NTPA – Taiwan, ROC

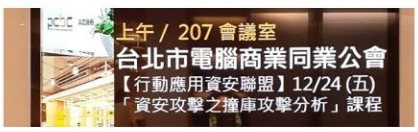
中華民國網路封包分析協會
會員電子報

www.nspa-cert-tw.org　　2022 年　第 1 季　　第 1 期

最新消息報導
行動資安聯盟資安訓練

秘書組整理編輯

雖是歲末年終，在 2021 年 12 月 24 日，本協會理事長劉得民先生，受邀台北市電腦商業同業公會與行動應用資安聯盟共同舉辦的內部資訊安全專題講座。此專題講座課程，係針對 2021 年的最後一季，台灣發生的證券商資安撞庫攻擊事件，提出相關的分析研究報告。並解說該類攻擊事件，在智慧手機(行動裝置)APP 與，網路服務主機端的異常徵兆與偵測預防方式。與會人員包括行動應用資安聯盟、與國內金融機構的資安稽核人員，總人數超過 30 人以上。



上午課程開始，由 陳會長振楠致歡迎詞，並介紹參與課程的相關機構組織與代表人員。隨後，由本協會的劉得民理事長，開始說明密碼撞庫攻擊(Credential Stuffing Attacking), 或稱為憑證填充攻擊的原理，同時分析比較另一種常見的密碼攻擊方式-密碼噴灑攻擊(Password Spraying Attacking)的近似與差異之處。接著劉得民理事長從程式設計、資安偵測、與使用者習慣等的多種不同層面及角度，加以解說分析密碼撞庫攻擊(Credential Stuffing Attacking)之各種特性。接著，在連接網際網路後，劉得民理事長示範網路外洩帳號密碼的資料販售市場，與在暗網市場(Dark Web) 取得買賣各知名企業外洩的檔案資料。

隨後，劉得民理事長接著繼續示範，如何幫自己與協助客戶，立即檢測檢視相關帳號密碼是否外洩?

在此同時，行動應用資安聯盟於會議場所，提供舒適的環境與飲料餐點，並在中場休息時間，介紹各方人員互相交流，現場氣氛愉快。

圖 1-本協會分享撞庫攻擊相關案例與緩解技術

本協會劉得民理事長並在現場示範，如何預先檢測自己遭遇撞庫攻擊的風險評估方式，以便於事先瞭解網路使用者的帳號密碼是否可能外洩? 甚至遭遇撞庫攻擊!!

圖 2-撞庫攻擊密碼外洩檢測範例

(本會刊僅限會員閱讀, 非會員須付費訂閱)

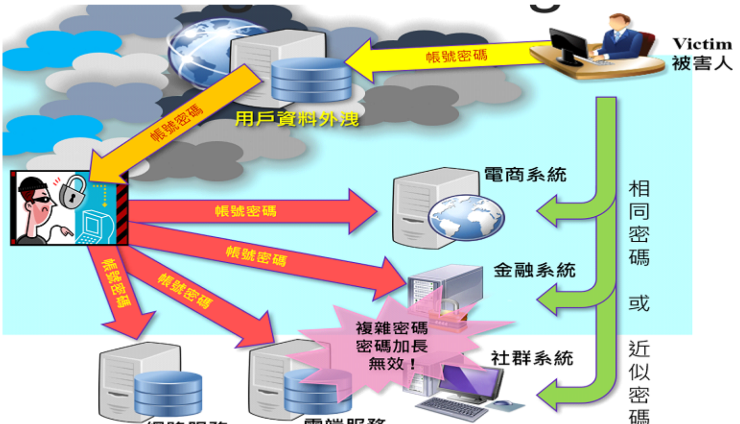
活動消息
飛安資安訓練

秘書組整理編輯

本協會於 2021 年 10 月 7 日、8 日配合交通部民航局與中華民國飛安基金會主辦之「航空保安種子講師網路保安差異訓練」訓練課程，此次課程內容包括: 民航局解說航空 ICAO 規範說明、中華航空的航空網路保安現況及脆弱點分析、中華民國網路封包分析協會的航空網路保安未來風險。

此項訓練活動係根據國際航空組織 ICAO-8973 保安規範，本協會由劉得民老師，在交通部民航局國際會議廳，訓練各航空公司的航空資安種子教師，相關國際航空飛行資安規範的課程訓練。本協會針對「航空網路保安未來風險」為題，提供相關案例分析與經驗分享。訓練課程參與人數超過 70 人次以上，為國內航空資訊保安的首次種子教師訓練活動。

圖 3-本協會提供航空網路保安的分險分析



帳號密碼撞庫攻擊

Credential Stuffing Attacking

圖 4-撞庫攻擊(Credential Stuffing Attcking)示意圖

技術組整理編輯

撞庫攻擊，全稱『帳密撞庫攻擊』，原文是 Credential Stuffing Attack，翻譯為『憑證填充攻擊』[註 1]。它在 ATT&CK Matrix 的攻擊分類編號為 T1110.004，相同意義的攻擊名稱分別有，Credential Spills[註 3], Account checker attack, Account checking, Account takeover, Account takeover attack, Login Stuffing, Password list attack, Password re-use, Stolen credentials, Use of stolen credentials[註 4]等。[illegible] 碼，攻擊者便在暗黑市場購買到這些外洩的帳密資料，便可以嘗試使用這些帳密登入金融證券系統，進而造成消費者的金錢損失。

撞庫攻擊的偵測技巧與緩解方式，雖然有許多不同方案，但是其根本緣由是「消 [illegible] 入密碼相同，就導致攻擊者可能得逞。

參考資料來源:

註 1: https://blog.trendmicro.com.tw/?cat=4038 , view in 2021

註 2: https://baike.baidu.com/item/%E6%92%9E%E5%BA%93/16480882 , view in 2021

註 3: https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report, view in 2021

註 4: https://owasp.org/www-project-automated-threats-to-web-applications/assets/oats/EN/OAT-008_Credential_Stuffing , view in 2021

註 5: Wang, Ke Coby, and Michael K. Reiter. "Detecting stuffing of a user's credentials at her own accounts." 29th {USENIX} Security Symposium ({USENIX} Security 20). 2020.

帳號密碼撞庫攻擊

主要 4 大步驟

技術組整理編輯

帳號密碼撞庫攻擊(Credential Stuffing Attacking) 屬於帳號密碼攻擊的一種方式，其攻擊階段可以區分的主要 4 個階段，分別是:

- Data Breach, 從 來源-A 竊取帳號密碼
- Searching, 尋找有價值的系統-B
- Offensive, 針對目標-C, 進行攻擊
- Crime, 成功登入 B 系統, 完成後續攻擊

上述四個攻擊步驟，可以參考圖 5 的圖示，進一步瞭解到『撞庫攻擊的難以防堵之處，在於 A 系統所洩漏的消費者帳號密碼，被拿來作為攻擊(入侵)B 系統的帳號，關鍵就是: 在不同系統(A 與 B)，消費者使用相同密碼』。

如此 B 系統就難以確認登入者是否為原始消費者? 緩解方式，對 B 系統而言，可以使用 [illegible]

[illegible]

[illegible] 也需要減少 A 系統的帳密外洩問題，與提高消費者 C 的資安危機意識。藉以多管齊下，才是全面解決之道。

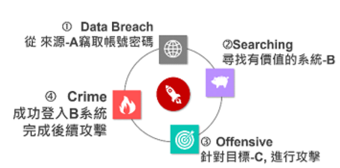


圖 5-帳號密碼撞庫攻擊的主要步驟

No.	Time	Source	Destination	Protocol	Length	Info
49	3.428997	10.0.1.58	163.17.65.134	HTTP	425	GET /news.asp HTTP/1.1
93	3.872817	163.17.65.134	10.0.1.58	HTTP	982	HTTP/1.1 200 OK (text/html)
95	3.892550	10.0.1.58	163.17.65.134	HTTP	455	GET /style.css HTTP/1.1
105	3.893981	10.0.1.58	163.17.65.134	HTTP	512	GET /images/hot_ico.gif HTTP/1.1
106	3.894027	10.0.1.58	163.17.65.134	HTTP	512	GET /images/new_ico.gif HTTP/1.1
111	3.895026	10.0.1.58	163.17.65.134	HTTP	508	GET /images/top.gif HTTP/1.1
112	3.895039	10.0.1.58	163.17.65.134	HTTP	515	GET /images/bullet_bak.png HTTP/1.1
126	3.929172	10.0.1.58	163.17.65.134	HTTP	512	GET /images/imp_ico.gif HTTP/1.1
132	3.929658	163.17.65.134	10.0.1.58	HTTP	1291	HTTP/1.1 200 OK (text/css)
134	3.933421	10.0.1.58	163.17.65.134	HTTP	510	GET /images/post3.gif HTTP/1.1
135	3.957618	163.17.65.134	10.0.1.58	HTTP	1285	HTTP/1.1 200 OK (GIF89a)
137	3.959743	10.0.1.58	163.17.65.134	HTTP	492	GET /header.html HTTP/1.1
139	3.963060	163.17.65.134	10.0.1.58	HTTP	462	HTTP/1.1 200 OK (GIF89a)
141	3.963433	10.0.1.58	163.17.65.134	HTTP	510	GET /images/post2.gif HTTP/1.1
142	3.964779	163.17.65.134	10.0.1.58	HTTP	514	HTTP/1.1 200 OK (GIF89a)
144	3.965097	10.0.1.58	163.17.65.134	HTTP	510	GET /images/post1.gif HTTP/1.1
145	3.970114	163.17.65.134	10.0.1.58	HTTP	549	HTTP/1.1 200 OK (PNG)
147	3.970522	10.0.1.58	163.17.65.134	HTTP	506	GET /top_link.gif HTTP/1.1
148	3.976028	163.17.65.134	10.0.1.58	HTTP	804	HTTP/1.1 200 OK (GIF89a)
150	3.977996	163.17.65.134	10.0.1.58	HTTP	717	HTTP/1.1 200 OK (GIF89a)
152	3.981364	163.17.65.134	10.0.1.58	HTTP	805	HTTP/1.1 200 OK (GIF89a)
154	3.988560	163.17.65.134	10.0.1.58	HTTP	798	HTTP/1.1 200 OK (GIF89a)
156	3.999128	163.17.65.134	10.0.1.58	HTTP	443	HTTP/1.1 200 OK (GIF89a)
168	4.022401	163.17.65.134	10.0.1.58	HTTP	1383	HTTP/1.1 200 OK (text/html)
170	4.035509	10.0.1.58	163.17.65.134	HTTP	495	GET /copyright.html HTTP/1.1
171	4.044720	10.0.1.58	163.17.65.134	HTTP	465	GET /style_header.css HTTP/1.1
172	4.047256	10.0.1.58	163.17.65.134	HTTP	514	GET /content_bg_green.gif HTTP/1.1
173	4.049319	10.0.1.58	163.17.65.134	HTTP	514	GET /images/FBicon.jpg HTTP/1.1
174	4.049666	10.0.1.58	163.17.65.134	HTTP	500	GET /bg.gif HTTP/1.1
175	4.050178	10.0.1.58	163.17.65.134	HTTP	486	GET /js_menu/stmenu.js HTTP/1.1
177	4.058982	163.17.65.134	10.0.1.58	HTTP	263	HTTP/1.1 200 OK (text/html)
186	4.083660	10.0.1.58	163.17.65.134	HTTP	330	GET /favicon.ico HTTP/1.1

網頁瀏覽的封包序列

圖 7-瀏覽網站網頁的封包行為序列

訓練組 整理編輯

HTTP 通訊協定，是網站服務的主要協定之一，屬於明碼傳送的基礎協定之一。而加密型態的 HTTP 協定，則是 HTTPS 通訊協定。在網路封包分析的角度，兩者類似卻不一樣，而在網站存取紀錄(LOG 分析)的角度，兩者則幾乎相同。

進行 HTTP/HTTPS 網路安全封包分析的關鍵，是要區分「人類操作」與「非人類行為」。如此，才能進一步從「非人類行為」裡面，繼續區分(1)系統程式行為，(2)應用程式行為，(3)異常程式行為(包括病毒木馬等等的惡意程式行為)。首先，要瞭解的 HTTP 封包就是人類操作行為：瀏覽網站的封包行為。

基本上，人類瀏覽網站的行為，常見有以下幾種方式：(A)輸入網站名稱，從網站首頁開始瀏覽，或是 (B)點擊搜尋引擎得查詢結果，由搜尋網頁轉進入網站瀏覽網頁，或 (C)由廣告網頁或其他 URL 網址，轉入網站瀏覽網頁，與 (D)經由書籤 Bookmark 進入目標網站網頁。

在進入網站前，會產生進行初始連線(稱為 TCP 3 Way Hand Shaking)，在此之前，通常會產生 DNS 查詢與覆答的封包 [註:某些瀏覽器，則將 DNS 包藏於 QUIC 與 GQUIC 封包，無法觀察到 DNS 活動封包]。使用者瀏覽一般網站網頁的內容，包括基本 HTML 文字、圖片、色塊與箝入項目。不論是 asp, aspx, php, jsp, html 網頁資源，在傳送網頁內容後，瀏覽器會解讀該網頁 HTML 架構與內容，並依序且快速地，逐一透過 HTTP 協定完成傳送其他資源檔案的 HTTP 指令(稱為 Request 或 Method)通常是 GET 或是 POST 指令，最常使用(最常出現)。

如同圖 7 所示，使用 HTTP 指令依序取回 news.asp 的 HTML 輸出文字，與許多 css 檔案、gif 檔案、png 檔案、jpg 檔案、js 檔案等網頁輔助資料檔案！這段 HTTP 動作，每個指令的間隔時間極為短暫迅速。

另外一方面，人類的瀏覽網頁過程，每次點擊滑鼠與閱讀網頁內容的間隔間距時間，是隨機過程，不同人閱讀網頁的停留時間，乃至同一人在不同情境閱讀網頁的停留時間，都不會完全相同，如圖 8 所示，就是呈現人類瀏覽與閱讀網站網頁內容的時間特性。

因此，下列 HTTP 行為特性，就是網路安全封包分析在 HTTP 通訊的基本項目:

(1) 前導 HTTP 連線的 DNS 詢答封包

(2) 閱覽網頁的間隔時間

(3) HTTP 的 Request(GET 或 POST)的重要欄位，包括 User-Agent、Host、Referer、Accept-Language、Accept 等等。

這些特性，將於後續技術文章，詳細解說。藉由前述 3 種特性，我們就可以區分最基本的人類 HTTP 行為，並且找出非人類 HTTP 行為後，針對異常程式行為的 HTTP 封包進行探討。在下期系列文章中，我們將具焦於非人類行為的網路封包特性。

圖 8-人類瀏覽網頁內容的時間間隔特性

No.	Time	Source	Destination	Country	Protocol	Length	Info
3534	87.572212	192.168.200.55	47.242.205.57	Hong Kong	HTTP	236	GET /posg/?RVe07=t/NymjUpuaLD1mR4G+w/dvwfa4zMuFr4+1dOBWu7SW9vz
3667	87.626110	47.242.205.57	192.168.200.55	Hong Kong	HTTP	343	HTTP/1.1 404 Not Found (text/html)
5424	92.629130	192.168.200.55	172.217.160.115	United States	HTTP	238	GET /posg/?RVe07=0ewOIJUiBrhQG8HREBZIT9RZRzEmmalcLppQkvyWhyJ6E
5426	92.639219	172.217.160.115	192.168.200.55	United States	HTTP	551	HTTP/1.1 302 Found (text/html)
5851	97.916141	192.168.200.55	188.165.33.127	France	HTTP	236	GET /posg/?RVe07=SF6dGwePBiXU2YDy8pBg8O1McfAnCuf37kbQ+Tv72jaoZ
5868	98.194140	188.165.33.127	192.168.200.55	France	HTTP	504	HTTP/1.1 404 Not Found (text/html)
5895	103.229570	192.168.200.55	23.227.38.74	Canada	HTTP	239	GET /posg/?RVe07=YnxWwuJkjw7/dCRerf4g7mcPecV4SPiQ15RS7qTroPdsn
5902	103.289086	23.227.38.74	192.168.200.55	Canada	HTTP	60	HTTP/1.1 403 Forbidden (text/html)
7845	108.424271	192.168.200.55	104.21.71.110		HTTP	236	GET /posg/?RVe07=P6fJhkh82jcpqDhI00oWlPADJh9KukOO0RWX18f3GMGk+
8347	108.584148	104.21.71.110	192.168.200.55		HTTP	824	HTTP/1.1 301 Moved Permanently
8475	119.000583	192.168.200.55	34.102.136.180	United States	HTTP	229	GET /posg/?RVe07=oDXz3AL/E/dKmohDjdkpJVWy7gxCn4GBvOR6hingcS0p0
8477	119.104486	34.102.136.180	192.168.200.55	United States	HTTP	515	HTTP/1.1 403 Forbidden (text/html)
8996	124.107665	192.168.200.55	199.59.243.200	United States	HTTP	224	GET /posg/?RVe07=1S/HE5r3wKSfbjkU36HwoFEi3ZCAzOv45zmOyYOiZaD7W
8999	124.459042	199.59.243.200	192.168.200.55	United States	HTTP	730	HTTP/1.1 200 OK (text/html)
9032	129.600033	192.168.200.55	104.21.80.25		HTTP	226	GET /posg/?RVe07=nMxJIAP6cc+JUQH3k32jGIEpoHUNJ7UynPGBM9wSfnicR
11610	140.864397	192.168.200.55	199.192.17.8	United States	HTTP	239	GET /posg/?RVe07=inUGJBeDPN8D0y4t7THvzAB5qaCHmuO6qeRivoB4XaUYp
11612	141.228626	199.192.17.8	192.168.200.55	United States	HTTP	515	HTTP/1.1 404 Not Found (text/html)
12161	153.408497	192.168.200.55	37.123.118.150	United Kingdom	HTTP	232	GET /posg/?RVe07=oz5+CxsSQv+DQSFd2n1hM5SHg751h1Rq3pT7+KnI0hF7h
12163	153.665471	37.123.118.150	192.168.200.55	United Kingdom	HTTP	391	HTTP/1.1 403 Forbidden (text/html)
12183	158.907149	192.168.200.55	92.205.7.199	France	HTTP	238	GET /posg/?RVe07=2SDgxewiAHIHeb9NVep0fYVz+/nb9U27ULMOhmRZF8Ihf
12185	159.198558	92.205.7.199	192.168.200.55	France	HTTP	538	HTTP/1.1 301 Moved Permanently
15426	190.328341	192.168.200.55	154.23.170.189	United States	HTTP	233	GET /posg/?RVe07=m14LeIzuznjoF/Hgs2vsjZgHPXp4mwyToPngn0sPksS+M
15428	190.461983	154.23.170.189	192.168.200.55	United States	HTTP	468	HTTP/1.1 404 Not Found (text/html)
17425	195.511477	192.168.200.55	47.242.205.57	Hong Kong	HTTP	236	GET /posg/?RVe07=t/NymjUpuaLD1mR4G+w/dvwfa4zMuFr4+1dOBWu7SW9vz
17427	195.564478	47.242.205.57	192.168.200.55	Hong Kong	HTTP	343	HTTP/1.1 404 Not Found (text/html)
17893	200.566745	192.168.200.55	172.217.160.115	United States	HTTP	238	GET /posg/?RVe07=0ewOIJUiBrhQG8HREBZIT9RZRzEmmalcLppQkvyWhyJ6E
17895	200.574363	172.217.160.115	192.168.200.55	United States	HTTP	551	HTTP/1.1 302 Found (text/html)
17931	205.852051	192.168.200.55	188.165.33.127	France	HTTP	236	GET /posg/?RVe07=SF6dGwePBiXU2YDy8pBg8O1McfAnCuf37kbQ+Tv72jaoZ
17943	206.130001	188.165.33.127	192.168.200.55	France	HTTP	504	HTTP/1.1 404 Not Found (text/html)
17959	211.163394	192.168.200.55	23.227.38.74	Canada	HTTP	239	GET /posg/?RVe07=YnxWwuJkjw7/dCRerf4g7mcPecV4SPiQ15RS7qTroPdsn

圖 9-偽冒 "Statement of Account-Invoices Overdue" (逾期發票報表) 惡意程式大量產生 HTTP 資料傳送行為

感染檔案總管的惡意程式

異常 HTTP 通訊序列案例

研究組 整理編輯

惡意程式，特別是木馬類型程式(稱為 Trojan, 或是 RAT)，在網路安全封包分析技巧中，經常會出現某些明顯而特殊的網路封包模式。常見的明顯封包模式有: **(1) 固定間隔時間的反覆通訊連線**，**(2) 固定整點時間的回報連線**(Active Connection) 不論上述哪種模式，在 NSPA-Skill 分析技巧中，皆有詳細的解說與範例。

本文要介紹其中一種異常的反覆通訊模式: HTTP/HTTPS 的持續反覆連線模式。程式樣本 MD5-HASH 值為 1E737DD92AA48A779D2B9B394017603A。

這個惡意程式被歸類為 xloader 家族系列、Formbook 家族系列 或 AgentTesla 家族系列，具備 Stealer 與 KeyLogger 的竊取資料能力。它主要是透過電郵社交工程方式，由被害人在瀏覽電郵的時候，開啟附件檔案而感染惡意程式。該郵件的標題(或附件檔案)名稱為 "Statement of Account-Invoices Overdue" (逾期發票報表) 用來混淆電腦使用者，受害對象為財務會計人員[註 1]。

但是，這個惡意程式，卻是頻繁而大量連接到許多不同國家的 C&C 中繼跳板主機，堪稱獨樹一格。在 NSPA-Skill 網路安全封包分析技巧，可以使用下列過濾條件，在封包檔案顯現異常通訊的封包分析結果:

http and ((not (ip.src==內網網段 and ip.dst==內網網段)) and (not ip.geoip.asnum in {8068, 8070, 8075, 15169}))

各位可以在台灣 NSPA/NTPA 網站[註 2] 取得這個封包範例檔案，自行使用上述過濾規則，在 Wireshark 找到關鍵特徵封包，過濾後的呈現結果，請參考 圖 9 所示。(其中 ***內網網段*** 按照封包內容特性，應該置換為 192.168.0.0/16)

另外一個特殊之處在於，若財務會計人員不慎感這個偽冒報表的惡意程式，它將會隱身於 Windows Explorer 當中。也就是利用 Explorer.exe 對外部連接 HTTP 網站。

TCP	192.168.200.55:49345	40.79.197.35:443	TIME_WAIT	0	
TCP	192.168.200.55:49352	96.7.253.196:443	ESTABLISHED	916	
TCP	192.168.200.55:49361	154.86.195.215:80	TIME_WAIT	0	
TCP	192.168.200.55:49363	107.163.176.251:80	TIME_WAIT	0	
TCP	192.168.200.55:49364	107.163.176.251:80	TIME_WAIT	0	
TCP	192.168.200.55:49365	15.197.142.173:80	TIME_WAIT	0	
TCP	192.168.200.55:49369	173.231.37.38:80	TIME_WAIT	0	
TCP	192.168.200.55:49373	92.205.7.199:80	FIN_WAIT_2	1608	
TCP	192.168.200.55:49374	92.205.7.199:80	ESTABLISHED	1608	

svchost.exe	852	C:\Windows\System32\svchost.exe
svchost.exe	884	C:\Windows\System32\svchost.exe
svchost.exe	916	C:\Windows\System32\svchost.exe
svchost.exe	1036	C:\Windows\System32\svchost.exe
VSSVC.exe	1088	C:\Windows\System32\VSSVC.exe
spoolsv.exe	1160	C:\Windows\System32\spoolsv.exe
svchost.exe	1196	C:\Windows\System32\svchost.exe
mDNSRespond...	1260	C:\Program Files\Bonjour\mDNSResponder.exe
taskhost.exe	1316	C:\Windows\System32\taskhost.exe
taskeng.exe	1384	C:\Windows\System32\taskeng.exe
svchost.exe	1460	C:\Windows\System32\svchost.exe
dwm.exe	1552	C:\Windows\System32\dwm.exe
GoogleCrashHa...	1564	C:\Program Files (x86)\Google\Update\1.3.36.122\GoogleCrashHan...
explorer.exe	1608	C:\Windows\explorer.exe
QiyiService.exe...	1692	C:\Program Files (x86)\IQIYI Video\LStyle\7.2.102.1343\QiyiServ...
SearchFilterHos...	1728	C:\Windows\System32\SearchFilterHost.exe
RichVideo.exe ...	1860	C:\Program Files (x86)\CyberLink\Shared Files\RichVideo.exe

原本 Explorer.exe 的作用，在 Windows 系統是提供 Windows 檔案總管與視窗桌面服務，因此極少會看到 Explorer.exe 對外部連線，特別是 HTTP 通訊。不過，從 Windows 8 以後，微軟在桌面服務提供天氣資訊與新聞資訊，竟然就是使用 Windows Explorer 對外連線，容易造成判斷困難與混淆。

我們觀察這個惡意程式異常通訊封包，這些 C&C 中繼跳板網站資訊，例如圖 9 的封包編號 12183 與 12185 封包，連線到 92.205.7.199 位址。而在左方的通訊連線清單(從 netstat 指令獲得的清單)可以看到最底下兩項資訊，連接到 92.205.7.199 的 PID 為 1608，它就是 Explorer.exe。

舉例來說，HTTPS 在瀏覽器的封包序列，

以上這個過濾條件，會過濾出所有的非

HTTPS 封包分析

HTTPS 的關鍵是封包動作，而不是封包內容

劉得民

不論加密演算法使哪種方式，當網路封包內容被加密後， 多數封包分析方法或工具，會將焦點放置到「資料解密」的項目。從 TLS (HPPTS) 到 SOCKS，其中 Session Key、加解密金鑰或加密憑證，就是經常出現在網路安全封包分析的先決條件。

不過，針對惡意程式的網路通訊封包分析來說，如果遇到被加密的封包內容，而沒有取得 SSLKEYLOGFILE 或是 RSA Key List 的情況下，似乎就無法分析了?! 其實這個也未必盡然是如此。因為，絕大多數的惡意程式加密通訊行為與人類使用瀏覽器的加密通訊行為，封包序列次序通常不相同。

舉例來說，HTTPS 在瀏覽器的封包序列，有著人類明顯的行為模式-瀏覽時間的隨機性 (Randomization of Browsing Time) 這個隨機時間的特性，包括瀏覽時間(何時瀏覽)與閱讀時間、跳選其他網頁時間(間隔間距時間)。而惡意程式，特別是 Worm、RAT 與 Trojan 程式，它們的程式碼在通訊連線這一段落，已經是寫固定的程式碼，因此既使加上隨機休眠這樣的程式碼(例如: Sleep(Random(date-time)) 這樣的方式) 仍然會有某些程式碼制式的通訊行為。更何況，某些惡意程式的加密通訊演算法，是攻擊者自行撰寫的自訂加密演算，不是標準 TLS 或 SOCKS 演算法。

根據這個特性，我們可以專注於以下的過濾條件:

tcp and ((tcp.flags.syn==1 and tcp.flags.ack==0) or (tcp.flags.fin==1 or tcp.flags.reset==1)) and not tcp.port in (80, 8000, 8080)

以上這個過濾條件，會過濾出所有的非 80, 8000, 8080 的通訊封包，而且只會留下 TCP 連線與 TCP 斷線封包，通常是 TCP-443 與其他通訊連線。當然，上述條件沒有區分內網與外網。接著，我們可以增加外網通訊條件: not (ip.src==內網網段 and ip.dst==內網網段) 例如:

not (ip.src==10.0.0.0/8 and ip.dst==10.0.0.0/8)

過濾完成後，就可以計算每個 TCP 通訊的起始與結束時間，這就是 Session 時間值。另外，相同發送端 IP 位址與接收端 IP 位址，可以計算每次 TCP-SYN 的時間差距，這就是時間的間隔距離值。人類的隨機瀏覽行為，這兩種時間數值，與惡意程式通訊的時間數值，必不會相同。在布朗運動(維納過程)的隨機性與分形微分，有較多的討論。

密碼潑灑攻擊 Password Spraying Attacking

劉得民

網路安全中，暴力式密碼攻擊、字典式密碼攻擊、帳密撞庫攻擊，都是常見的攻擊手法。各種網路系統再登入的階段，會採用不同的方式阻擋這類帳密嘗試攻擊方法，例如多因子認證登入方式、或登入錯誤次數限制等等。不過，除了帳密撞庫攻擊之外，還有另外一種密碼攻擊方式，稱為「密碼潑灑攻擊 (Password Spraying Attacking)」其攻擊概念是：在 A 系統，針對不同帳號，反覆嘗試相同登入密碼，如圖 6 所示。

當被害人的密碼與攻擊者猜測的密碼相同，則該帳號便遭受入侵。如果遭遇密碼潑灑攻擊方式，網路系統採用「帳號登入錯誤次數限制方式」是無效的防禦偵測方式，原因是攻擊者針對每個帳號，只會攻擊 1 次而已。

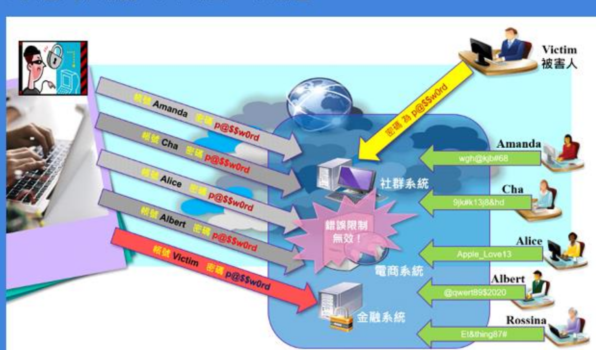


圖 6 -密碼潑灑攻擊

此份電子報檔案為網站閱讀版本，內容有縮減遮蔽。另有會員專用版本，內容為完整版本。