

區網網管會議

臺灣大學計資中心

李美雯

mli@ntu.edu.tw

3366-5010

2016/11/11



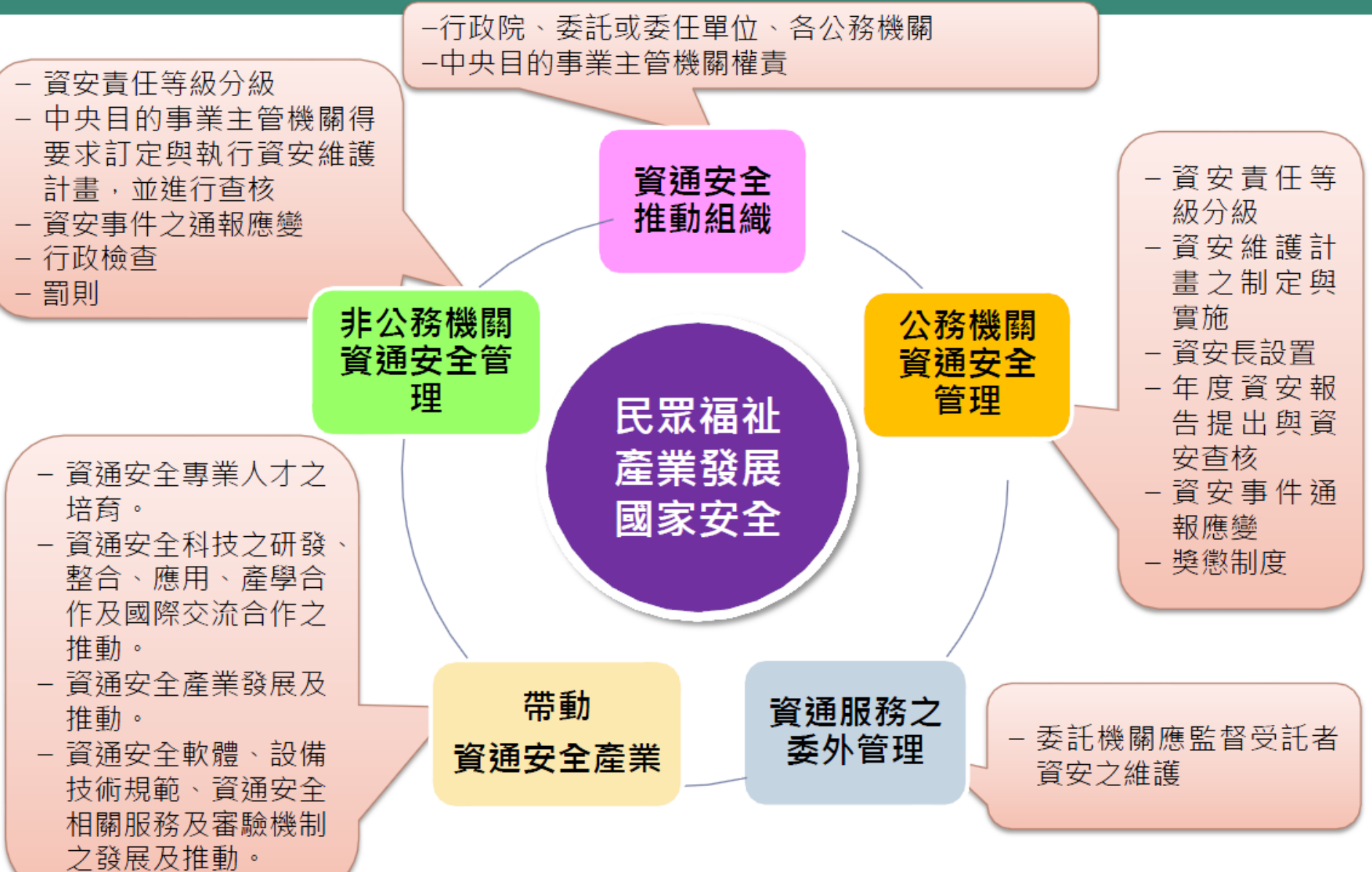
主管機關政策討論

資通安全管理法草案





法規要點





整體架構

❖ 本法以資通安全管理為核心，分為5個章節，計24條

資通安全管理法草案

第1章 總則(§1~§8)

立法目的、名詞定義、資通安全產業之推動、行政院職責、幕僚任務委任或委託、資安責任等級分級、情資分享機制、資通委外監督

第2章 公務機關資通安全管理(§9~§14)

資通安全管理與維護計畫、資通安全長之設置、年度資通安全報告之提出、資通安全查核、通報應變措施、獎懲措施

第3章 非公務機關資通安全管理(§15~§18)

關鍵基礎設施提供者資通安全維護之管理與監督、受指定之非公務機關所提供之產品或服務資通安全管理之管理與監督、資通安全事件通報應變、行政檢查

第4章 罰則(§19~§22)

行政處分

第5章 附則(§23~§24)

施行細則授權、施行日期

資通安全事件情資分享機制



情資分享

資通安全事件通報機制

其他情資



行政院建立資通安全情資分享機制

行政院、上級機關

中央目的事業主管機關

經濟部、金管會、交通部、通傳會...等

公務機關資通安全事件通報(\$13)(強制通報)



公務機關

非公務機關資通安全事件通報(\$17)(強制通報)



關鍵基礎設施提供者



+ 適用資安責任等級分級及受指定之非公務機關之產品或服務

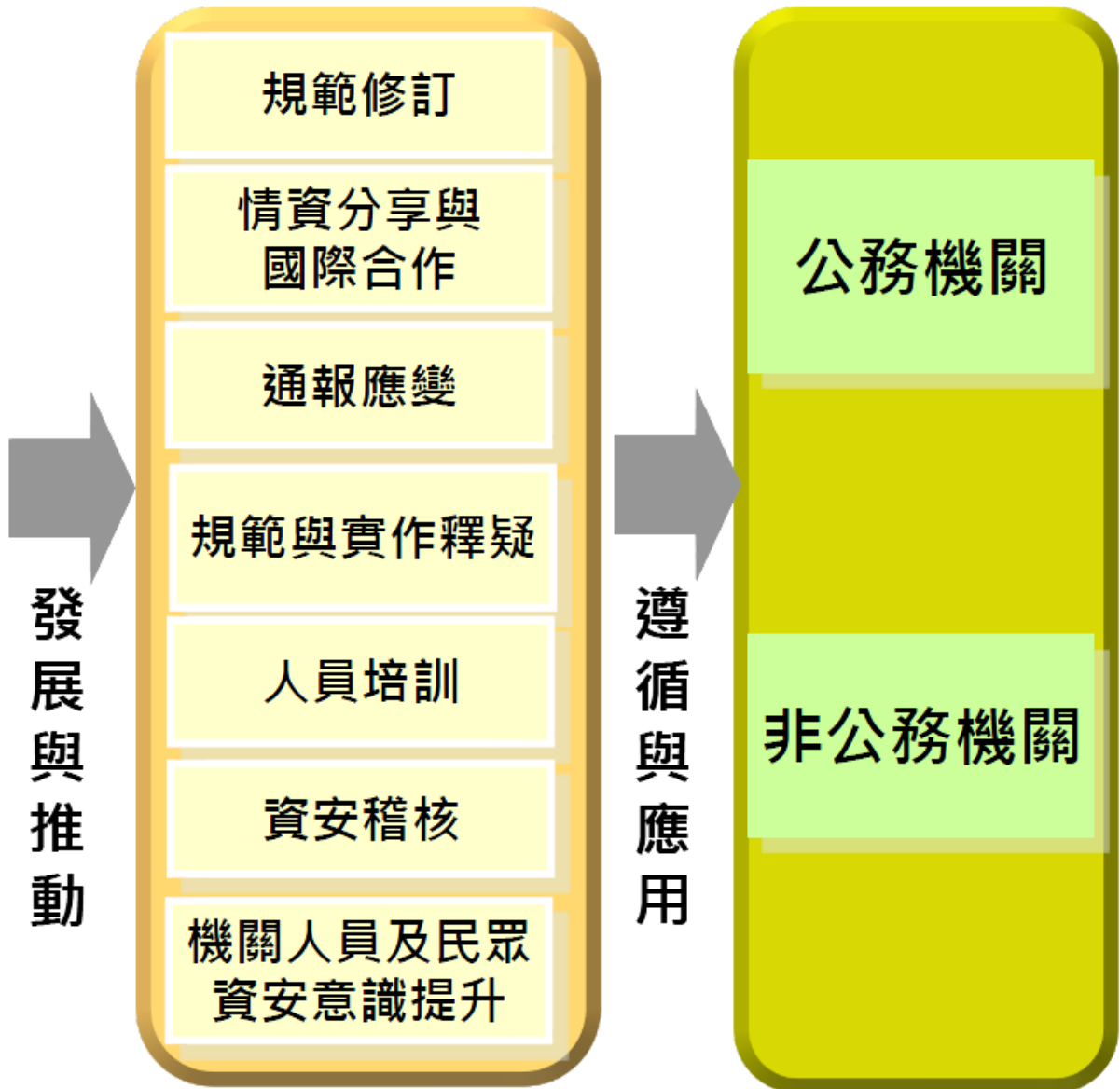
非公務機關資通安全事件通報(自願通報)



所有非公務機關



資通安全管理法推動措施





資安案例分享

關鍵基礎建設SCADA系統

烏克蘭發電廠遭駭



烏克蘭緊急電腦應變中心

(Ukrainian CERT)證實了在2015年12月23日的發電廠停電事件，是由Black Energy攻擊所致，此事件造成烏克蘭局部地區停電將近六小時，約有七萬人受到影響。

資安攻擊未來趨勢-

關鍵基礎建設SCADA系統(續)

某自來水廠遭駭



資安業者Verizon Security在其年度報告中揭露，某自來水廠遭受網路攻擊，透過SQL injection等手法，成功感染廠中AS/400等工業用主機，並已成功取得自來水廠中各種控制器的控制權，但因不慎誤觸警報，才導致自來水廠運作中斷，進而驚覺遭駭。

資安攻擊未來趨勢-

關鍵基礎建設SCADA系統(續)

台灣國家級資安演練納入核電廠



針對未來趨勢，目前政府機關每年資安攻防演練亦將重要基礎設施納入演練範圍，透過實際演練尋找是否存在關鍵弱點，找出潛藏的資安風險。

資安攻擊未來趨勢-

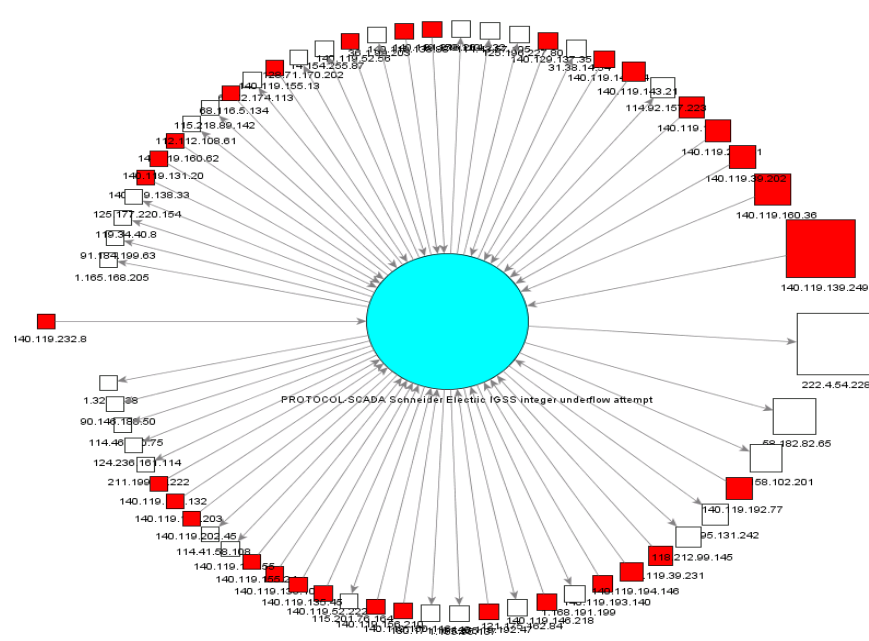
關鍵基礎建設SCADA系統(續)

SCADA系統資安防範範疇



- 1.)重要SCADA系統若需聯網，則需透過防火牆嚴格控管。
- 2.)落實內部系統高強度密碼及定期更換密碼的安全性原則。
- 3.)若系統為封閉環境，仍須留意是否有實體資料交換的可能性(USB)。
- 4.)定期稽核系統各項參數及設定是否出現異常。
- 5.)定期進行內部資安演練，強化資安意識。

關鍵基礎建設SCADA系統(續)

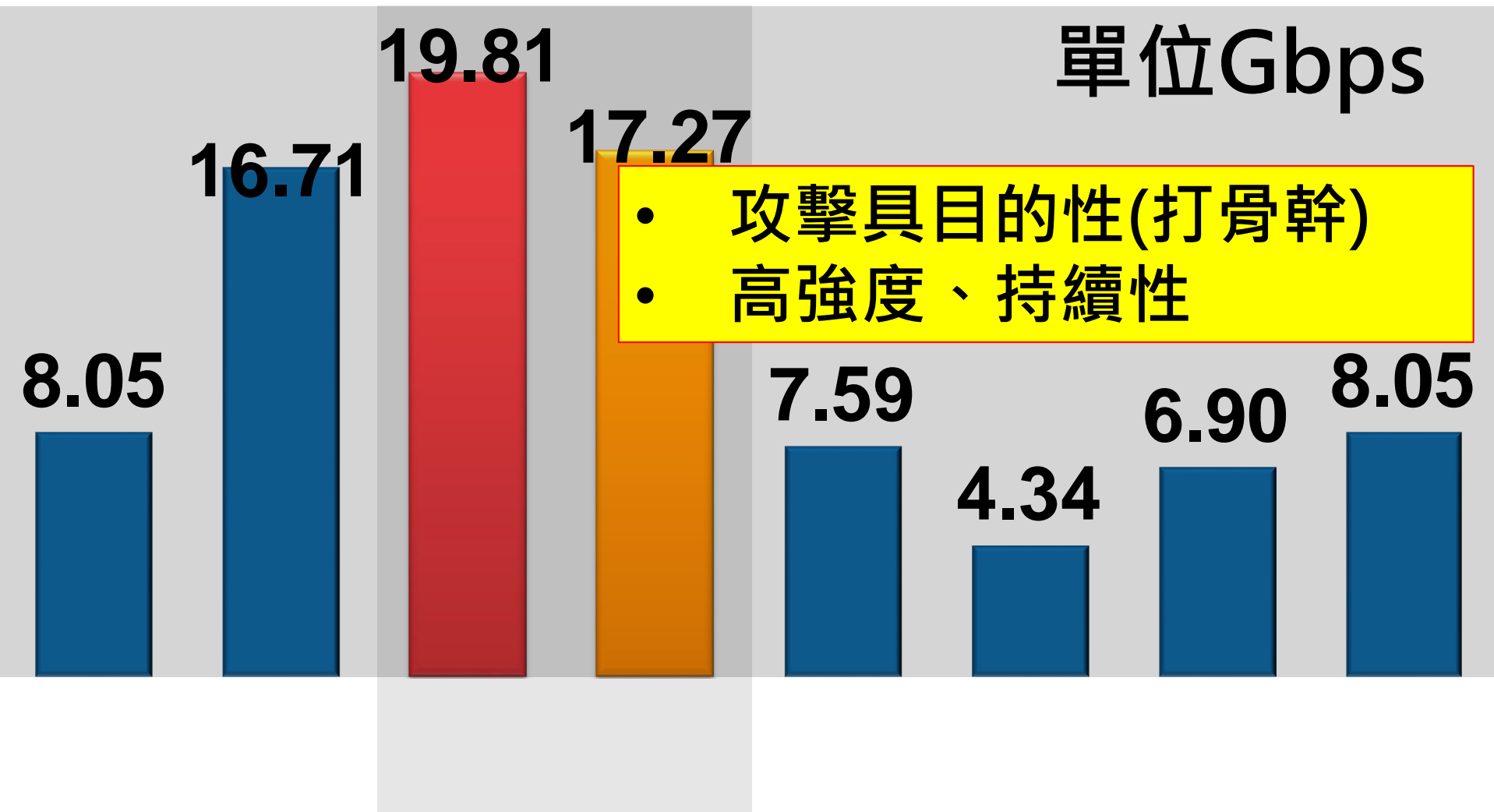


目前北區ASOC針對SCADA系統攻擊事件，相關規則已有247條，並持續更新中，而在各轄下單位的流量中，亦偵測到不少針對SCADA系統的緩衝區溢位攻擊，顯示潛在風險確實存在，加上SCADA系統多半位屬重要設施，因此對於此類型攻擊更須提高警覺。

十大 DDOS 事件

每日最大單筆攻擊

單位 Gbps

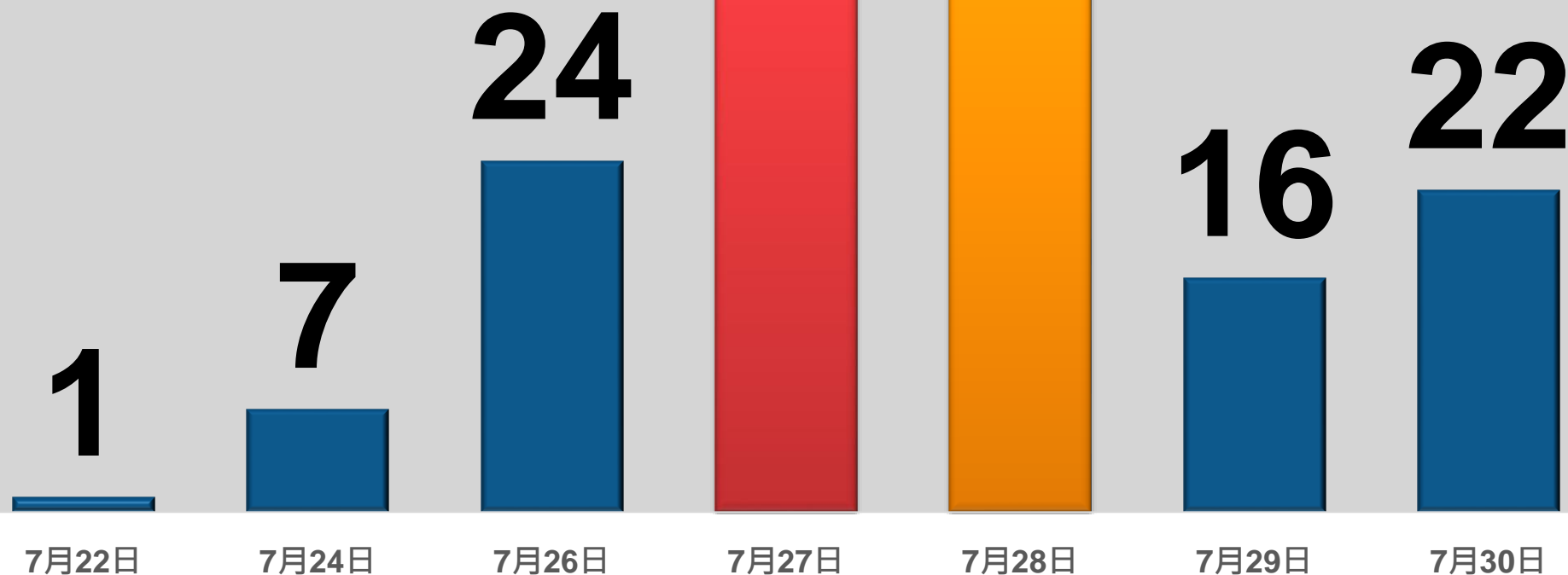


○大 DDOS事件

毎日攻撃次數

高密度強攻：
單日最高48次

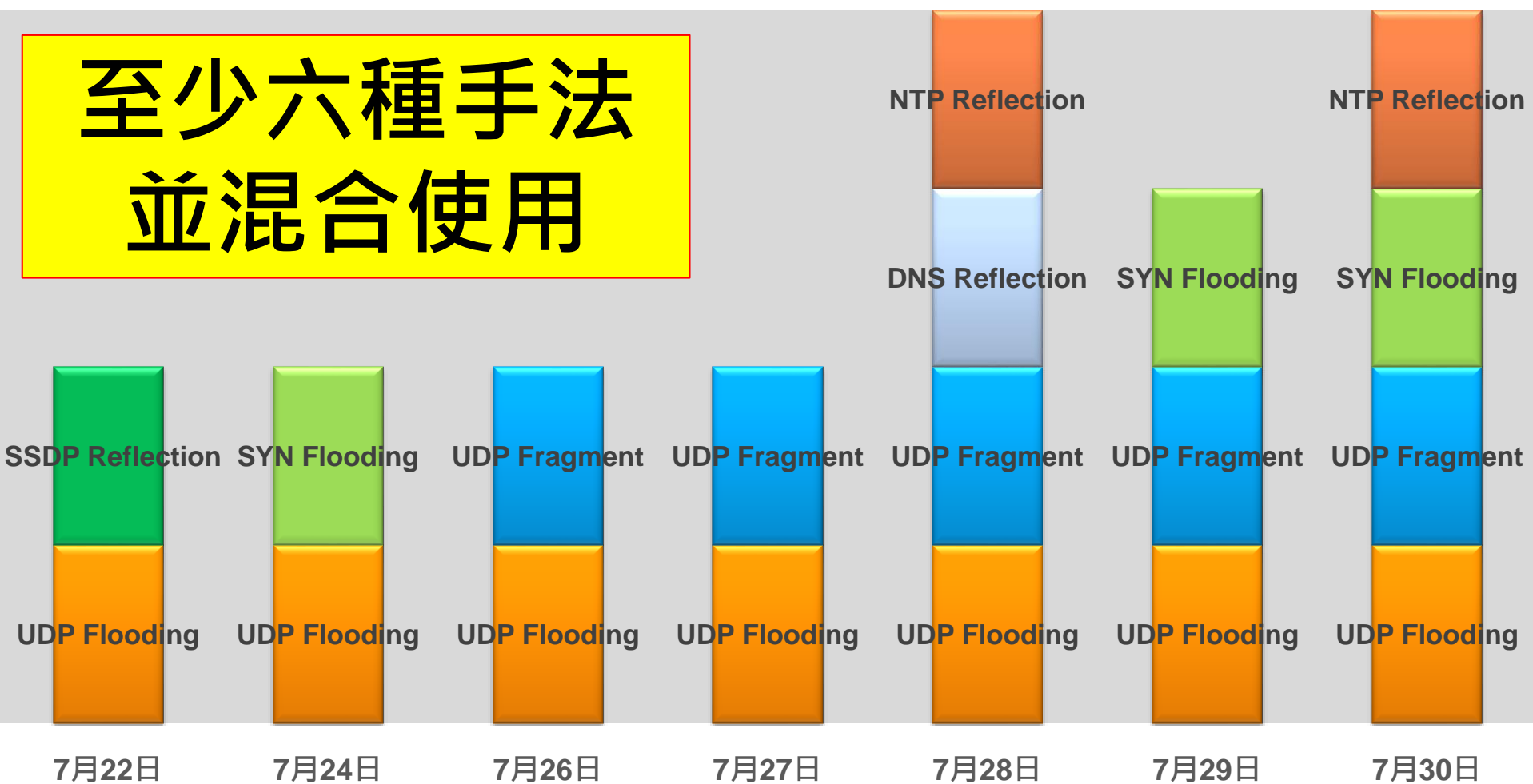
單位(次)



○大 DDOS事件

每日攻擊手法

至少六種手法
並混合使用



○大 DDOS事件

攻擊手法說明

直接式攻擊

UDP
Flooding

本次攻擊
最大流量
達到
19.81
Gbps

UDP
Fragment

以大量
UDP
Fragment
封包直接
塞滿頻寬

SYN
Flooding

此次攻擊
中混雜了
SYN-ACK
Flood與
ACK
Flood

反射式攻擊

SSDP
Reflection

放大倍數
可達到近
30倍左右

DNS
Reflection

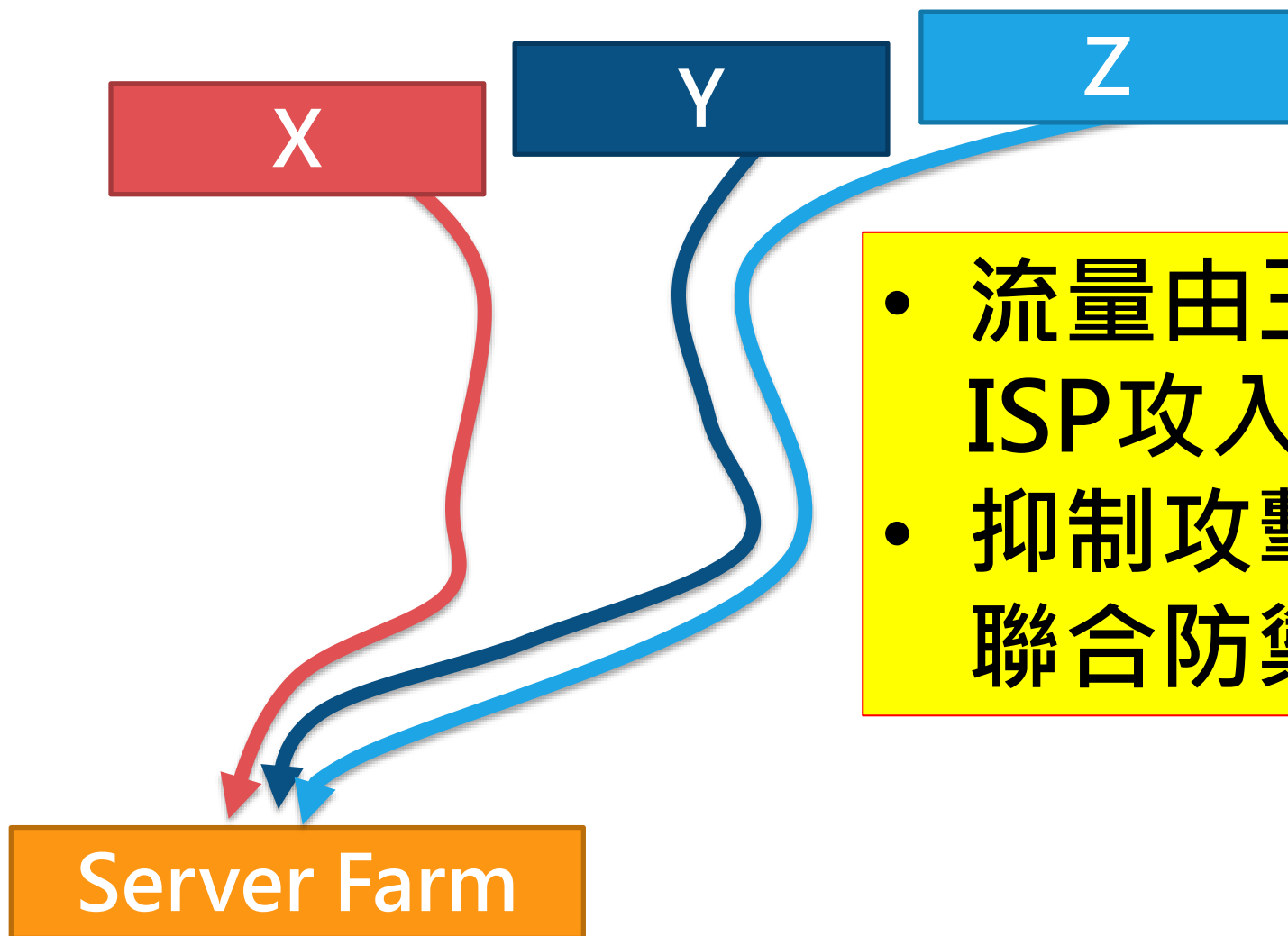
放大倍數
最高可達
到近100
倍左右

NTP
Reflection

放大倍數
最高可達
到近200
倍左右

○大 DDOS事件

攻擊路徑說明



- 流量由三家ISP攻入
- 抑制攻擊：聯合防禦

O大 DDOS事件 小結



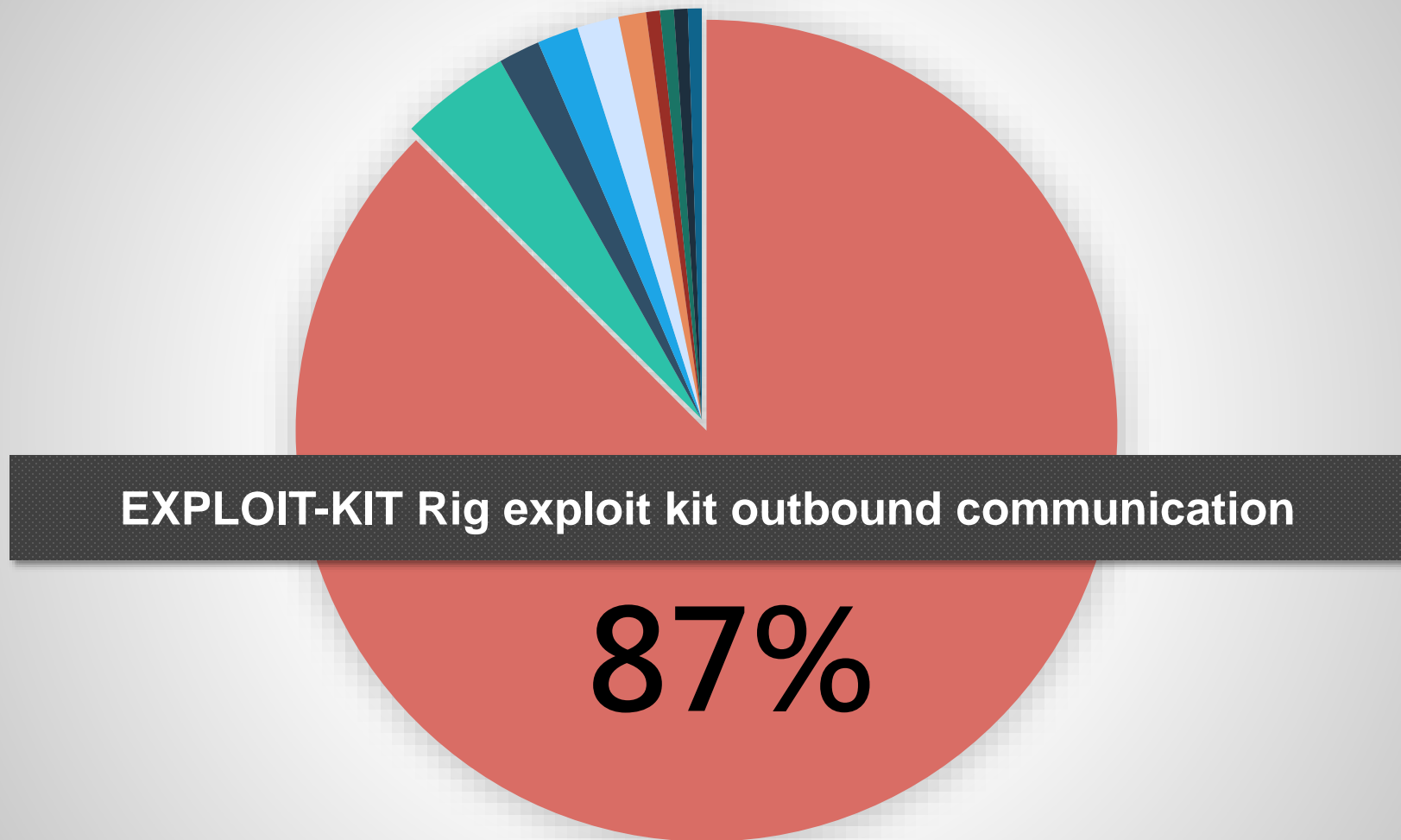
Tsunami Damage

Source: Wren & Brown (2013)

- DDOS攻擊具目的性、高密度、強度、持續性
- O大事件：連續攻擊七日，並攻擊網路骨幹
- 攻擊手法具多樣性，並混合正常流量，需分析後再處理，避免誤判
- O大事件：混合六種手法
- 攻擊抑制需聯合防禦整合邊境路由器與上游ISP
- O大事件：三家ISP攻入

重大資安事件統計-Rig Exploit kit

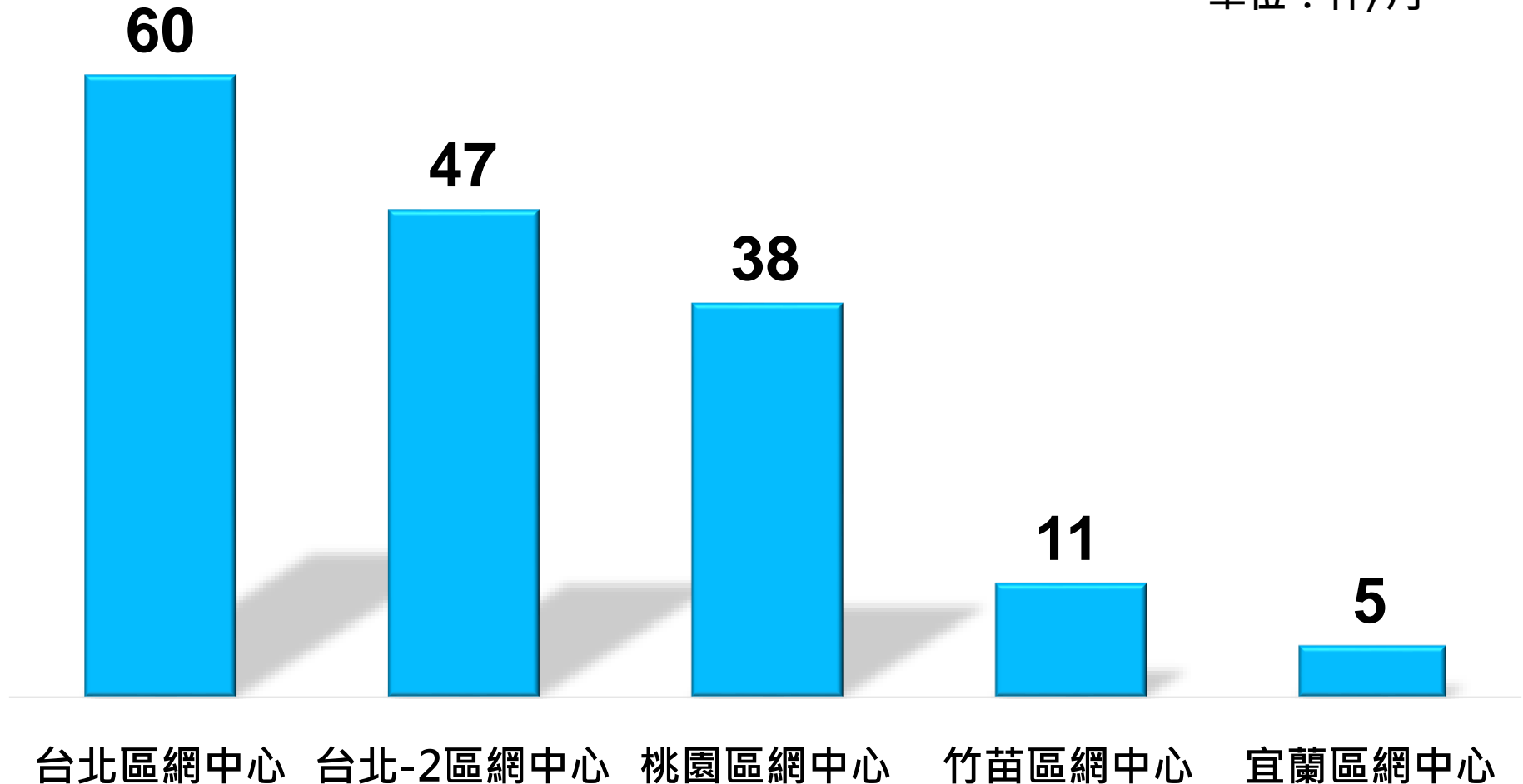
九月份七大區網中心
EXPLOIT-KIT(攻擊套件)類型事件概況



重大資安事件統計-Rig Exploit kit (續)

本月份各區網 Rig Exploit kit 感染概況

單位：件/月



重大資安事件統計-Rig Exploit kit (續)

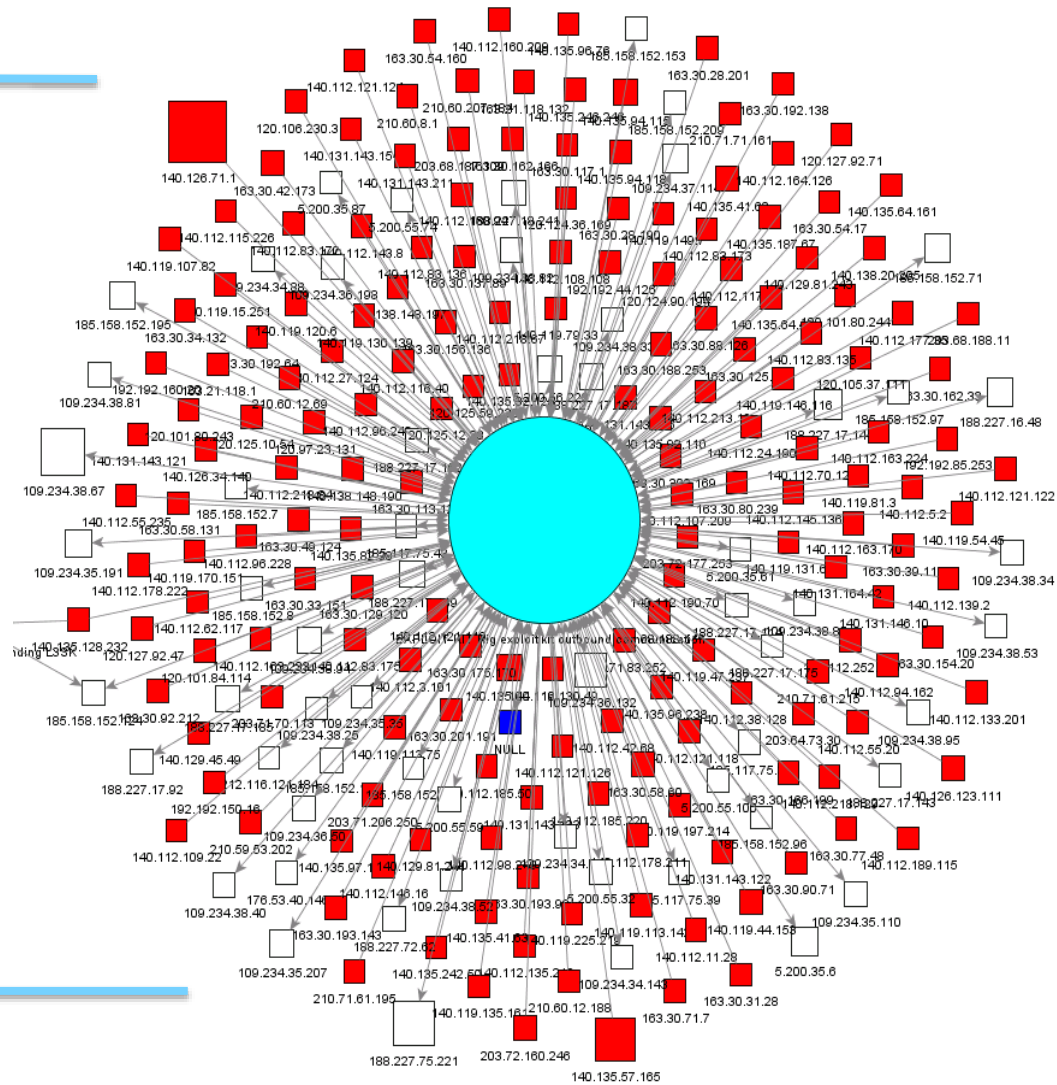
北區ASOC於八月份觀

察到各區網中心出現大量Rig

Exploit kit事件，多為學術網

路內已遭感染之主機嘗試對

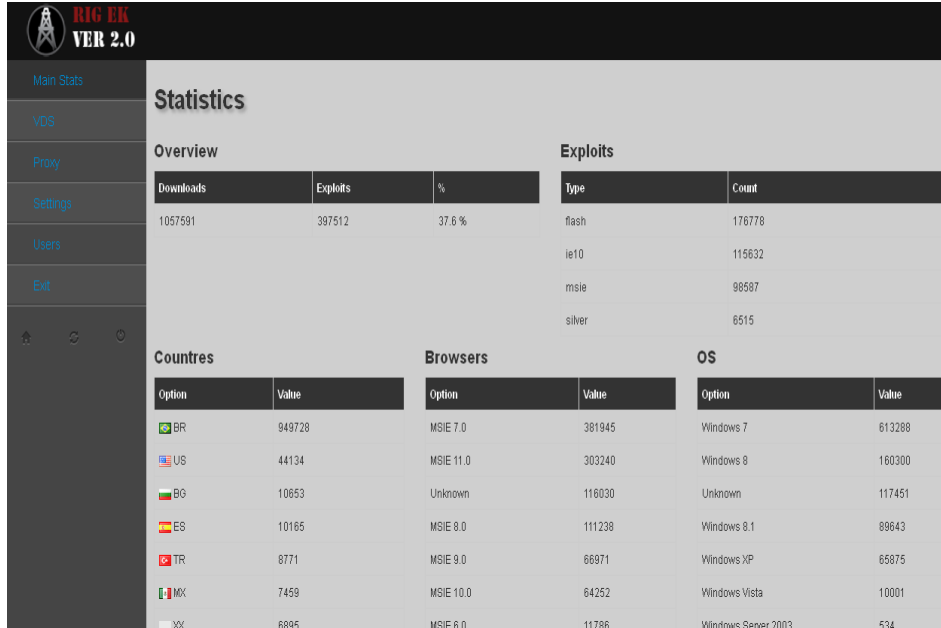
外連線而觸發規則。



重大資安事件統計-Rig Exploit kit (續)

Rig Exploit kit 簡介

攻擊者從Rig exploit操作介面可以得知目前感染概況，包括感染人數、國家、瀏覽器、作業系統等資訊，同時也能得知各種漏洞使用率。



The screenshot shows the Rig Exploit kit interface. On the left is a sidebar with navigation links: Main Stats, vDS, Proxy, Settings, Users, and Exit. The main content area is titled 'Statistics' and contains an 'Overview' section with three tables: Downloads, Exploits, and %. The Downloads table shows 1057591 downloads, the Exploits table shows 397512 exploits, and the % table shows 37.6%. Below the Overview section are three tables: Countries, Browsers, and OS, each with two columns: Option and Value.

Downloads		Exploits		%	
1057591	397512	37.6 %			

Countries	
Option	Value
BR	949728
US	44134
BG	10853
ES	10165
TR	8771
MX	7459
XX	6895

Browsers	
Option	Value
MSIE 7.0	381945
MSIE 11.0	303240
Unknown	116030
MSIE 8.0	111238
MSIE 9.0	66971
MSIE 10.0	64252
MSIE 6.0	11786

OS	
Option	Value
Windows 7	813288
Windows 8	160300
Unknown	117451
Windows 8.1	89643
Windows XP	65875
Windows Vista	10001
Windows Server 2003	534

Rig Exploit kit是漏洞攻擊套件的一種，含有多種漏洞攻擊模組，而Rig Exploit主要攻擊路徑有下列兩種：

- 針對各種內容管理系統 (WordPress、Joomla和Drupal)這些內容管理系統或其plugin存在弱點，可以讓攻擊者插入惡意代碼，藉此轉導到惡意網站並植入惡意程式
- 以購買廣告的方式，於檔案下載網站或色情網站置入大量的廣告視窗，一旦使用者點擊，隨即被轉導至惡意網站，並利用攻擊模組發動攻擊

重大資安事件統計-Rig Exploit kit (續)

Rig Exploit kit 主要目標



販售DDoS攻擊流量



竊取本機機敏資訊



重大資安事件統計-Rig Exploit kit (續)

應變措施



- 利用IPS偵測、阻擋攻擊封包
- 透過INT事件單對已感染主機提出告警
- 彙整相關資料提交TACERT

史上最大DDoS攻擊來襲



法國的網站代管服務供應商OVH在9月中遭到大規模的分散式阻斷服務攻擊（DDoS），其顛峰攻擊流量接近1Tbps，為目前史上最大的DDoS攻擊。

經觀察分析，該攻擊是經由近14萬台的攝影機與監視器（IOT）所組成的殭屍網路進行發動，而多數的攻擊流量來自亞洲，包含中國、南韓、台灣與越南等國的攻擊流量。

TANet IOT 資安事件分析

Stream Content

1 /hi_cloudflare_guys.i_think_u_offer_best_protection_srsly_so_hard_to_fuck_it HTTP/1.1

Connection: close

Host:

2 Cookie: __cfduid=d151d269c05aebb056d00336e40c692a51475885755; cf_clearance=b0ee8669d08d839542875ee39eedbebbff87796b-1475885759-900;

User-Agent: Tantric DDoS fucked your server :)

Content-Length: 800000

3 [REDACTED]

Date: Sat, 08 Oct 2016 00:16:57 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: close

Cache-Control: max-age=15

Expires: Sat, 08 Oct 2016 00:17:12 GMT

X-Frame-Options: SAMEORIGIN

Server: cloudflare-nginx

CF-RAY: 2ee5683161a90663-SJC

10f3

<!DOCTYPE html>

<!--[if lt IE 7]> <html class="no-js ie6 old">

<!--[if IE 7]> <html class="no-js ie7 old">

<!--[if IE 8]> <html class="no-js ie8 old">

<!--[if gt IE 8]><!--> <html class="no-js" >

<head>

<title>Attention Required! | CloudFlare</tit

<meta charset="UTF-8" />

<meta http-equiv="Content-Type" content="tex

<meta http-equiv="X-UA-Compatible" content="

<meta name="robots" content="noindex, nofol

<meta name="viewport" content="width=device-

<link rel="stylesheet" id="cf_styles-css" hr

<!--[if lt IE 9]><link rel="stylesheet" id="

[endif]>>

<style type="text/css">body{margin:0;padding

<!--[if lte IE 9]><script type="text/javascript" src="/cdn-cgi/scripts/jquery.min.js"></script><![endif]>>

<!--[if gte IE 10]><!--><script type="text/javascript" src="/cdn-cgi/scripts/zepto.min.js"></script><!--<![endif]>>

<script type="text/javascript" src="/cdn-cgi/scripts/cf.common.js"></script>

</head>

進一步分析封包後，確認為設備遭入侵並利用發動DDoS攻擊，並觀察到幾個特點：

1.)攻擊者於封包中留下挑釁的字眼

2.)利用超長content-length欄位進行第七層的攻擊

3.)於http封包中塞滿垃圾字串，藉此癱瘓服務

TANet IOT 資安事件分析

140.112

```
@@@FILE -> ../../Source/TransportServer.cpp, LINE -> 558Transport: CPacket Invalid
failed
login(root, *****, Console, address:)
user:root account invalid
User not valid!
user name:HTTPD: fd: 331, IP: 0x6503708c
HTTPD: invalid request
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: Begin web download
HTTPD: Web download ok
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: Begin web download
HTTPD: Web download ok
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: Begin web download
HTTPD: Web download ok
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
recv: No such file or directory
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: Begin web download
HTTPD: Web download ok
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
HTTPD: fd: 331, IP: 0x6503708c
```

雖然設備已遭入侵且竄改密碼，但透過TELNET方式，在未登入的狀態下，依然可以看到攻擊者透過IOT設備對外發動攻擊的紀錄

TANet IOT 資安事件分析

Stream Content

```
GET /hi_cloudflare_guys.i_think_u_offer_best_protection_srsly_so_hard_to_fuck_it HTTP/1.1
```

Connection: close

Cookie: __cfduid=d151d269c05aebb056d00336e40c692a51475885755; cf_clearance=b0ee8669d08d839542875ee39eedbebbff87796b-1475885759-900;

```
User-Agent: Tantric DDoS fucked your server :)
```

Content-Length: 800000

[illegible]

Date: Sat, 08 Oct 2016 00:16:57 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: close

```
Cache-Control: max-age=15
```

Expires: Sat, 08 Oct 2016 00:17:12 GMT

X-Frame-Options: SAMEORIGIN

```
Server: cloudflare-nginx
```

CF-RAY: 2ee5683161a90663-SJC

10f3

```
<!DOCTYPE html>
```

```
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]
```

```
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]
```

```
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]
```

```
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]
```

```
<head>
```

<title>Attention Required! | Cloudflare</title>

```
<meta charset="UTF-8" />
```

```
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
```

```
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
```

```
<meta name="robots" content="noindex, nofollow" />
```

```
<meta name="viewport" content="width=device-width,initial-scale=1,max
```

<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.er

```
<!--[if lt IE 9]><link rel="stylesheet" id="cf_styles-ie-css" href="/
```

```
[endif]...
```

提供給	提供給	提供給
-----	-----	-----

根據Cloudflare提供的Ddo

依据CloudNative提供的DDO

起生可以砍切 功殺柱微與

GET /en HTTP/1.1

User-Agent: <some string>

Cookie: <some cookie>

Host: example.com

Connection: close

Content-Length: 800000

$$a[] = \&b[] = \&a[] = \&b[] = \&a[] = \&b[] = \&a[] = \&b[] = \&a[] = \&b[] = \dots$$

根據Cloudflare提供的DDoS攻擊分析報告可以確認，攻擊特徵與Mirai相同

```
if]-->
```

```
!--<![endif]-->
```

TANet IOT 資安事件分析

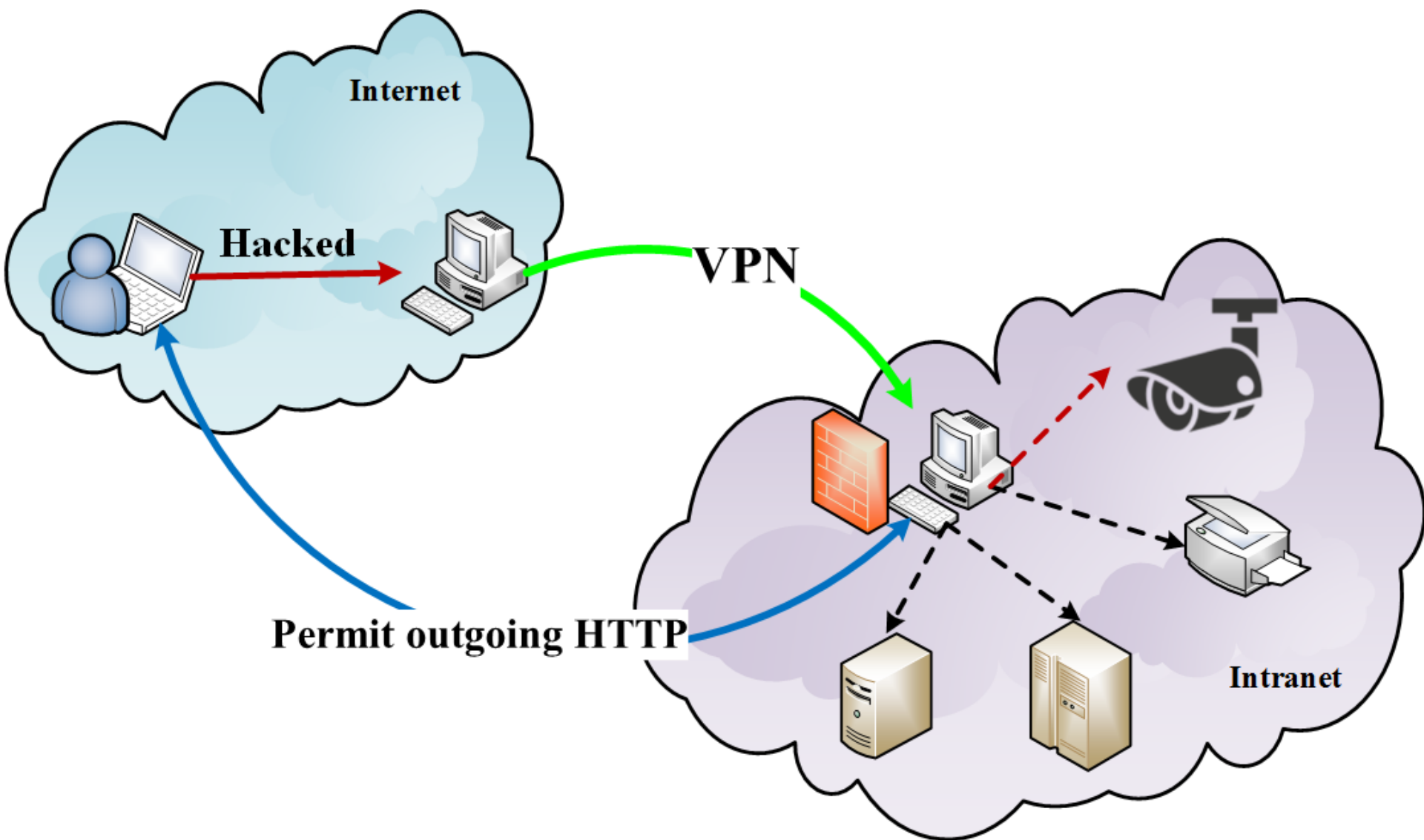
```
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);
add_auth_entry("\x50\x4D\x4D\x56", "", 4);
```

Mirai是一套利用C語言所寫的攻擊程式，主要攻擊目標為網路攝影機，內建多組預設帳號密碼，一旦入侵成功即可透過殭屍網路方式控制為數眾多的攝影機發動DDoS攻擊。

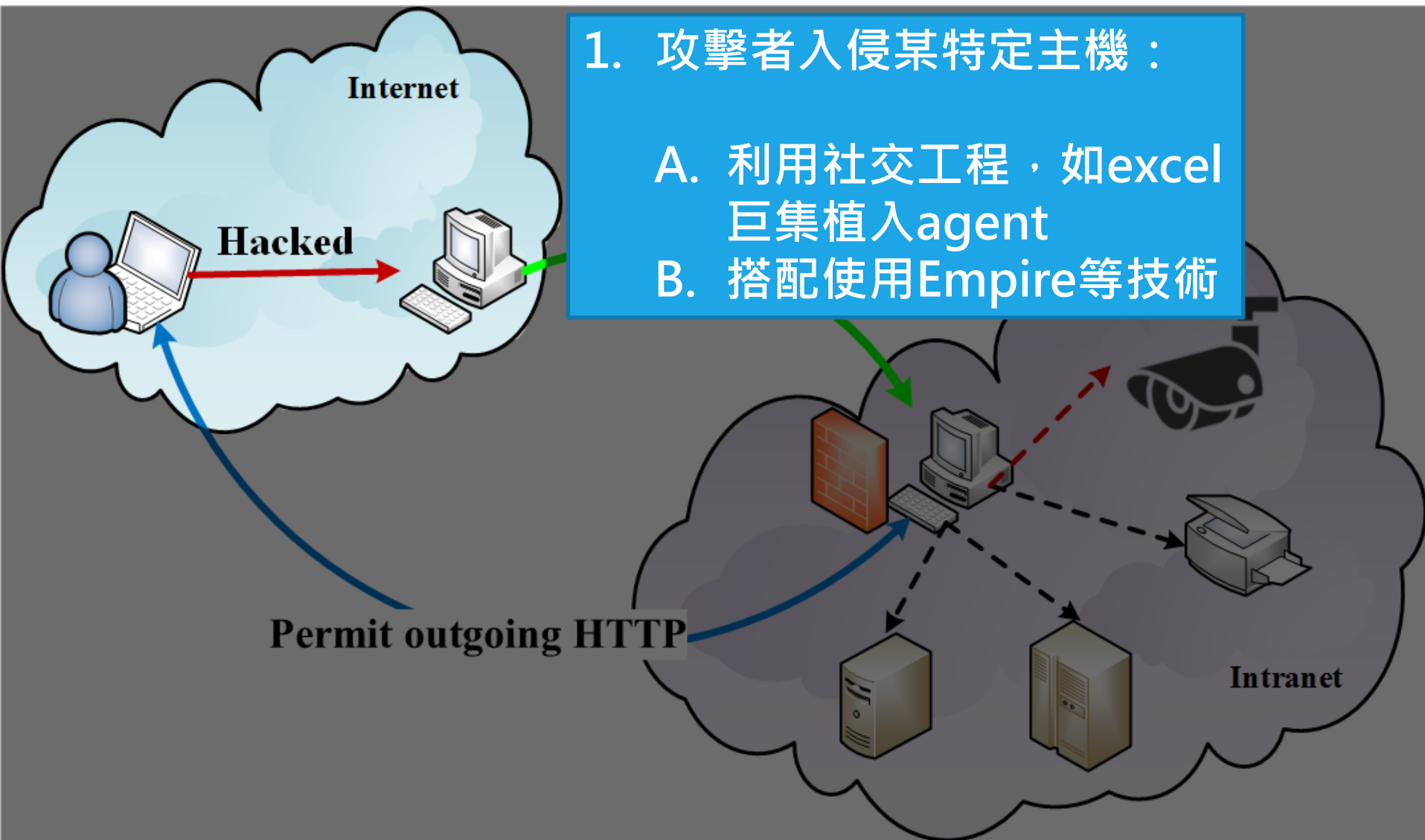
目前Mirai原始碼已被作者公開，因此這類型攻擊將會大幅成長。

```
// root xc3511
// root vizxv
// root admin
// admin admin
// root 888888
// root xmhdipc
// root default
// root juantech
// root 123456
// root 54321
// support support
// root (none)
// admin password
// root root
// root 12345
// user user
// admin (none)
// root pass
// admin admin1234
// root 1111
// admin smcadmin
```

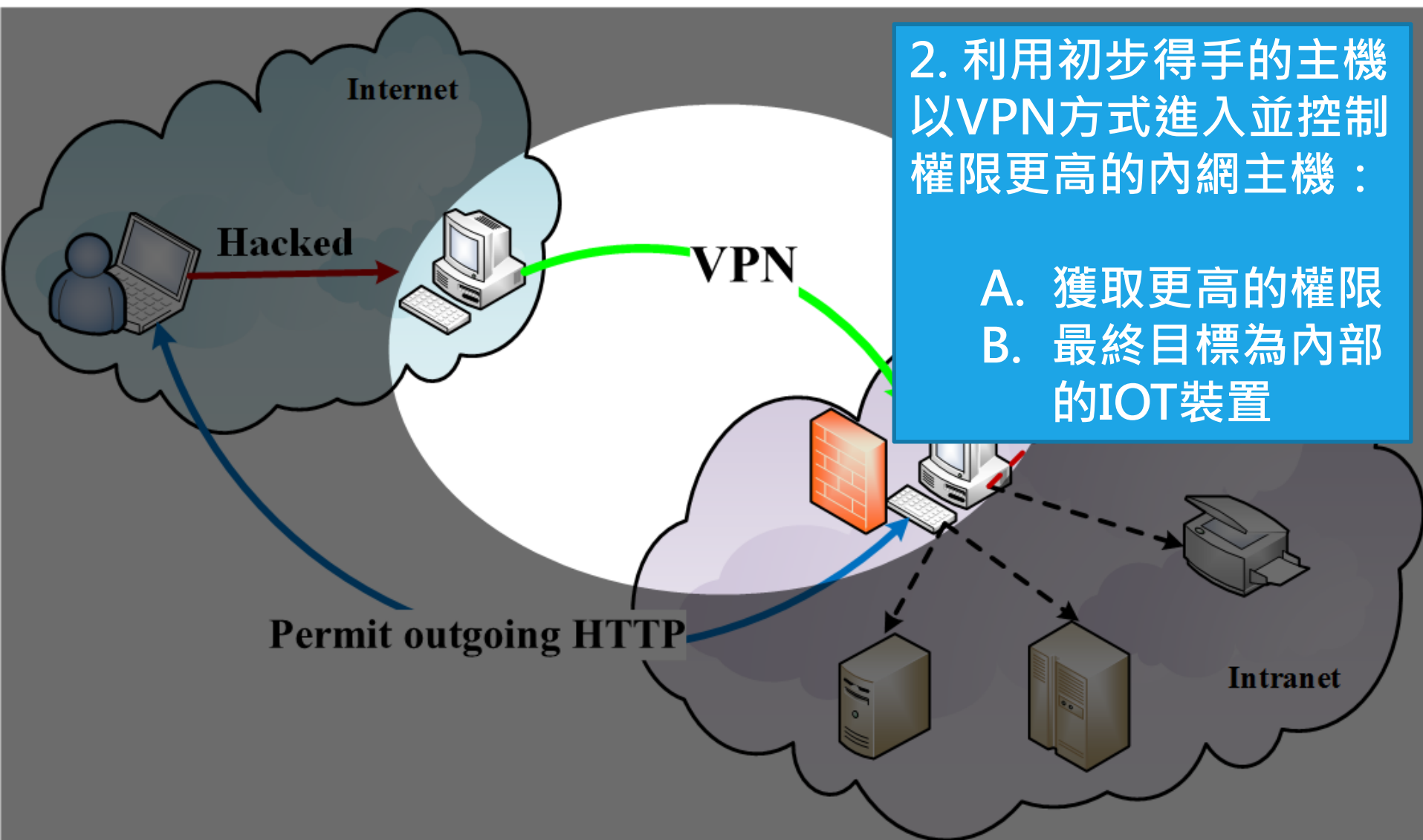
IOT 入侵手法分析



IOT 入侵手法分析



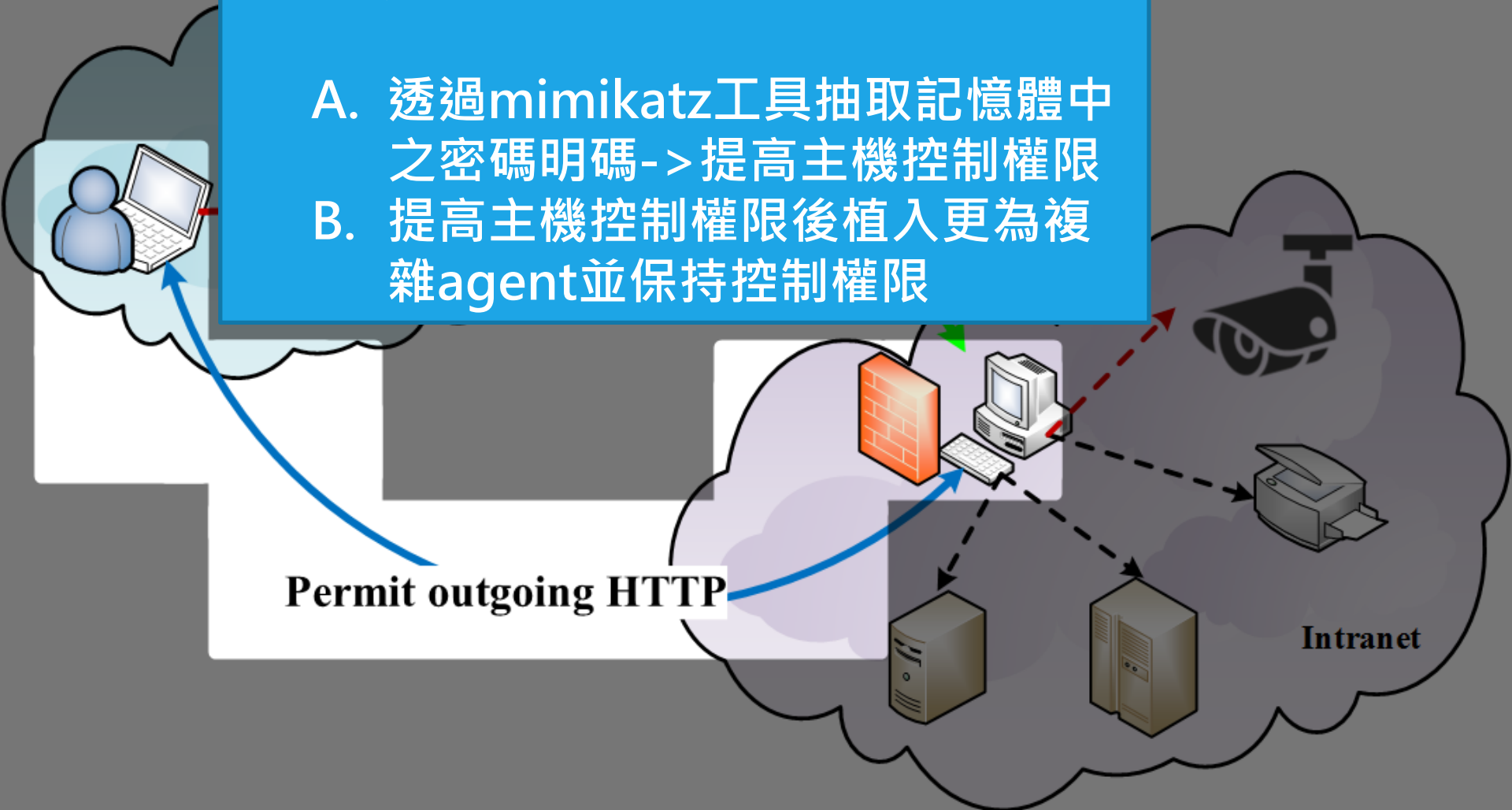
IOT 入侵手法分析



IOT 入侵手法分析

3. 持續保有控制權限：

- A. 透過mimikatz工具抽取記憶體中之密碼明碼->提高主機控制權限
- B. 提高主機控制權限後植入更為複雜agent並保持控制權限

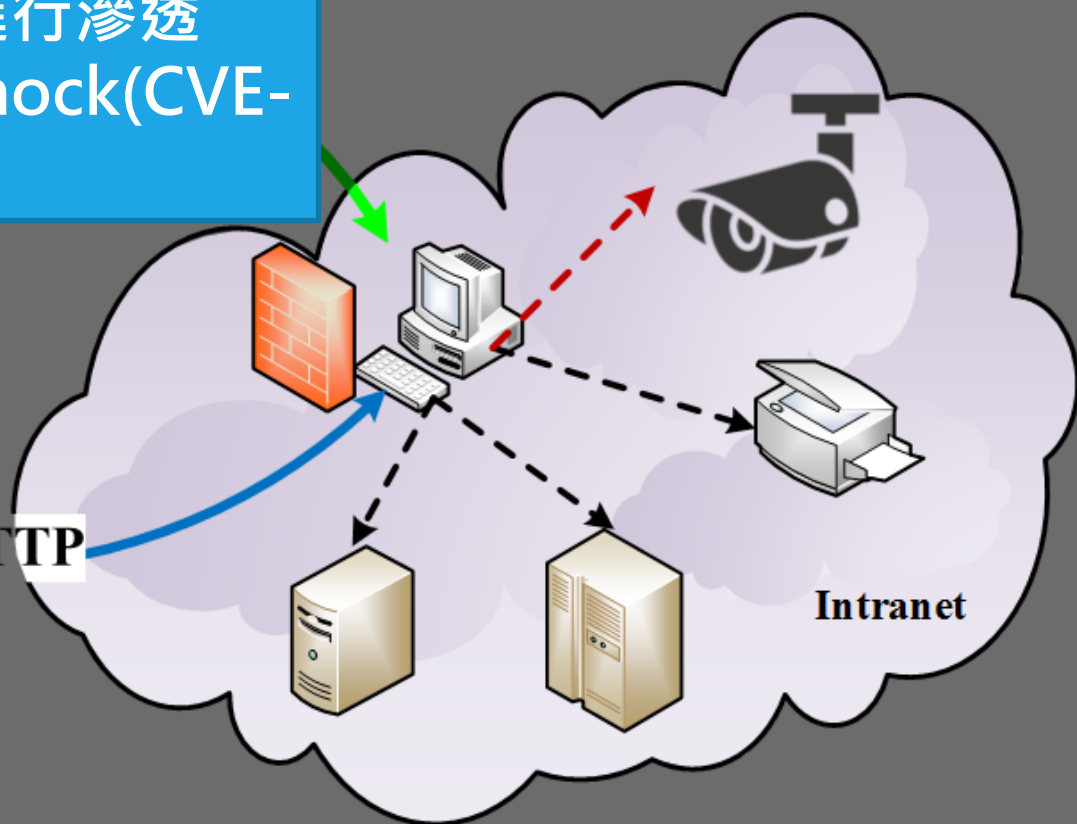


IOT 入侵手法分析

4. 利用特定漏洞入侵內網裝置，以取得並控制更多主機：

- A. 搭配metapreter進行滲透
- B. 漏洞利用如Shellshock(CVE-2014-6271)

Permit outgoing HTTP



IOT 入侵手法分析

(1:31976) OS-OTHER Bash CGI environment variable injection attempt

alert tcp \$EXTERNAL_NET any -> \$HOME_NET \$HTTP_PORTS (msg:"OS-OTHER Bash CGI environment variable injection attempt"; flow:to_server,established;

content:"() {";

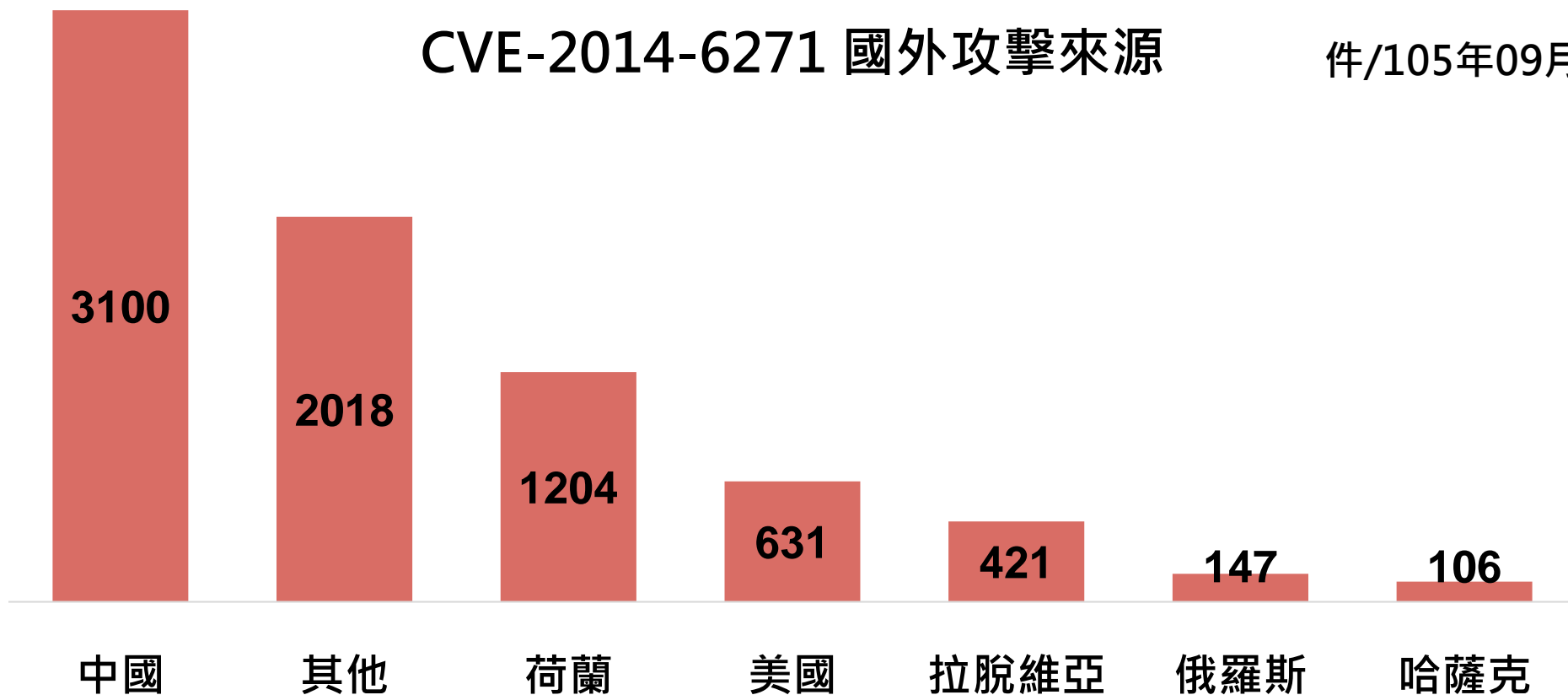
fast_pattern:only; http_client_body; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, ruleset community, service http; reference:cve,2014-6271; reference:cve,2014-6277; reference:cve,2014-6278; reference:cve,2014-7169; classtype:attempted-admin; sid:31976; rev:5;)

Shellshock (CVE-2014-6271) 是在2014年公開發布的漏洞，其利用bash對環境變數的解析上產生的錯誤。導致只要是能夠引入環境變數的部分，能夠輕易的利用參數塞入任何程式碼，影響甚至可控制目標主機。以上述北區ASOC使用的偵測規則而言，主要偵測的便是「往伺服器的資料流」是否被塞入「**() {**」此字串。

IOT 入侵手法分析

CVE-2014-6271 國外攻擊來源

件/105年09月



北區ASOC在Shellshock相關漏洞公佈兩日內，便在所有資安設備上增設Shellshock的偵測規則，並有效的對轄下區網進行保護，防止轄下區網內的設備遭受測試及漏洞被利用。

從上圖表統計內容可以知道兩年後的今日，此漏洞的嘗試利用仍不在少數，九月份即有近八千筆的漏洞嘗試利用。



Q & A