IPv6網路安全威脅

報告人： 朱彥如
中華電信研究院 寬網所
2017年12月

內容

- IPv6 DDoS網路安全威脅
- IPv6弱點公告及補強
- 4G/LTE行動數據網路IPv6安全威脅

DDoS攻擊概觀 (1/2)

- DoS Attack (阻斷服務攻擊)
  - ✓ 網路攻擊手法的一種，目的在耗盡目標電腦的網路或系統資源，使服務暫時中斷或停止，導致正常用戶無法存取
- DDoS (Distributed DoS- 分散式阻斷服務攻擊)
  - ✓ 駭客使用網路上 多個被攻陷的電腦作為「殭屍」(Botnet) 向特定的目標發動「阻斷服務」攻擊
- 歷史事件
  - ✓ 歐洲反垃圾郵件組織Spamhaus遭受流量高達300Gbps的DDoS攻擊 (2013)
  - ✓ 反課綱事件-「匿名者」亞洲支部(Anonymous Asia)攻擊台灣政府部會網站 (2015 July)

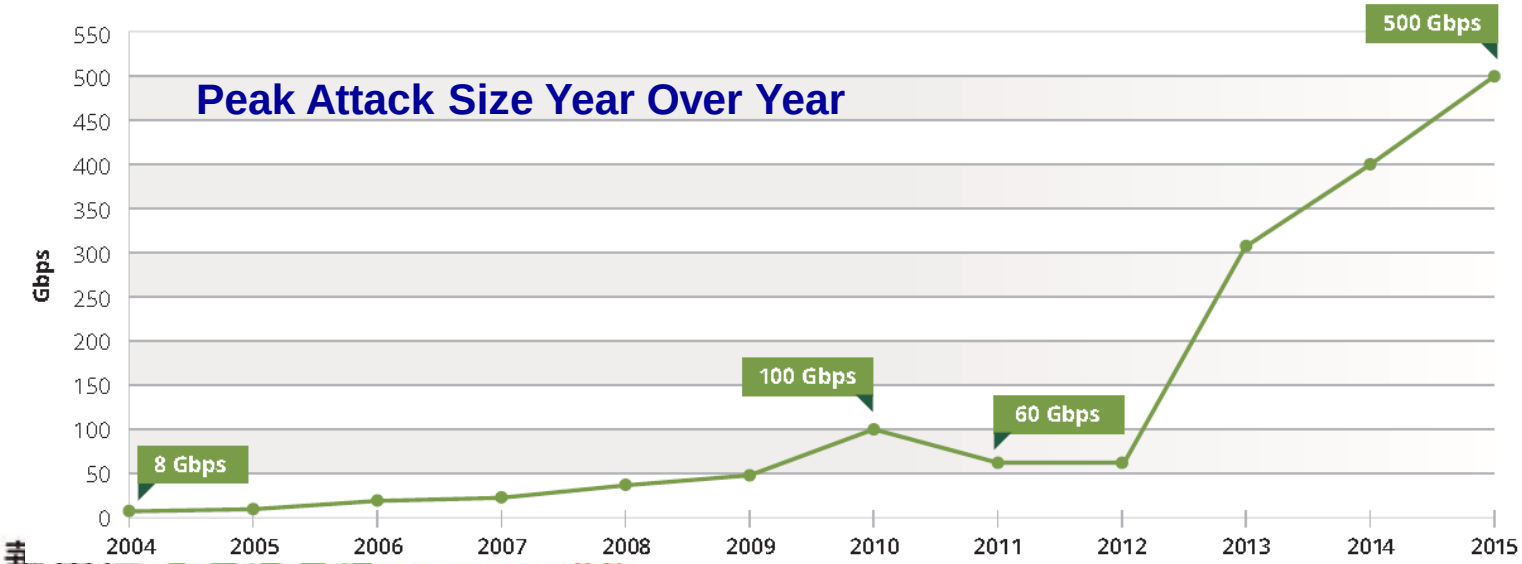
DDoS攻擊概觀 (2/2)

✓ 大量的IoT設備成為發動DDoS的跳板- Mirai惡意軟體

- 針對網路安全部落客Brian Krebs個人網站的攻擊 (620Gbps) (2016 Sep.)
- 對法國網站代管商OVH的攻擊 (1 Tbps) (2016 Sep.)

- 預估未來幾年，DDoS攻擊仍持續是ISP主要的安全考量議題

✓ DDoS最大攻擊量逐年提高，凸顯DDoS scale議題



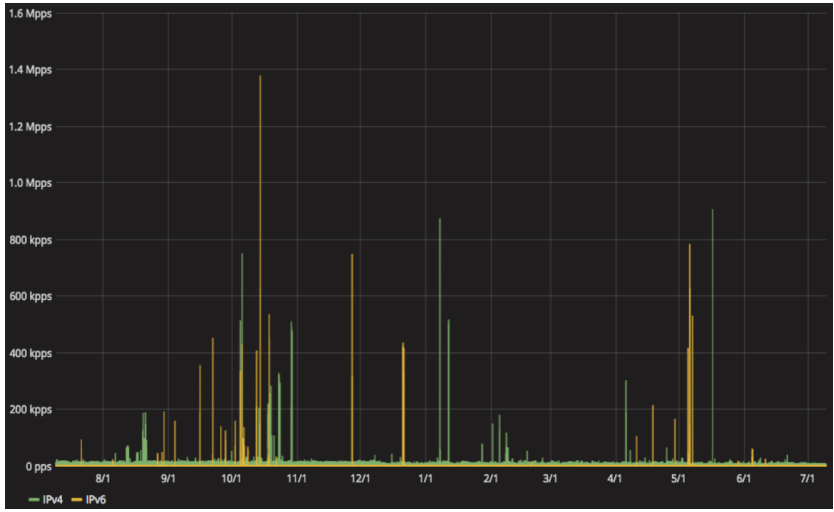
資料來源: Arbor Network WISR

IPv6 DDoS網路安全威脅 (1/4)

- 隨著IPv6日漸普及，DDoS安全威脅陸續浮現
  - ✓ CDN公司CloudFlare在World IPv6 Launch滿周年時，公開表示自兩個月前IPv6攻擊開始明顯增加 (2013 April)
  - ✓ 根據Arbor Network全球網路安全年報，2012年首次觀察到 IPv6 DDoS攻擊，約4%受訪者觀察到IPv6 DDoS攻擊。到2016年，成長至9%受訪者觀察到此類攻擊
  - ✓ 相對於IPv4 DDoS (500 Gbps)，IPv6攻擊量還不算大 (6 Gbps)，但持續成長中 (Arbor WISR 2016年)

IPv6 DDoS網路安全威脅 (2/4)

- 2015年IRCCloud觀察到IPv6 DDoS攻擊
  - ✓ IRCCloud位於英國，是提供行動用戶長時連線IRC服務的公司，員工僅4人
    - ~20,000 active outbound IRC connections
    - ~30 servers, in managed and cloud hosting
  - ✓ 已支援IPv6多年，約65% outbound IRC連線是透過IPv6，每個用戶配發unique IPv6位址
  - ✓ IPv6 DDoS攻擊量已高於IRCCloud gigabit edge ports (2017年7月)



資料來源: UK IPv6 Council IPv6 Security Workshop

IPv6 DDoS網路安全威脅 (3/4)

- MalwareMustDie在2016年10月，公告一款透過IPv6攻擊物聯網的DDoS軟體
  - ✓ 針對Linux IoT boxes弱點，感染滲透成為IRC botnet，藉此啟動DDoS攻擊

MMD-0059-2016 - Linux/IRCTelnet (new Aidra) - A DDoS botnet aims IoT w/ IPv6 ready

29 Oct 2016

It's a Kaiten/Tsunami? No.. STD?? No! It's a GayFgt/Torlus/Qbot? No!! Is it Mirai?? NO!!
*It's a **Linux/IRCTelnet (new Aidra)**! ..a new coded IoT DDoS botnet's Linux malware..*

Summary

This post is a report of what it seems to be a new IRC botnet ELF malware, that is obviously used for performing DDoS attack via IRC botnet. It was coded with partially is having specification as per Tsunami/Kaiten protocol, but it is a re-coded one with the different way, with adding some more features in messaging and malicious/attack vectors used. The malware (the bot client) is designed to aim IoT device via telnet protocol, by using its originally coded telnet scanner

IPv6 DDoS網路安全威脅 (4/4)

- IPv6 DDoS攻擊防禦
  - ✓ IDS、Firewalls 、 Blackholing and Router filtering 、DDoS Cleaning、Over-provisioning
- 企業IDS若由現有產品擴充支援IPv6，需考量
  - ✓ 若沿用IPv4既有的偵測參數，針對IPv6-only欄位不易制定偵測條件
  - ✓ 針對IPv6特有攻擊(如ICMPv6 DDoS)，偵測防禦能力可能不足
  - ✓ 是否可順利顯示Alert中的IPv6資訊

IPv6弱點公告

- CVE-2016-1409
  - ✓ The ND implementation in the IPv6 stack allows remote attackers to cause a DoS (packet-processing outage) via crafted ND message
  - ✓ 受影響的平台: 多款知名ISP路由器
- CVE-2016-10142
  - ✓ An issue was discovered in the IPv6 protocol specification, related to ICMP PTB messages.
  - ✓ 駭客可透過IPv6 atomic fragments進行Fragmentation-Based attack
  - ✓ 受影響的平台: 支援發送IPv6 Atomic Fragment的所有設備

CVE-2016-10142弱點公告

Vulnerability Details : CVE-2016-10142

An issue was discovered in the IPv6 protocol specification, related to ICMP Packet Too Big (PTB) messages. (The scope of this CVE is all affected IPv6 implementations from all vendors.) The security implications of IP fragmentation have been discussed at length in [RFC6274] and [RFC7739]. An attacker can leverage the generation of IPv6 atomic fragments to trigger the use of fragmentation in an arbitrary IPv6 flow (in scenarios in which actual fragmentation of packets is not needed) and can subsequently perform any type of fragmentation-based attack against legacy IPv6 nodes that do not implement [RFC6946]. That is, employing fragmentation where not actually needed allows for fragmentation-based attack vectors to be employed, unnecessarily. We note that, unfortunately, even nodes that already implement [RFC6946] can be subject to DoS attacks as a result of the generation of IPv6 atomic fragments. Let us assume that Host A is communicating with Host B and that, as a result of the widespread dropping of IPv6 packets that contain extension headers (including fragmentation) [RFC7872], some intermediate node filters fragments between Host B and Host A. If an attacker sends a forged ICMPv6 PTB error message to Host B, reporting an MTU smaller than 1280, this will trigger the generation of IPv6 atomic fragments from that moment on (as required by [RFC2460]). When Host B starts sending IPv6 atomic fragments (in response to the received ICMPv6 PTB error message), these packets will be dropped, since we previously noted that IPv6 packets with extension headers were being dropped between Host B and Host A. Thus, this situation will result in a DoS scenario. Another possible scenario is that in which two BGP peers are employing IPv6 transport and they implement Access Control Lists (ACLs) to drop IPv6 fragments (to avoid control-plane attacks). If the aforementioned BGP peers drop IPv6 fragments but still honor received ICMPv6 PTB error messages, an attacker could easily attack the corresponding peering session by simply sending an ICMPv6 PTB message with a reported MTU smaller than 1280 bytes. Once the attack packet has been sent, the aforementioned routers will themselves be the ones dropping their own traffic.

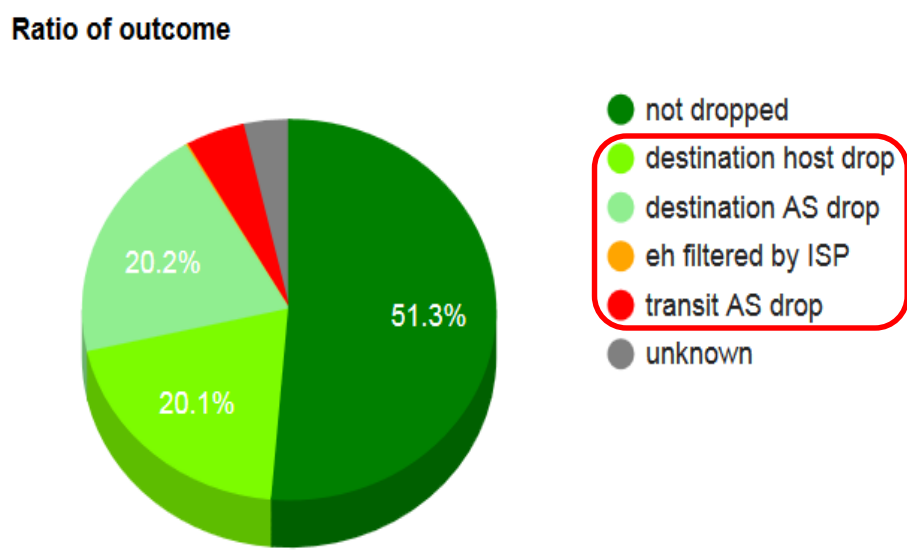
Publish Date : 2017-01-14 Last Update Date : 2017-07-10

IPv6 Fragments網路透通現況

- RFC 7872: Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World

The data set is about: IPV6 web servers in Alexa top million sites Spring 2016, the test was done by sending IPv6 packets with Fragmentation Header (first fragment).

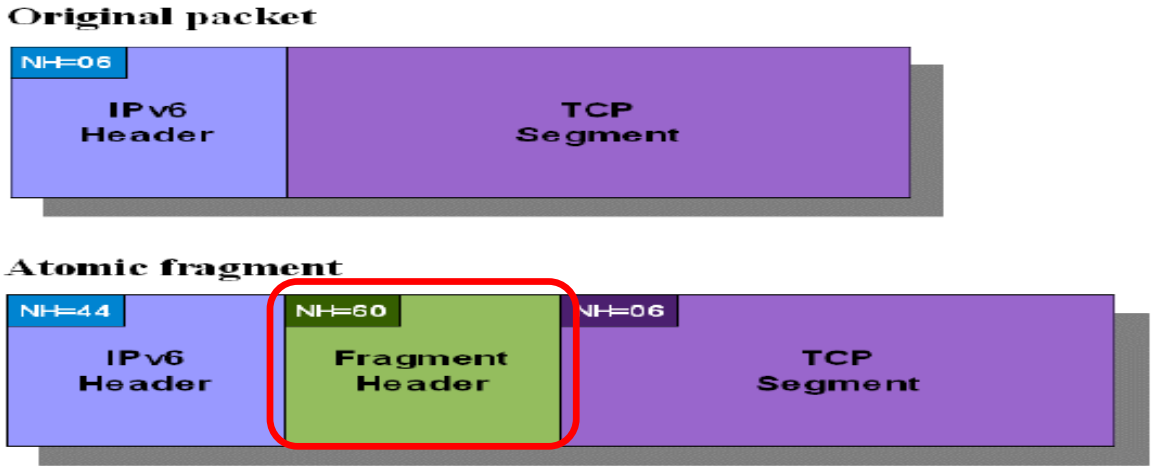
Test result	Number of destinations	%-age of reachable destinations
not dropped	667	51.3
destination host drop	261	20.1
destination AS drop	263	20.2
eh filtered by ISP	2	0.2
transit AS drop	60	4.6
unknown	47	3.6
not reached	221	-



資料來源: https://btv6.vyncke.org/exthdr/index.php?ds=alexa2016&t=fh

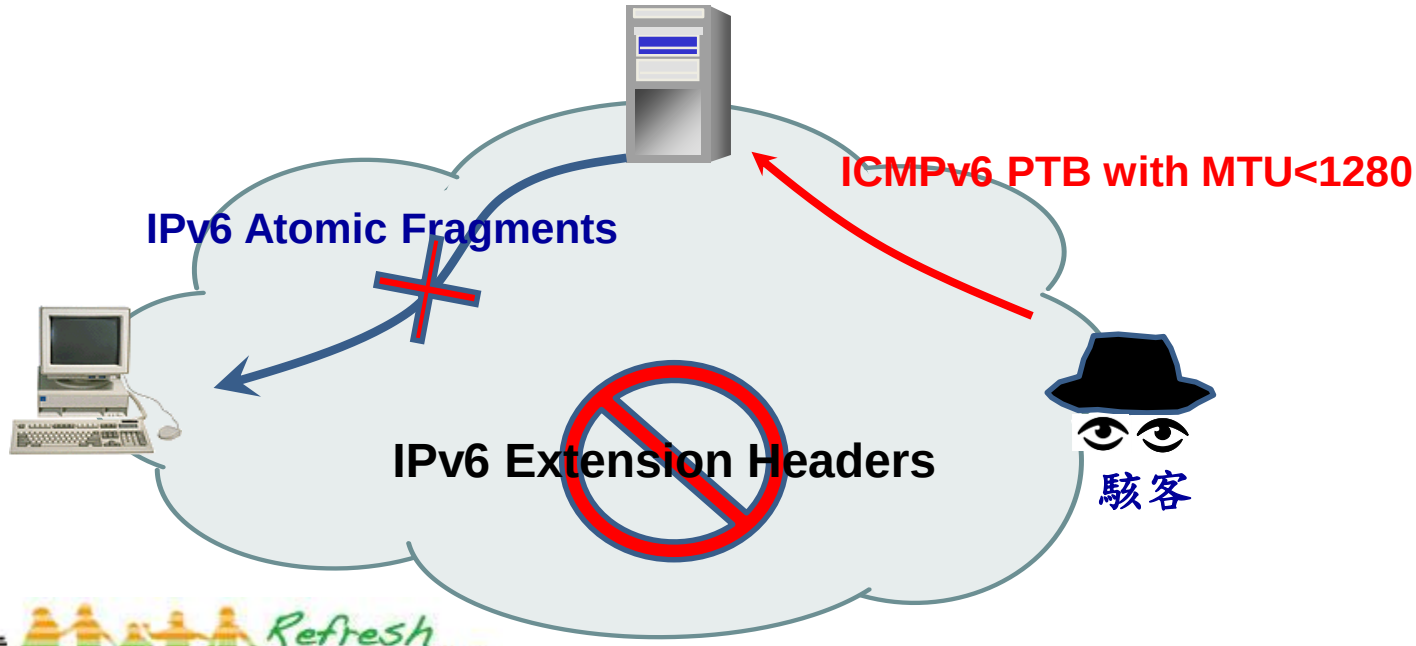
IPv6 Atomic Fragment

- RFC 2460:
  - ✓ In response to an IPv6 packet that is sent to an IPv4 destination, the originating IPv6 node may receive an ICMP Packet Too Big message (PTB) reporting a Next-Hop MTU less than 1280. In that case, the IPv6 node is not required to reduce the size of subsequent packets to less than 1280, but must include a Fragment header in those packets so that the IPv6-to-IPv4 translating router can obtain a suitable Identification value to use in resulting IPv4 fragments
- 結果: 產生IPv6 Atomic Fragments (Frag Offset=0, More Frag=0)



IPv6 Atomic Fragment攻擊 (1/2)

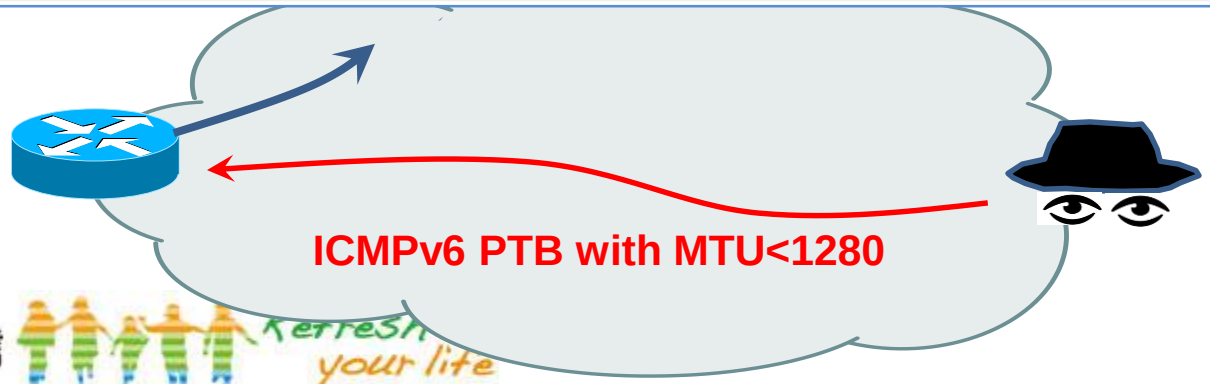
- 駭客可以藉由發送偽造" ICMPv6 PTB with MTU<1280" ，讓接收端設備產生 IPv6 atomic fragments ，藉此中斷正常通訊
  - ✓ 駭客僅需偽造ICMPv6 payload中的IPv6位址，不需偽造source address，Ingress Filtering無法防堵



IPv6 Atomic Fragment攻擊 (2/2)

- 此攻擊主要影響有固定聯絡對象的網路設備
  - ✓ 伺服器: mail server 、DNS server

```
◢ Internet Protocol Version 6, Src: 2001:b02a:0:b::2, Dst: 2001:ca0:1:101::4
    0110 .... = Version: 6
  ▷ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00 (DSCP: CS0,
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 16
    Next header: Fragment Header for IPv6 (44)
    Hop limit: 64
    Source: 2001:b02a:0:b::2
    Destination: 2001:ca0:1:101::4
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ◢ Fragment Header
      Next header: ICMPv6 (58)
      Reserved octet: 0x00
      0000 0000 0000 0... = Offset: 0 (0 bytes)
      .... .... .... .00. = Reserved bits: 0
      .... .... .... ...0 = More Fragments: No
      Identification: 0x00000006
▷ Internet Control Message Protocol v6
```



建議方案 (1/2)

- 更新設備: 收到ICMPv6 PTB with MTU<1280時，後續不要送出IPv6 Atomic Fragments
  - ✓ RFC 8021: Generation of IPv6 Atomic Fragments Considered Harmful
  - ✓ RFC 8200: IPv6 Specification (Obsoletes RFC 2460)

```
10.  Security Considerations

o  Removed the paragraph in Section 5 that required including a
   Fragment header to outgoing packets if an ICMP Packet Too Big
   message reporting a Next-Hop MTU is less than 1280.  See
   [RFC6946] for more information.
```

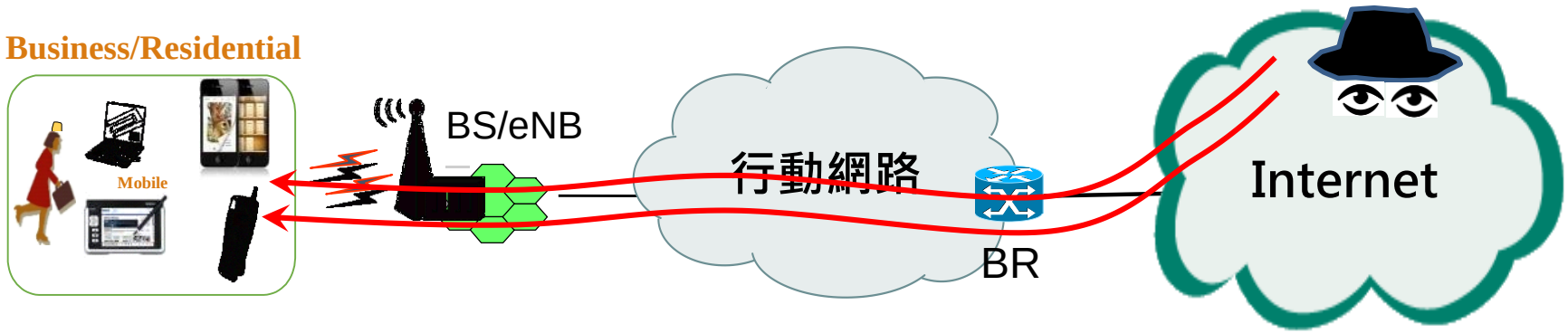
- 更新SIIT技術(包括stateless及stateful NAT64): 不要依賴IPv6 Atomic Fragments來運作

建議方案 (2/2)

- 一般伺服器可能的暫時性防禦方法：
  - ✓ 阻擋傳送到伺服器的ICMP PTB with MTU<1280
    - 防火牆必須能依ICMPv6 error訊息內容來制定過濾條件，有些防火牆設備可能無法支援
  - ✓ 將伺服器MTU設為1280 bytes，並拒絕所有ICMP PTB訊息進入
    - 將造成傳送效能降低

4G/LTE行動數據網路IPv6安全威脅 (1/2)

- 行動通訊設備，若配發Public IP位址，容易遭受惡意攻擊
  - ✓ 耗盡傳輸量月配額
  - ✓ 耗盡行動設備電池
- 無法以行動設備本身的防火牆防禦



4G/LTE行動數據網路IPv6安全威脅 (2/2)

- 新加坡大學曾經以3 Mb/s 的資料串流在幾分鐘之內成功耗盡行動用戶傳輸量月配額，全然掐住用戶的行動通訊。並透過低速UDP stream，順利防止手機進入休眠模式，提高電池耗電量達24倍

- IPv4行動通訊傾向配發私有位址，而IPv6行動通訊則配發公用位址，更凸顯此議題嚴重性

建議方案 (1/2)

- 4G/LTE與網際網路介接處設置防火牆，阻擋所有源自網際網路的流量進入4G/LTE
  - ✓ 可能影響部分應用服務(如peer-to-Peer)或行動用戶自架服務
  - ✓ 4G/LTE與網際網路間流量極大，需考量防火牆處理容量，及對通訊品質的可能衝擊

IPv6 Stateful firewall for Internet to 4G/LTE: Block all traffic originating from Internet

建議方案 (2/2)

- 強化異常訊務監視告警與處理，盡可能達到及時防堵，以降低此議題對網路品質之影響及對客戶之衝擊

結語及討論

- 隨著IPv6日漸普及，IPv6安全威脅事件開始浮現，IPv6協定本身或設備實做上弱點也陸續被公告，需及時進行補強
- 由於許多設備預設啟動IPv6，即使ISP未提供IPv6服務，或企業網路尚未啟動IPv6，使用者仍可能遭受潛在IPv6安全威脅，建議網路維運者及資安人員及早布局
- 雖然既有IPv4網路安全機制多可沿用於IPv6，但需進一步了解IPv6特有議題並加以防範，以免駭客有機可趁

Thank You

Q&A