Remote Code Execution Vulnerability (BID 34839)
- Adobe Reader and Acrobat ‘newplayer()’ JavaScript Method Remote Code Execution Vulnerability (BID 37331)
- Microsoft Excel ‘FEATHEADER’ Record Remote Code Execution Vulnerability (BID 36945)
- Adobe Flash Player CVE-2011-0611 ‘SWF’ File Remote Memory Corruption Vulnerability (BID 47314)
- Multiple Microsoft Products DLL Loading Arbitrary Code Execution Vulnerability (BID 47741)
- Adobe Acrobat and Reader CVE-2011-2100 DLL Loading Arbitrary Code

Execution Vulnerability (BID 48252)

特別注意到的是 Taidoor 都不是使用 Zero-day 進行攻擊，都是利用公開的系統和軟體漏洞，因此著重於系統或軟體尚未進行補丁修補的目標。

圖八主要顯示了攻擊者在 2011 年所選擇的電子郵件附檔類型，從這我們可以看到 2011 年 9 月所舉辦的美台國防工業會議這段時間內，附檔為 Word 的使用頻率增加，這表示著在此期間使用 Word 來誘騙目標的機率是較為顯著的，而像是上述所提到的漏洞 BID 47741，雖然這是比較新的漏洞，但與之前的漏洞相較起來較為不顯著，因此還是會被替換成比較舊的。

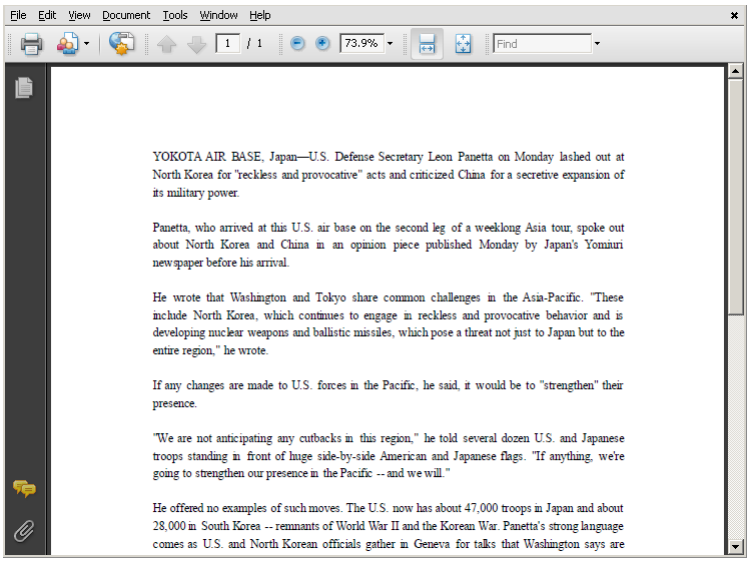


圖八、2011 年電子郵件附檔型態的分析

此電子郵件的目的為誘騙目標打開惡意的附檔，此附檔的目標為暗中複製木馬到目標的電腦並啟動它，而這之間並不會提醒目標已受害的事實。

針對前面所提到的 PDF 附檔，我們來檢驗一下將此檔案打開會發生甚麼事情，此針對的是在 Adobe Reader 中漏洞也就是 BID 47314 這邊，可讓使用者選擇要攻擊的程式碼，當此程式碼被解密之後，Dropper 便會將後門程式植入目標的電腦，並將此惡意 PDF 轉變為正常的 PDF，藉此不讓目標察覺其已受害。

圖九所顯示的內容為美聯社在 2011 年 10 月 24 日所出現的文章，主要被使用來當作誘騙目標點擊的。



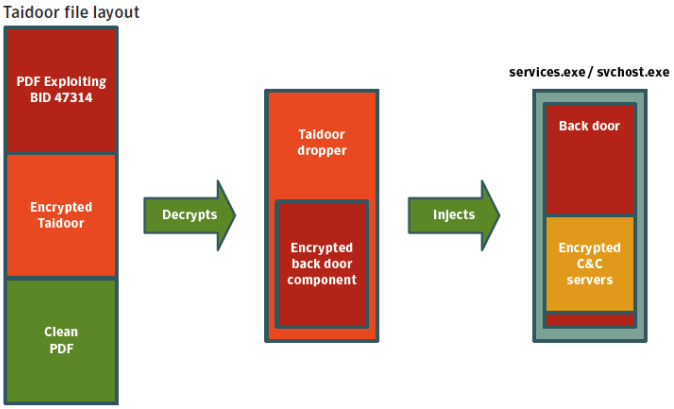
圖九、Taidoor 的 PDF 附檔

3. Dropper

一旦目標打開惡意的附檔之後，便會將感染程序啟動，再來 Dropper 如果在系統中建立的話，便會將以下這些合法程序開啟直到惡意的後門程式取代這些程序：

- services.exe
- svchost.exe

後門程式的組成要件通常是 dropper 程式部分之中的一個加密的資源通道，或是一個加密的二元陣列，圖十主要描述了當惡意附檔啟動時，其每個檔案的感染流程與組成要件。



圖十、Taidoor 檔案設計

4. payload

此為與 C&C 伺服器溝通的後門程式要件，會將 C&C 伺服器的配置資訊儲存在「.data」之中，而此配置資訊包含了三個 C&C 伺服器與其連結的 Port 和預設的睡眠時間。

一旦成功的在系統上安裝後門程式的話，便會透過 HTTP 協定與 C&C 伺服器進行通訊。

5. C&C 伺服器

(1) 協定

Trojan.Taidoor 使用 HTTP 協定與其 C&C 伺服器進行通訊，表一為其請求的格式與內容：

http://[C&C_SERVER]:[PORT]/[RANDOM].php?id=[RAND][ID][OPTIONAL]

Table 1
HTTP communication format

Variable	Description
[C&C_SERVER]	Up to three configurable C&C servers
[PORT]	Up to three configurable ports
[RANDOM_PATH]	Five random, lower-case letters. Recreated every time Taidoor initializes or fails to contact its configured servers.
[RAND]	Six-decimal, random number recreated for each request. The values are between 0-32767 (limited by RAND_MAX).
[ID]	Twelve characters derived from MAC address of the compromised computer.
[OPTIONAL]	Is "&ext=[FILENAME]", which may be present in requests, related to specific commands.

表一、HTTP 通訊格式

當在請求或回應訊息時，主要都會透過 RC4 來進行加密，而 RC4 的鑰匙主要是透過受害電腦的網卡位置以字串的型式組成，像是 01-27-89 AB-CD-EF，而這就表示能夠透過[ID]來獲得 RC4 的鑰匙，因為每一個[ID]對於控制伺服器來說唯一的。

而當 Trojan.Taidoor 在產生此[ID]的時候，主要會利用一種演算法，首先會將所獲得的網卡位置已字串型式表示，如果未獲得網卡位置的話，便會以默認值「01-01-01-01-01-01」表示，然後再將每一個「-」去掉之後，將每一個字元值遞增，如果遇到「9」的話，便會將其設為「0」，例如「01-27-89-AB-CD-EF」會轉變為「123890BCDEFG」。

Trojan.Taidoor 會定期根據 C&C 所配置的資訊發送給 C&C 伺服器一個空的 GET 請求，而其睡眠時間間格中最短為 2 秒、最長則為 600 秒，伺服器的回應中其第一個 Byte 為命令 ID，再來則是可搭配的參數，表二列出命令資訊。

Table 2

Taidoor C&C commands

ID*	Format	Command	Details
2	DWORD	Set Delay	Period in milliseconds for the sleep time in between requests.
3	STRING	Execute Command	Command to be executed. The generated output is collected in a temporary file and sent in a separate POST request. The POST request does not contain any indication about the corresponding command.**
4	STRING	Download and Execute	The URL location to download a file, which is saved to the %Temp% folder and executed.
5	STRING	Download File	Path of the file to be created. The content of the file is downloaded using a separate GET request with [OPTIONAL] set to "&ext=[BASE64_ENCODED_FILENAME]"
7	STRING	Upload File	Parameter is the path of the file to be uploaded. Content of the file is uploaded using separate POST request with [OPTIONAL] set to "&ext=[BASE64_ENCODED_FILENAME]"

*All other commands are IDs treated as pings. **A strong indicator this back door is designed for human operators.

表二、Taidoor 的 C&C 指令

(2) 實際捕捉到的互動程序

我們的 honeypot 捕捉到攻擊者透過後門在下達指令的情況，表三主要列出其活動，為 UTC 2 點 23 分 06 秒開始之後的第一個 60 秒紀錄。

Table 3

Example of attacker activities through back door

Timeline	Commands Received
2011-09-16 02:23:06 UTC: RECV	[Ping]
2011-09-16 02:23:15 UTC: RECV	[Set sleep interval to 1 second]
2011-09-16 02:23:23 UTC: RECV	cmd /c net start
2011-09-16 02:23:31 UTC: RECV	cmd /c dir c:\docume~1\
2011-09-16 02:23:52 UTC: RECV	cmd /c dir "c:\docume~1\<CurrentUser>\recent" /od
2011-09-16 02:24:00 UTC: RECV	cmd /c dir c:\progra~1\
2011-09-16 02:24:12 UTC: RECV	cmd /c dir "c:\docume~1\<CurrentUser>\desktop" /od
2011-09-16 02:24:25 UTC: RECV	cmd /c netstat -n
2011-09-16 02:24:32 UTC: RECV	cmd /c net use

表三、攻擊者透過後門下達命令的活動紀錄

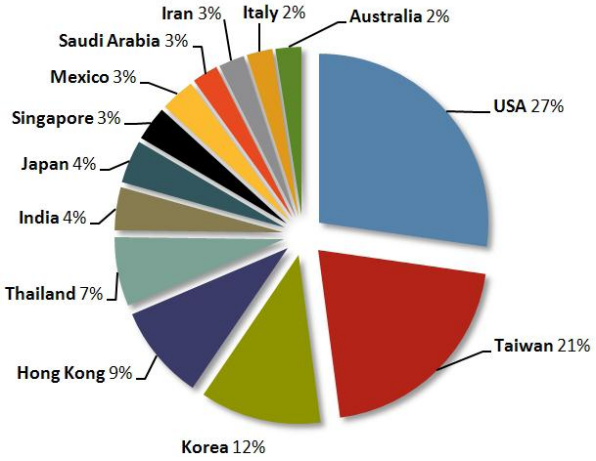
安全緊急應變中心在攻擊者開始此活動之前啟動了命令列模式，其中 Taidoor 主要根據指示將其睡眠時間間格設置為 1 秒以方便改善 Trojan.Taidoor 的攻擊者在發送命令之後的回應時間，接下來的 60 秒內主要是攻擊者在尋找有關受害電腦的以下資訊：

- 目前「Documents and Settings」資料夾的內容與系統有哪些使用者？
- 「Recently Used Documents」項目中的內容
- 「Program Files」資料夾中的內容：安裝了哪些軟體？
- 桌面上的內容
- 目前開放的 TCP/IP 連結清單
- 可用的網路連結清單

當攻擊者在受害電腦中搜尋資訊之後，如果此為不感興趣的目標的話，攻擊者便可透過此電腦對其他價值更高的電腦透過下載額外工具等方式進行網路感染以協助其在網路中潛伏，不過值得注意的是這並不是自動化的流程，而是真正有攻擊者坐在另外一端輸入這些指令。

(3) 受害的第三方伺服器

許多基本的偵查都會透過 Trojan.Taidoor 所利用的 C&C 伺服器來進行，而這些 C&C 伺服器有時後似乎好像是受害的第三方伺服器，而非租用的伺服器，這些受害的伺服器主要是用來隱藏攻擊者的真實位置，根據圖十一調查顯示 Trojan.Taidoor 的 C&C 伺服器最有可能的位置在美國和台灣。



圖十一、C&C 伺服器所在國家

圖十二所表示的為一個受害的第三方伺服器，通常會做這樣的汙損可能代表著此電腦上的服務微不足道、沒有進行補丁修補貨是維護不良等等。

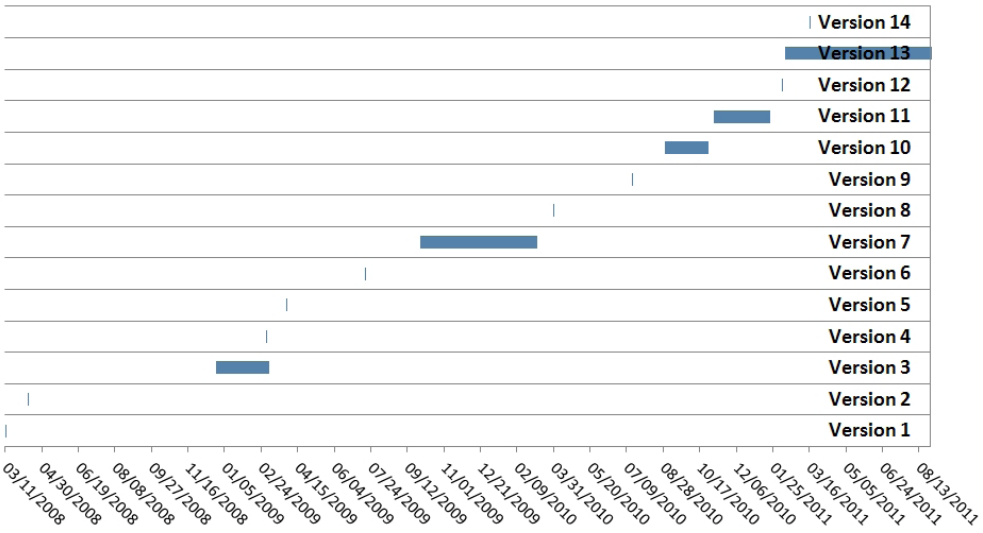
圖十二、先前受害的 C&C 伺服器

6. 變種

到目前為止，我們已經發現到至少有 14 個不同的 Trojan.Taidoor 變種，最早發現的時間為 2008 年 3 月 11 日，隨著時間的推移，Trojan.Taidoor 本身的版本資訊並不會跟著轉變，會轉變的主要為後門要件程式碼方面的修改，這就表示著不同的 PE 執行檔擁有相同的程式碼區段，不同的在於 C&C 伺服器詳細資訊攻擊中的 data 區段。

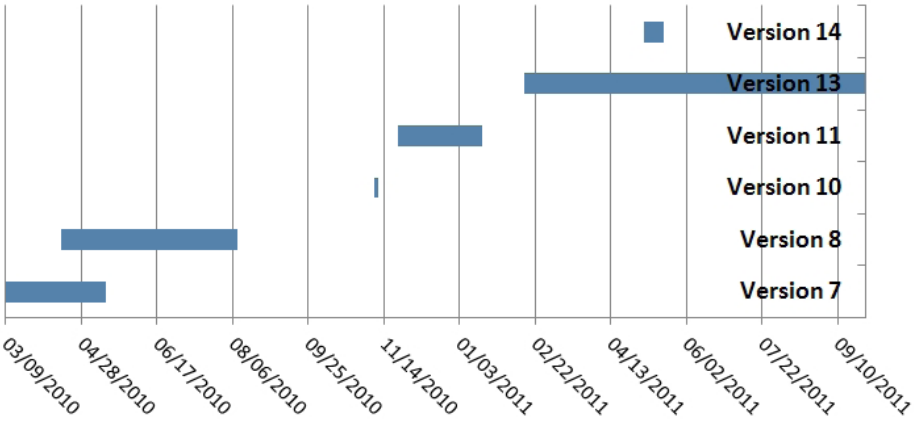
根據圖十三顯示有些版本已廣泛使用，但有些版本其存活時間非常短，而其中還可以觀察到其後門版本之間很少有重疊部分，這表示其版本主要是由一個單一的實體負責開發，因為如果是由多個實體共同開發的話，那麼將會有很多版本存在且互相重疊。

其中最廣泛的版本為第 13 個版本，主要目標使用於智囊團。



圖十三、以 PE 程式碼區段相似度為基準的 Trojan.Taidoor 版本演進

圖十四主要為電子郵件時間的比較而不是編譯時間的比較，許多後門的版本有某種程度上的重疊，但之後再使用的則是不同的版本，而這情形也鞏固了上述所假設的其版本是為單一實體所控制的。



圖十三、透過電子郵件散佈的 Trojan.Taidoor 版本演進

7. 活動模式

根據一些觀察可以發現這些伺服器會在某一個時間點醒來發出一個連結重置或是回傳一個「HTTP 404」的訊息，而這時間通常發生在 UTC 1 點~8 點之間。

8. 攻擊者概況

將這些 Taidoor 的攻擊歸屬於某一個團體是比較不可能的，由於 Taidoor 的攻擊當中其版本會隨著後門的版本演進且比較一致，因此比較偏向於全職的個體，然而這還需要有一些額外的 C&C 伺服器基礎設施，所以這也有可能是由具有組織規模且其團員都具有某種程度的駭客攻擊能力的團體，藉此將此工作妥善配置，對不同的攻擊階段給予特別的角色來進行攻擊。

雖然這些行動是由某些人所組成的，但根據其不使用 Zero-day 進行攻擊來看，其資源是有限的，但其 C&C 伺服器大部分都是由受害的第三方伺服器所組成，因此可以判定此組織並沒有一定的資金來源。

根據模式顯示與 C&C 伺服器進行溝通的時間主要發生在 UTC 1 點~8 點之間，圖十四顯示了世界各地不同國家所代表的時間。

Table 4
Time zones

Region	Local Time
Japan	10:00am—5:00pm
Taiwan	9:00am—4:00pm
China (Beijing)	9:00am—4:00pm
India	6:30am—1:30pm
Russia (Moscow)	5:00am—12:00pm
UK	1:00am—8:00am
US (Eastern)	8:00pm—3:00am
US (Pacific)	5:00pm—12:00pm

圖十四、世界各地時區

除此之外，透過其所寄發的電子郵件可以發現到該組織對於使用英文與繁體中文撰寫電子郵件上有一定的水準能力。

雖然其動機難以確定，但自從 2011 年之後，從其目標的轉變來看，可以發現到其最初目標是分散的，之後則轉變為專注於特定類型的政策目標也就是智囊團，且著重在「美台交易」這主題上。

因此這主要探討的主題在於這些駭客最感興趣的議題是什麼，對於相關議題最有可能影響到的是哪些私人企業或智囊團等等。

四、 總結

Trojan.Taidoor 的基本攻擊手法為製作一個具有針對性目標的電子郵件並附加惡意檔案，其主要特徵是此攻擊會持續且積極的進行攻擊，從 Taidoor 的版本變動和目標的轉換，可以發現這些攻擊將會是持續與永無停止的。

五、 資料來源

[1]. 賽門鐵克-Trojan.Taidoor: Targeting Think Tanks:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/trojan_taidoor-targeting_think_tanks.pdf