

SSL CBC 暴力破解帳號密碼 事件分析

資安事件名稱: SERVER-OTHER SSL CBC ENCRYPTION MODE
WEAKNESS BRUTE FORCE ATTEMPT

前言

- ASOC在三月份報告中，統計出**SSL CBC 暴力破解帳號密碼**事件量為當月第二名。
- 查詢開單系統紀錄中，此規則是去年12月月底才新增，而且1月、2月的事件量並非很多。

年份	月份	事件數量(單位:筆)
2017	12	5
2018	1	44
	2	22
	3	251
	4	350 (截至4/27統計)

IPS攔截封包紀錄

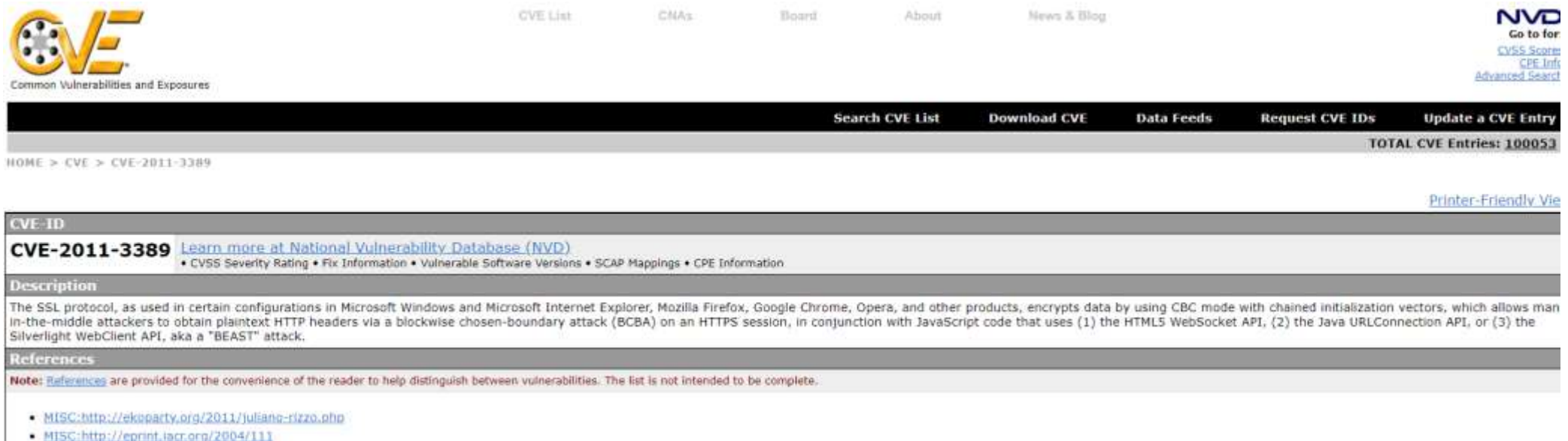
#	- Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	Message
#	2018-04-09 19:13:38	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64782 / tcp	55536 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 19:12:21	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64771 / tcp	55537 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 19:11:06	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64753 / tcp	55536 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 19:09:08	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64739 / tcp	55537 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 19:06:01	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64727 / tcp	55545 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 19:04:50	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64715 / tcp	55539 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 19:02:50	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64695 / tcp	55553 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 19:01:12	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64675 / tcp	55558 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 18:59:54	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64662 / tcp	55540 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 18:57:10	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64628 / tcp	55536 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 18:53:22	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64588 / tcp	55530 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 18:52:24	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64576 / tcp	55562 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 18:50:35	medium	0	↓	120.107.162.108	TWN	140.112.10.220	TWN	64557 / tcp	55547 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 12:10:25	medium	0	↓	140.335.57.230	TWN	140.112.254.38	TWN	64480 / tcp	83 (mit-ml-dev) / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 08:10:56	medium	0	↓	163.20.242.76	TWN	140.124.104.173	TWN	61612 / tcp	2092 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-09 08:04:22	medium	0	↓	163.20.242.76	TWN	140.124.104.173	TWN	61063 / tcp	2092 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-08 22:54:59	medium	0	↓	150.116.192.112	TWN	140.124.104.173	TWN	58655 / tcp	2365 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-05 01:50:09	medium	0	↓	118.150.148.22	TWN	203.64.154.27	TWN	20773 / tcp	2443 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-05 21:24:38	medium	0	↓	61.60.61.62	TWN	140.124.104.173	TWN	32143 / tcp	2094 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-05 21:10:12	medium	0	↓	61.60.61.62	TWN	140.124.104.173	TWN	48921 / tcp	2094 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-05 20:09:40	medium	0	↓	150.117.8.8	TWN	203.71.63.17	TWN	59037 / tcp	2205 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-05 19:51:14	medium	0	↓	150.117.8.8	TWN	203.71.63.17	TWN	58740 / tcp	2205 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-05 19:34:48	medium	0	↓	150.117.8.8	TWN	203.71.63.17	TWN	58336 / tcp	2205 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-05 19:22:55	medium	0	↓	150.117.8.8	TWN	203.71.63.17	TWN	57718 / tcp	2205 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force
#	2018-04-05 19:05:11	medium	0	↓	61.60.61.62	TWN	140.124.104.173	TWN	62966 / tcp	2094 / tcp	Unknown / Unknown	101	SERVER-OTHER SSL CBC encryption mode weakness brute force

事件分析

CVE弱點描述

◆此事件是跟CVE-2011-3389相關:

1. 使用CBC加密模式時，因SSL 3.0和TLS 1.0 舊版通訊協定中的設計缺點，所造成資訊洩漏的問題，這個弱點會使加密的 SSL/TLS 流量遭到解密
2. 瀏覽器(IE, Firefox, Chrome, Opera等)為主要攻擊媒介
3. 此弱點又稱為BEAST Attack (Browser Exploit Against SSL/TLS Attack，野獸攻擊)



The screenshot shows the NVD entry for CVE-2011-3389. The page includes a navigation bar with links for CVE List, CNAs, Board, About, and News & Blog. A search bar is located at the top right, and a navigation menu at the bottom contains links for Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. The main content area displays the CVE ID, a link to learn more at the NVD, and a description of the vulnerability. The description states that the SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack. The page also includes a references section with links to external sources.

CVE ID
CVE-2011-3389 [Learn more at National Vulnerability Database \(NVD\)](#)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

References
Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- [MISC:http://ekoparty.org/2011/juliano-rizzo.php](http://ekoparty.org/2011/juliano-rizzo.php)
- [MISC:http://eprint.iacr.org/2004/111](http://eprint.iacr.org/2004/111)

IPS偵測規則 (snort id:20212)

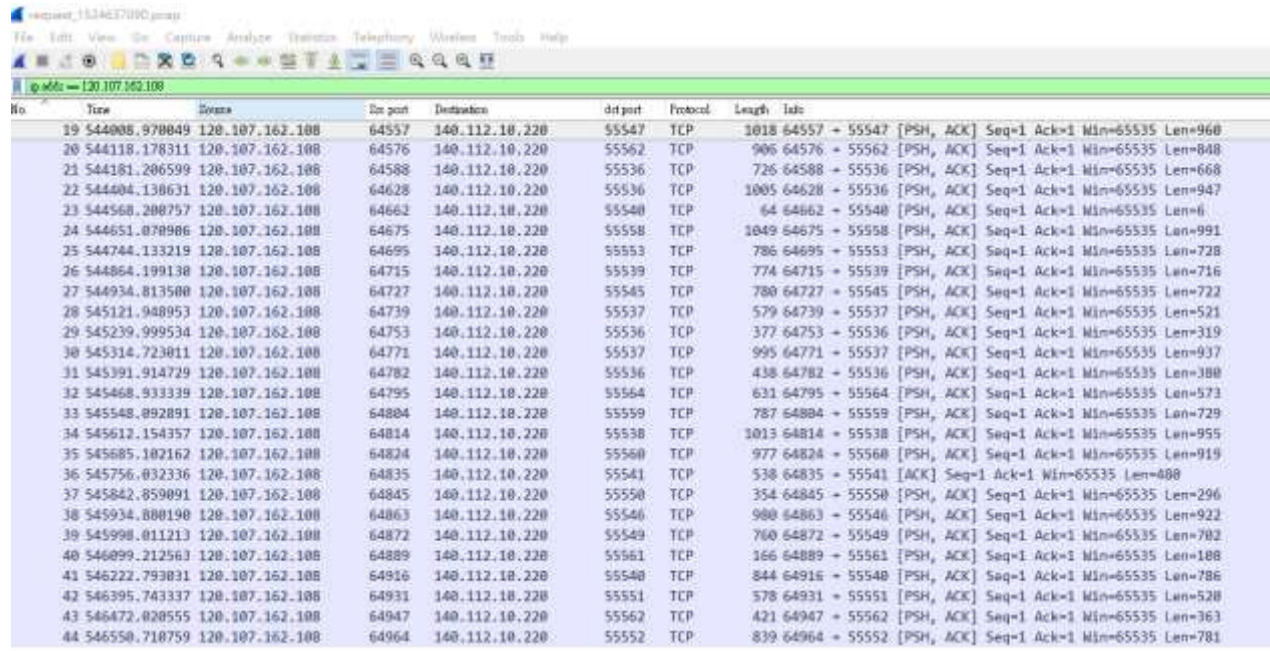
1. 外對內攻擊
2. 跟行為有關:在短時間內的連線次數大於某個門檻值以上 (非正常連線行為)
3. 跟封包內容無關:規則說明中沒有提到封包內容要符合任何關鍵字

IPS記錄的封包

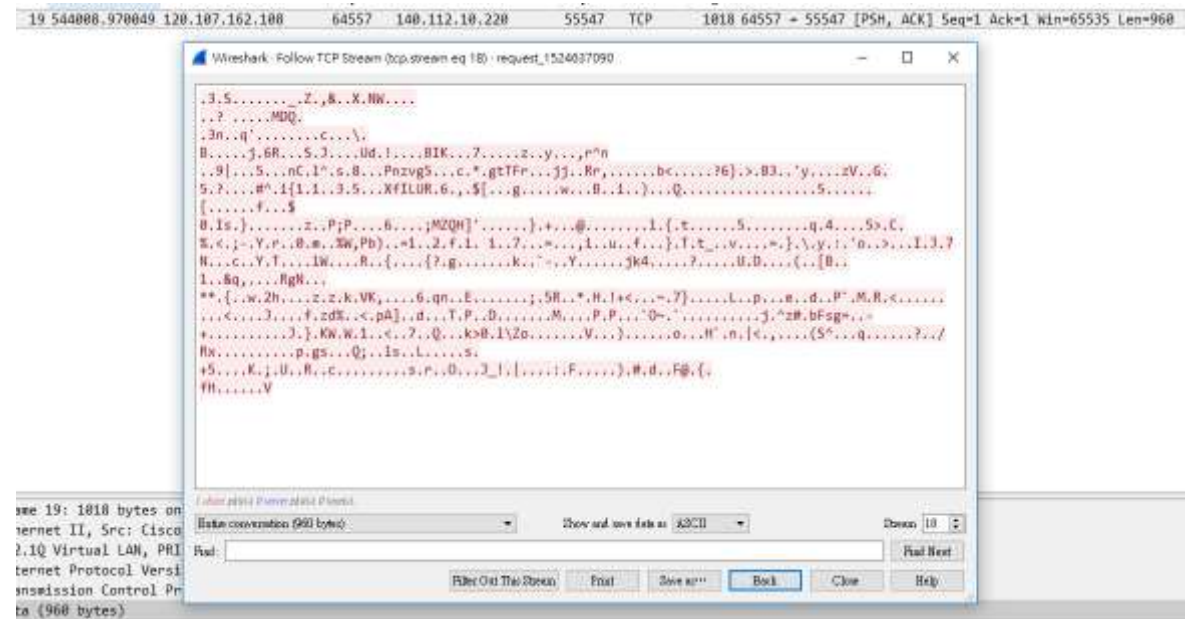
- IPS只能檢查未加密的封包內容
- IPS會根據規則，把符合規則條件的封包做阻擋並記錄
- 從IPS下載此事件封包，觀察被記錄的封包內容

封包內容

- 可參考下面兩張圖



No.	Time	Source	Src port	Destination	dst port	Protocol	Length	Info
19	544008.970049	120.107.162.100	64557	140.112.10.220	55547	TCP	1018	64557 → 55547 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=960
20	544118.178311	120.107.162.100	64576	140.112.10.220	55562	TCP	906	64576 → 55562 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=840
21	544181.206599	120.107.162.100	64588	140.112.10.220	55536	TCP	726	64588 → 55536 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=668
22	544404.130631	120.107.162.100	64628	140.112.10.220	55536	TCP	1005	64628 → 55536 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=947
23	544568.200757	120.107.162.100	64662	140.112.10.220	55540	TCP	64	64662 → 55540 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=6
24	544651.070906	120.107.162.100	64675	140.112.10.220	55558	TCP	1049	64675 → 55558 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=991
25	544744.133219	120.107.162.100	64695	140.112.10.220	55553	TCP	786	64695 → 55553 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=728
26	544864.199130	120.107.162.100	64715	140.112.10.220	55539	TCP	774	64715 → 55539 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=716
27	544934.813500	120.107.162.100	64727	140.112.10.220	55545	TCP	780	64727 → 55545 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=722
28	545121.940953	120.107.162.100	64739	140.112.10.220	55537	TCP	579	64739 → 55537 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=521
29	545239.999534	120.107.162.100	64753	140.112.10.220	55536	TCP	377	64753 → 55536 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=319
30	545314.723011	120.107.162.100	64771	140.112.10.220	55537	TCP	995	64771 → 55537 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=937
31	545391.914729	120.107.162.100	64782	140.112.10.220	55536	TCP	438	64782 → 55536 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=380
32	545468.933339	120.107.162.100	64795	140.112.10.220	55564	TCP	631	64795 → 55564 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=573
33	545548.892091	120.107.162.100	64804	140.112.10.220	55559	TCP	787	64804 → 55559 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=729
34	545612.154357	120.107.162.100	64814	140.112.10.220	55538	TCP	1013	64814 → 55538 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=955
35	545685.102162	120.107.162.100	64824	140.112.10.220	55560	TCP	977	64824 → 55560 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=919
36	545756.032336	120.107.162.100	64835	140.112.10.220	55541	TCP	538	64835 → 55541 [ACK] Seq=1 Ack=1 Win=65535 Len=400
37	545842.859091	120.107.162.100	64845	140.112.10.220	55550	TCP	354	64845 → 55550 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=296
38	545934.880190	120.107.162.100	64863	140.112.10.220	55546	TCP	980	64863 → 55546 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=922
39	545998.011213	120.107.162.100	64872	140.112.10.220	55549	TCP	760	64872 → 55549 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=702
40	546099.212563	120.107.162.100	64889	140.112.10.220	55561	TCP	166	64889 → 55561 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=108
41	546222.793031	120.107.162.100	64916	140.112.10.220	55540	TCP	844	64916 → 55540 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=786
42	546395.743337	120.107.162.100	64931	140.112.10.220	55551	TCP	378	64931 → 55551 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=520
43	546472.020555	120.107.162.100	64947	140.112.10.220	55562	TCP	421	64947 → 55562 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=363
44	546550.710759	120.107.162.100	64964	140.112.10.220	55552	TCP	839	64964 → 55552 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=781



19 544008.970049 120.107.162.100 64557 140.112.10.220 55547 TCP 1018 64557 → 55547 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=960

Wireshark - Follow TCP Stream (tcp.stream eq 18) - request_1524037090

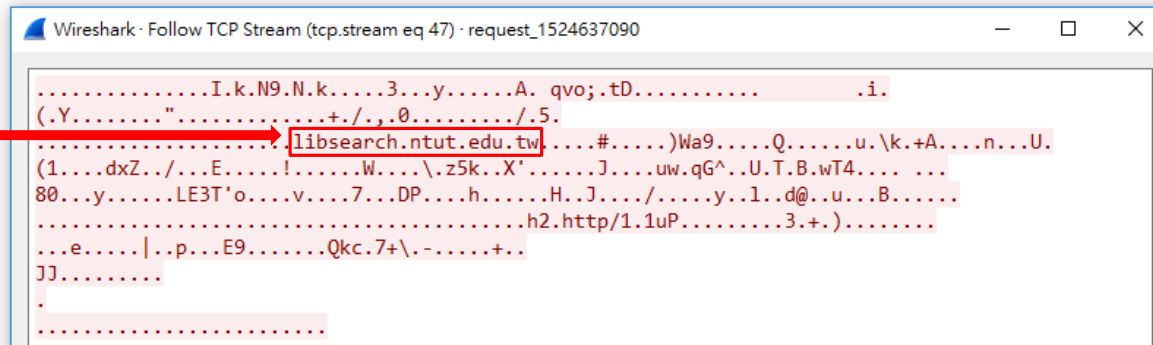
```
..3.S.....Z.,&..X.NW...  
...?.....MDQ...  
..3n..q'.....c...  
B.....j.6R...S.J....Ud.I....BIK...7.....z.y...p^n  
..9]...S...nC.I'..s.B...Pnzvg5...c.*.gtTFr...jj..Rr.....bc.....?6).>.B3...y...zV...G.  
5..?.....H'.1{.1..1.3.5...XFLUR.6.,,$[...g.....w...B...1...}...Q.....5.....  
[.....f...$  
B..Is.).....z...P;P...B...;MZQH'.....}...@.....1.[.t.....5.....q.4.....S>.C.  
%<.j..Y..P...0.m..Xw(Pb)...=1..2.f.l..1..?..&...;L...u...f...;l.t...v...>}.y...n...>...I.3.7  
H...c..Y..f...1W...R...{...{?g.....k...}...Y.....3K4.....?.....U.D...{...{B...  
1..Bq.....RgM...  
**.{...w.2h...z.z.k.VK.....6.qm..E.....;5H...*..H..1<...7).....L..p...m...d..P'..M.R.<.....  
<<...3...J...f.zdK.<.pA],d...T.P...D.....M...P...P...0...}.....3..*zW..bFsg...=  
+.....{...}.KN.W.1...<.7..Q...k>B.LY2o.....V...}.....o...H'..n[<.....(S<...Q.....?</  
Rk.....p.g...Q;...l...L.....S.  
+S...K;..l..U..R...C.....s.P...D...2_l|.....;F.....;W..d..F@..{  
FH.....V
```

Packet 19: 1818 bytes on interface II, Src: Cisco 2.1Q Virtual LAN, Prio: 0, Dst: 140.112.10.220, Len: 960

分析封包

- 幾乎大部分的封包內容是沒有特定的特徵值
- 極少數的封包有殘留的關鍵字(如下圖，此種封包數量約10~20個，約3%~6%)
- 查詢下圖關鍵字，會連線到台北科技大學圖書館登入頁面；連線到此IP也會是同個畫面

Time	Source	Src port	Destination	dst port	Protocol	Length	Info
48	552160.165090	61.60.61.62	140.124.104.173	2094	TCP	575	36856 → 2094 [PSH, ACK] Seq=1 Ack=



結論

- 依照目前現有的證據推論：
 1. 此資安事件名稱**命名不精準**，會有誤導處理資安事件的方向；可能是因為以CVE-2011-3389弱點描述而命名此規則
 2. ASOC認為此事件處理方向要從觸發規則條件著手，本事件重點在**試圖暴力破解帳號密碼**
 3. 要關注在**連線行為**上，會**短時間內的大量連線**到網頁不是正常使用網路行為

建議

- 更新作業系統與瀏覽器到最新版本
- 如果觸發本資安事件，請使用者先使用防毒軟體掃描電腦主機
- 檢查正在使用的程式是否會產生大量連線的行為
- 檢查自身使用電腦的習慣

資料來源

- 1) <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2011-3389>
- 2) <https://docs.microsoft.com/zh-tw/security-updates/SecurityAdvisories/2011/2588513>
- 3) <https://docs.microsoft.com/zh-tw/security-updates/SecurityBulletins/2012/ms12-006>
- 4) <https://vnhacker.blogspot.tw/2011/09/beast.html>
- 5) <http://securityalley.blogspot.tw/2014/07/ssltls-beast.html>