內政部警政署 刑事警察局
CRIMINAL INVESTIGATION BUREAU

電話節費器遭 Mirai TBOT Botnet 駭侵案例分享

內政部警政署刑事警察局
科技犯罪防制中心

113年12月25日

大綱
AGENDA

壹	貳	參	肆	伍
案件背景	攻擊手法與來源	漏洞分析	全國使用狀況分析	後續作為

壹、案件背景

9:41

113年9月9至18日
165報案紀錄

4家法人門號發出詐騙電話

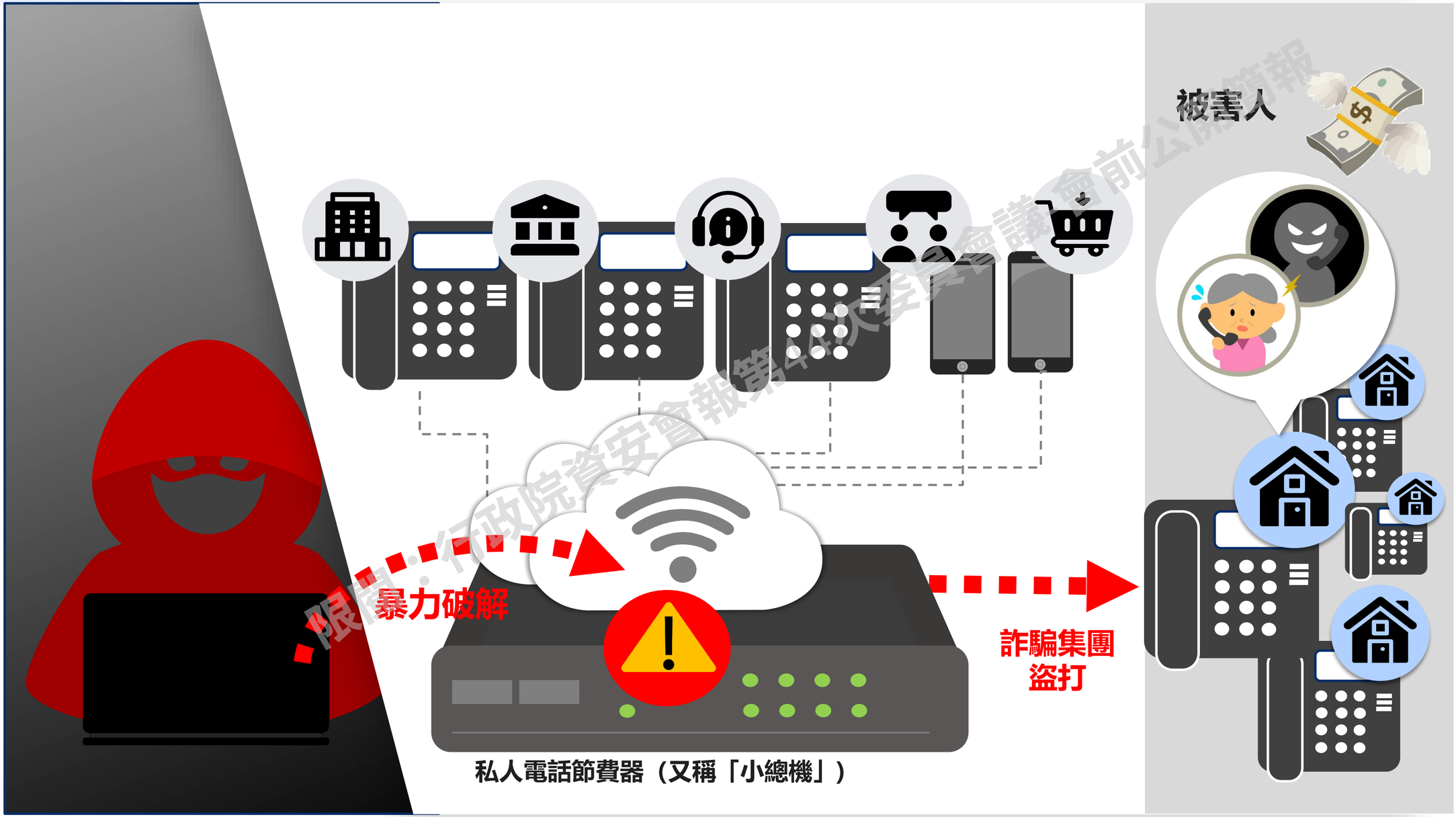
- ○○高中
  遭檢舉47次，被害1件
- ○○○○驗證中心
  遭檢舉33次
- ○○實業有限公司
  遭檢舉17次
- ○○○○股份有限公司
  遭檢舉12次

異常點

- 沒有「+號」，
  非國外偽號進線、亦非個人人頭卡
- 遭盜打者均為
  中華電信「法人」用戶
- 共同均使用
  

  Tenor AX Series VoIP Gateway
  - 由美商 Quintum 公司製造，96年被 Net.com 收購
  - 約91至94年間推出
  - 俱備FXS/FXO介面，可連接VoIP、PSTN網路，一般用於做為電話節費器或小總機使用

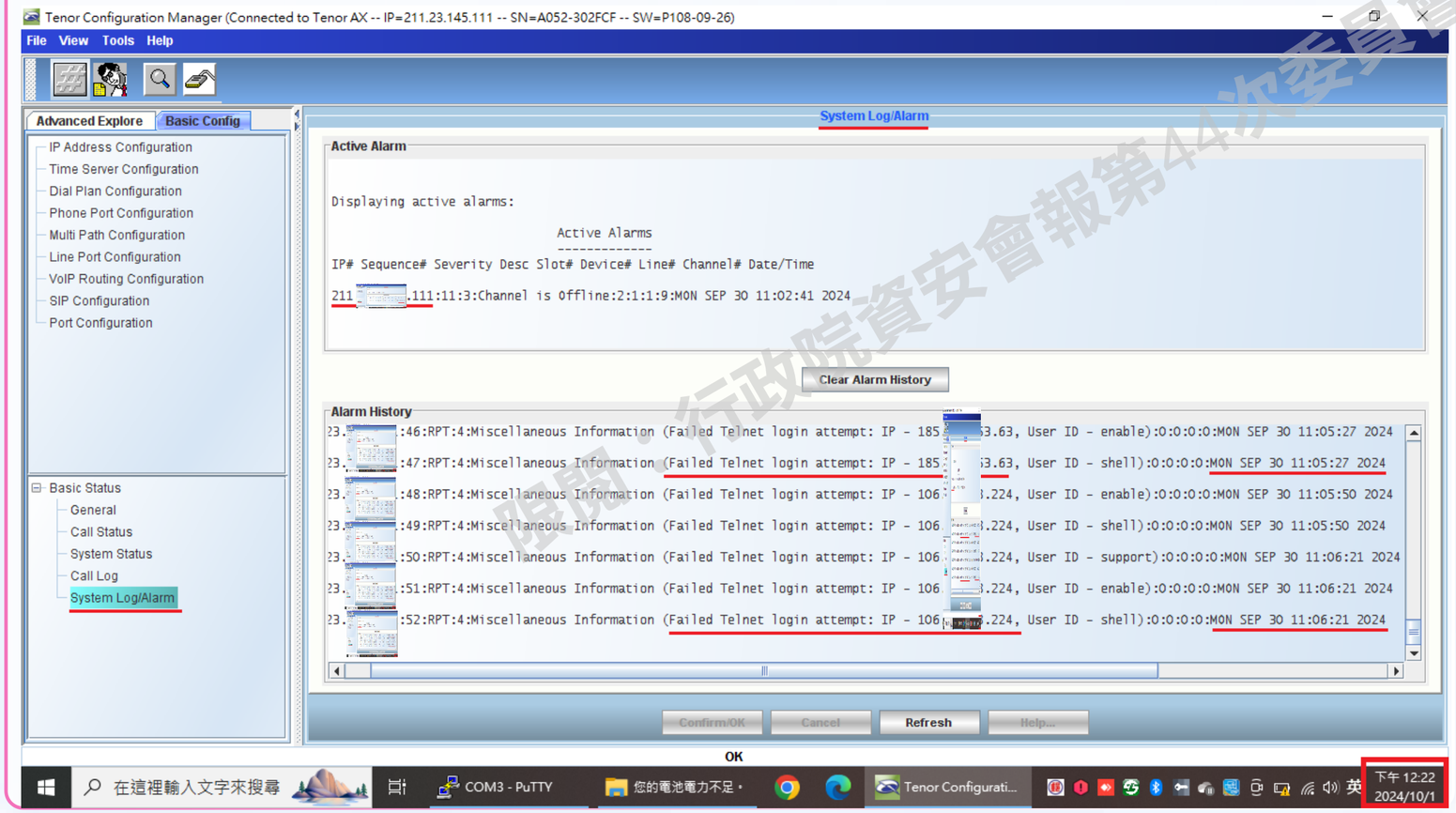
貳、攻擊手法與來源（一）



貳、攻擊手法與來源（二）

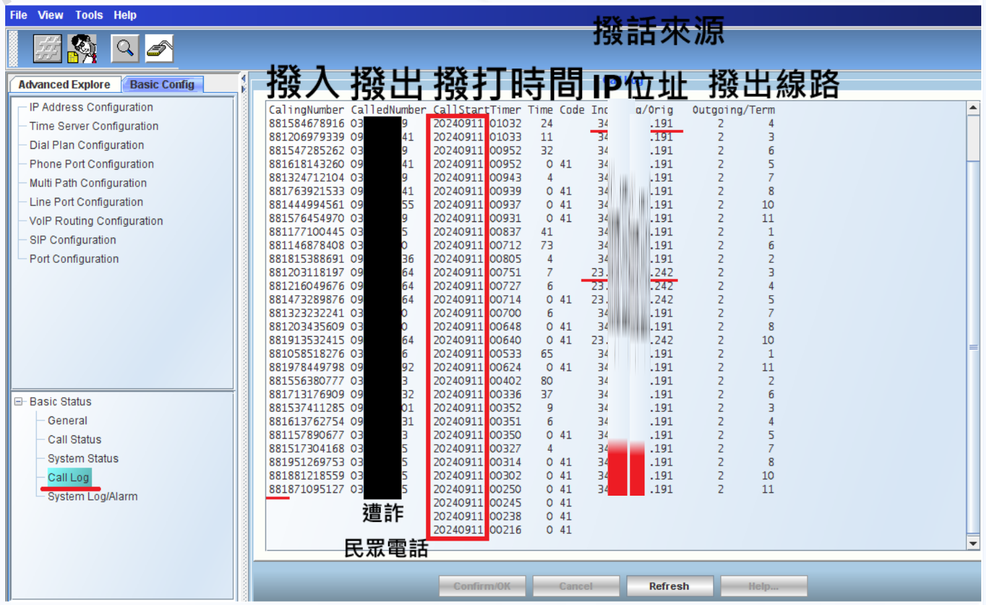
⚠ System Log / Alarm History 系統警告提示 登入 IP來源

- 荷蘭 (Failed Telnet login attempt: IP - 185.[redacted].63, User ID - shell)
- 中國 (Failed Telnet login attempt: IP - 106.[redacted].224, User ID - shell)



⚠ Call Log 撥話紀錄 來源 IP 位置

- 中國香港 34.[redacted].191
- 美國 23.[redacted]5.242

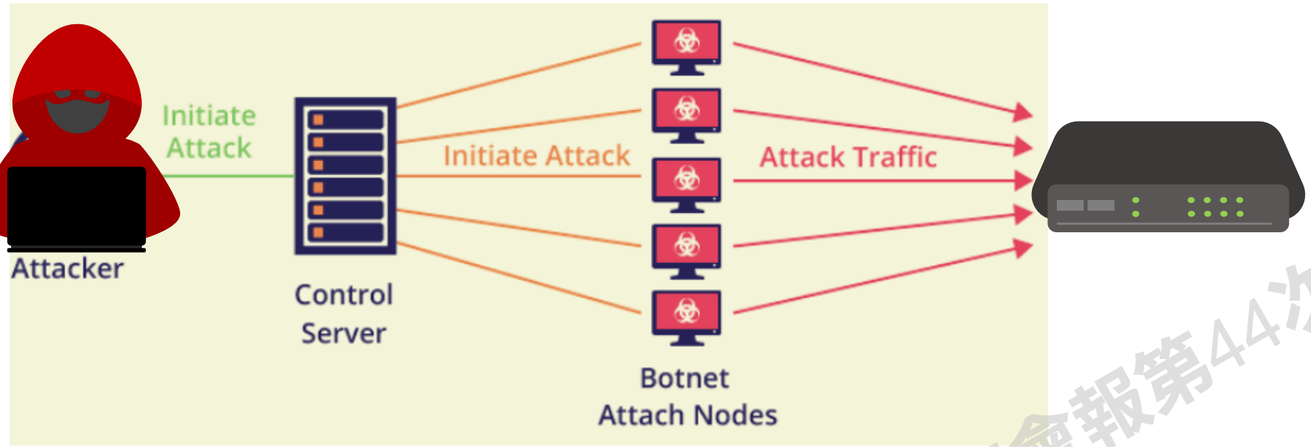


參、漏洞分析（一）

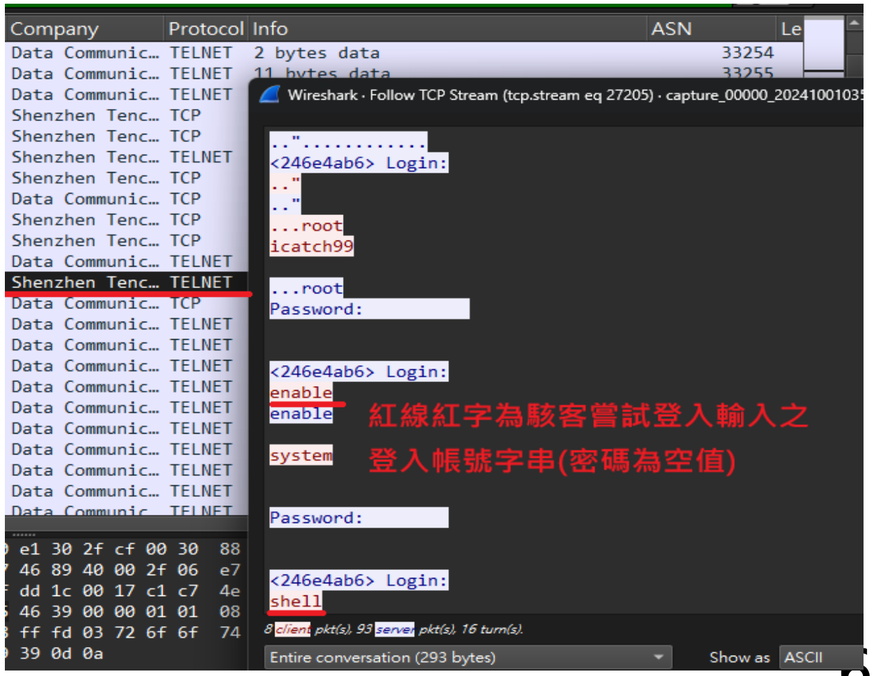
攻擊手法解析

- 駭客利用節費器預設允許用戶遠端登入（Telnet）、且無密碼錯誤保護機制等特性。嘗試進行暴力攻擊。
- 現場側錄封包顯示，駭客嘗試用「enable」、「shell」等字串登入，符合惡意程式 Mirai botnet* 特徵。

Mirai botnet 示意圖



*Mirai botnet：利用 IoT 裝置中的安全漏洞，駕馭數百萬 IoT 裝置的集體力量，組成殭屍網路來發動攻擊。



參、漏洞分析（二）

FTP 使用預設帳密

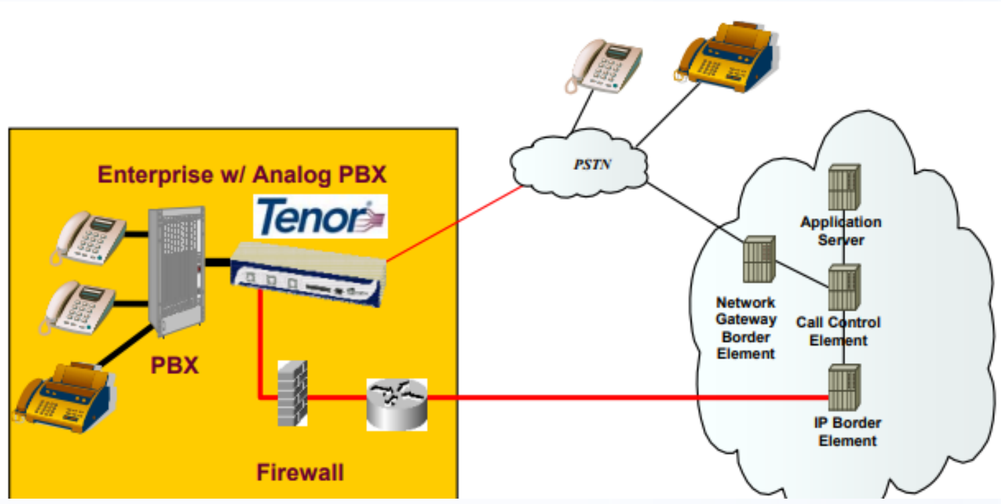
節費器另有 FTP 伺服器功能，使用者可能未關閉該服務或變更預設帳密。

```
Quintum# cmd bootconfig

Current system time is MON SEP 30 11:09:45 2024


boot device           : emac
unit number           : 0
processor number      : 0
host name             : host
file name             : file
inet on ethernet (e)  : 192.      150:FFFFFF00
gateway inet (g)      : 211.      .254
user (u)              : g       r
ftp password (pw)     : g       r
flags (f)             : 0x8
other (o)             : emac

Quintum#
```

Tenor AX FTP協定使用預設登入帳密

網路架構未加裝防火牆

原廠使用手冊建議將節費器安裝於防火牆後，如未依指引安裝，可直接從網路連線該節費器。



肆、全國使用狀況分析

公開情資工具 censys

使用此設備場域：
政府、學校共11筆，
餘為私人用戶。

全臺共 376 筆，
其中大部分（277組）
均開啟Telnet 服務。

搜尋條件：

臺灣使用 Quintum Tenor AX VoIP Gateway 設備 IP 位址

伍、後續作為

113年10月15日 第1次通報

- 將政府機關與學校，通報A-ISAC與N-ISAC。

10月16日 發布新聞稿

- 提醒民眾更換設備或調整網路架構。
- 該設備使用之OS為「Wind River Vxworks 5.4.2」，為88年開發，Wind River公司對於仍在使用5.4.2或更早版本的組織，建議通過網路隔離、防火牆保護等機制減少潛在風險。

11月11日 清查 IP

- 全面清查後，可直接連線進行遠端登入之IP共有 139 個，經調閱基資後其中16個為公務機關、學校及農漁會、航空公司等單位。

公務機關　航空公司

學校　漁農會

11月20日 第2次通報

- 第2次通報A-ISAC與N-ISAC。

THANK YOU