prop-125-v001:
Validation of "abuse-mailbox" and other IRT emails

Proposer: **Jordi Palet Martínez**
Aftab Siddiqui

主講人：亞太電信 楊捷雄

義務

- 於APNIC Whois database中填寫inetnum, inet6num, aut-name等IRT(Incident Response Team) object屬於義務行為 (2010/11/08)
- 目的在使當網路發生不當使用行為時，得以取得手段聯繫與有效反應至最終負責之單位組織

問題

- 相關物件聯絡資訊大多屬於過期、不正確、不存在、或是無人關心的信箱資訊
- 實務上導致不當使用行為發生時，無法有效率取得正確聯絡資訊以要求處理，造成受侵害者(victim)安全問題與處理成本上升

提案目標

- 此提案目標在於提供確保abuse-mailbox等聯絡資訊及其流程具備有效性
- 確保處理不當使用行為之相關程序所造成的成本必須歸屬於對的LIR(Local Internet Registry)，而非受侵害者，並節省雙方時間與成本
  - 該LIR之所屬客戶為不當使用行為製造者及從中獲得經濟利益者
  - 成本包含因行為產生之法院訴訟、律師費用等

其它區域狀態

- LACNIC已有類似提案進行討論中
- ArfiNIC及RIPE NCC正在準備類似提案
- ARIN已進行年度POC(point of contact)驗證
- RIPE NCC亦已進行”abuse-mailbox:”內容之年度驗證
  - ripe-705

Proposed policy solution

abuse-mailbox, email, admin-c, tech-c

- Email送至”abuse-mailbox”, “email”, “admin-c”, “tech-c”信箱，必須具備以下處理要求
  - 定期人工檢查處理
  - 不應有信件過濾機制處理
  - 信件最初回覆可為自動發送，包含指派ticket number、分類、要求提供資訊等，但不應為要求以固定格式或表格提報
    - 接受檢舉者需配合不同案件型態進行個別檢視、處理
    - 處理成本應由製造不當行為者承擔、而非受侵害者
- 檢舉者於最初通報中檢附log、SPAM mail副本(完整附件或標頭)、或是可證明abuse之其它證據等為合理行為
  - 相對，檢舉者可能無法預期在相關證據尚未被有效提供前，整體流程能得到有效執行。但同樣的，流程必須給予檢舉者重複提交或補充證據之機制
  - 此步驟可透過如fail2ban, SpamCop或其他自動手段進行，以節省雙方處理成本

abuse-mailbox, email, admin-c, tech-c 驗證目的

- 驗證程序由APNIC定義之，且必須符合以下目的
  - 一個可確保驗證來自於APNIC而非第三者的簡單流程，避免安全性風險
    - 避免使用單一直接URL機制進行驗證
  - 避免自動流程
  - 執行驗證者需了解驗證的程序及目的，且採取某些作法定期監控”abuse-mailbox”, “email”, “admin-c”, “tech-c”信箱，並會在接受abuse舉報時會收到回覆
  - 驗證程序不應超過15天
  - 若驗證失敗，應反應至LIR並啟動另一不超過15天之驗證程序

abuse-mailbox, email, admin-c, tech-c 驗證

- 當”abuse-mailbox”, “email”, “admin-c”, “tech-c”被創建、更新時，APNIC得以進行驗證相關物件的有效性；APNIC亦應每6個月或合適頻率下進行定期驗證
- APNIC得以在一般或特殊情況下，採用不同於apnic.*之網域、甚至修改信件標題或內文以使驗證程序更有效率
  - 特殊情況如下述Escalation to APNIC等
- APNIC 可在成員未充分配合下，依據所定義之政策、程序、與會員規範等暫停myapnic存取權限，直到解決

Escalation to APNIC

- 為避免詐欺行為發生(如abuse-mail僅回覆來自於APNIC的信箱、或是帶有特定主旨及內容) ，或不完全遵守政策要求(如對於abuse的不正確或缺乏回應)，及確保區域內APNIC資源之服務品質等情境時，APNIC可透過信箱(如”escalation-abuse@apnic.net”)提昇處理層級、或要求重新驗證、或甚至由APNIC直接中介進行處理
  - APNIC需經由合適的政策、程序、會員協議為之
- 該IRT無任何相關email有所回覆時，則標記該IRT物件無效並停止myapnic存取權限，並透過其它管道(如財務或企業窗口)聯繫之
- 如該IRT某些關連email無回應者，則標記該屬性無效並聯繫會員處理之。若無法在15天內修正問題，則停止myapnic存取權限，並透過其它管道(如財務或企業窗口)聯繫之

Advantages / Disadvantages and Impact

優點

- APNIC Whois database中建立IRT物件的目的，是能有正確、有效率的途徑，作為不當使用行為發生時，得以聯繫正確網路對應窗口
- 填寫上述物件及確保有效聯絡窗口，可提昇當不當使用行為發生時之服務效率
- 有助於提昇資訊品質，並達成控制網路上的不當使用之目的

缺點

- 無

衝擊

- APNIC成員需定期檢查並更新所屬IRT物件

Example of the validation procedure

1. APNIC自動啟動驗證程序，對每個信箱送出兩封連續信件

2. 每個信箱負責人員需前往認證網站並填上第二封信所提供之驗證碼

3. 若驗證碼未能在期限內鍵入，系統將該IRT標記為”temporarily invalid”，以新產生之驗證碼寄送提醒信並通知APNIC工作人員，使APNIC得以人工方式持續跟催LIR處理

4. 若確認未能收到驗證，在經過3個工作天後，該IRT將被永遠標記為”invalid”

5. 一旦問題被解決，驗證程序將自動重複執行(步驟1~3)。如符合要求，該IRT將被標記為”valid”，否則將被視為違反政策

a. 信件僅會以純文字方式送出
b. 第一封信包含認證URL位址(如validation.apnic.net)，且帶有程序及政策之簡短說明
c. 第二封信帶有英數字組合之唯一驗證碼

a. 認證網站應具備防止自動填寫機制(如captcha)
b. 網站需以文字說明驗證程序及政策，並要求驗證人員以checkbox勾選同意政策、定期監控並處理不當行為舉報事件
c. 驗證碼最大有效期限應為15天

智慧生活

Thanks

https://www.apnic.net/wp-content/uploads/2018/08/prop-125-v001.txt

亞太電信