

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

案件背景

貳

攻擊手法
與來源

參

漏洞分析

肆

全國使用狀況
分析

伍

後續作為

限閱：行政院資安會報第44次委員會議-會前公開簡報

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



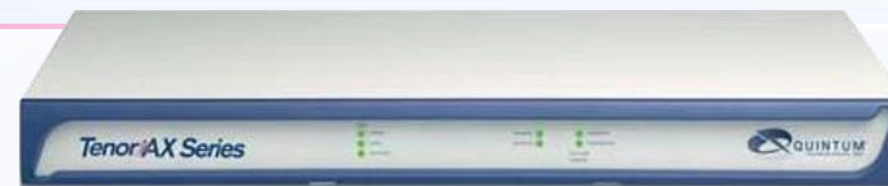
沒有「+號」，
非國外偽號進線、亦非個人人頭卡



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

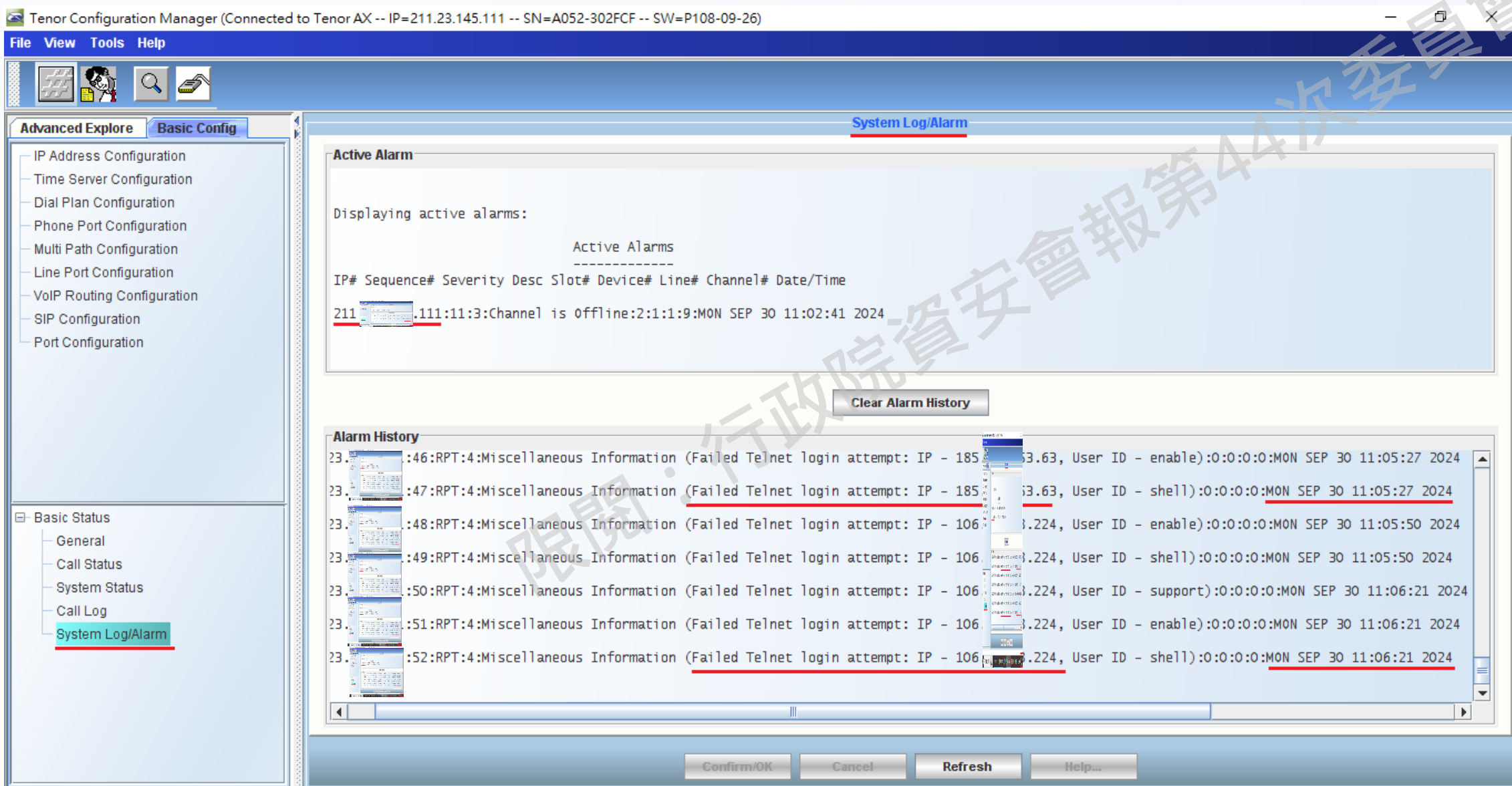
貳、攻擊手法與來源（一）



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 - 185.111.111.63, User ID - shell)
- 中國 (Failed Telnet login attempt: IP - 106.111.111.224, User ID - shell)



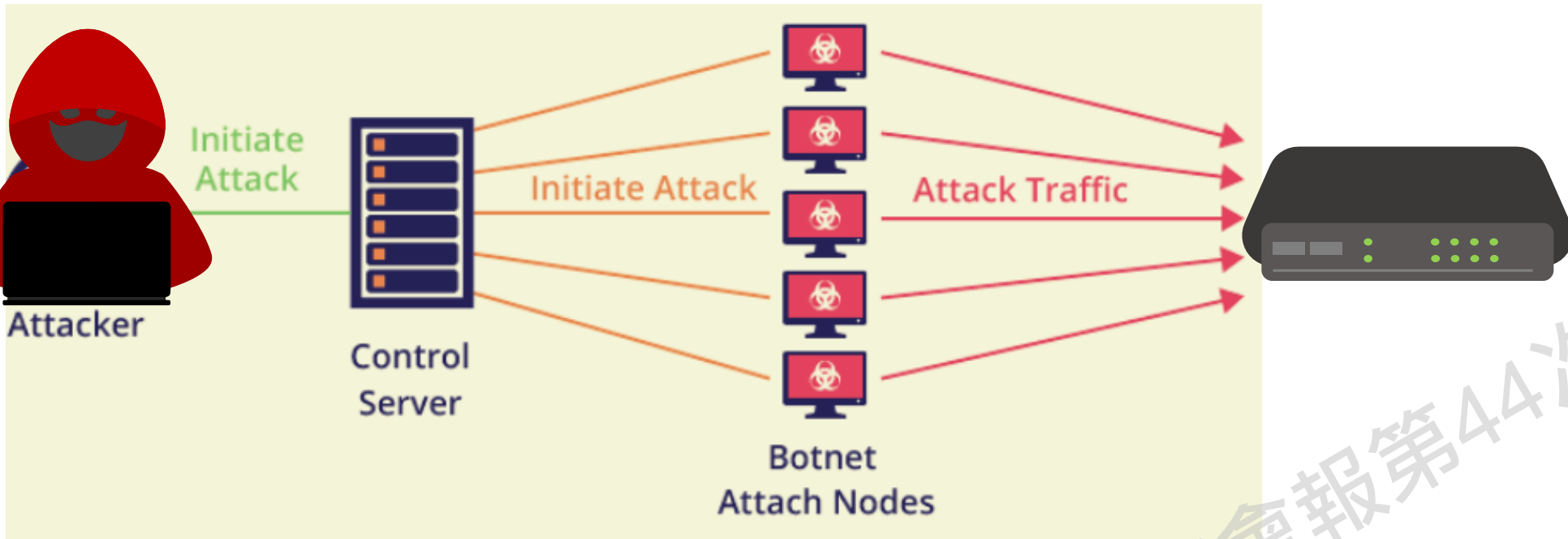
! Call Log 撥話紀錄 來源 IP 位置

- 中國香港 34.191.111.191
- 美國 23.191.111.242



參、漏洞分析（一）

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。

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。

Company	Protocol	Info	ASN	Le
Data Communic...	TELNET	2 bytes data	33254	
Data Communic...	TELNET	11 bytes data	33255	
Data Communic...	TELNET	Shenzhen Tenc...		
Shenzhen Tenc...	TCP			
Shenzhen Tenc...	TCP			
Shenzhen Tenc...	TELNET	<246e4ab6> Login:		
Shenzhen Tenc...	TCP	...		
Data Communic...	TCP	...		
Shenzhen Tenc...	TCP	...root		
Shenzhen Tenc...	TCP	icatch99		
Data Communic...	TELNET	...		
Shenzhen Tenc...	TELNET	...root		
Data Communic...	TCP	Password:		
Data Communic...	TELNET			
Data Communic...	TELNET	<246e4ab6> Login:		
Data Communic...	TELNET	enable		
Data Communic...	TELNET	enable		
Data Communic...	TELNET	system		
Data Communic...	TELNET			
Data Communic...	TELNET	Password:		
Data Communic...	TELNET			
Data Communic...	TELNET	<246e4ab6> Login:		
Data Communic...	TELNET	shell		

Wireshark · Follow TCP Stream (tcp.stream eq 27205) · capture_00000_20241001035

...<246e4ab6> Login: enable enable system Password: <246e4ab6> Login: shell

8 client pkt(s), 93 server pkt(s), 16 turn(s).

Entire conversation (293 bytes) Show as ASCII

紅線紅字為駭客嘗試登入輸入之登入帳號字串(密碼為空值)

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
```

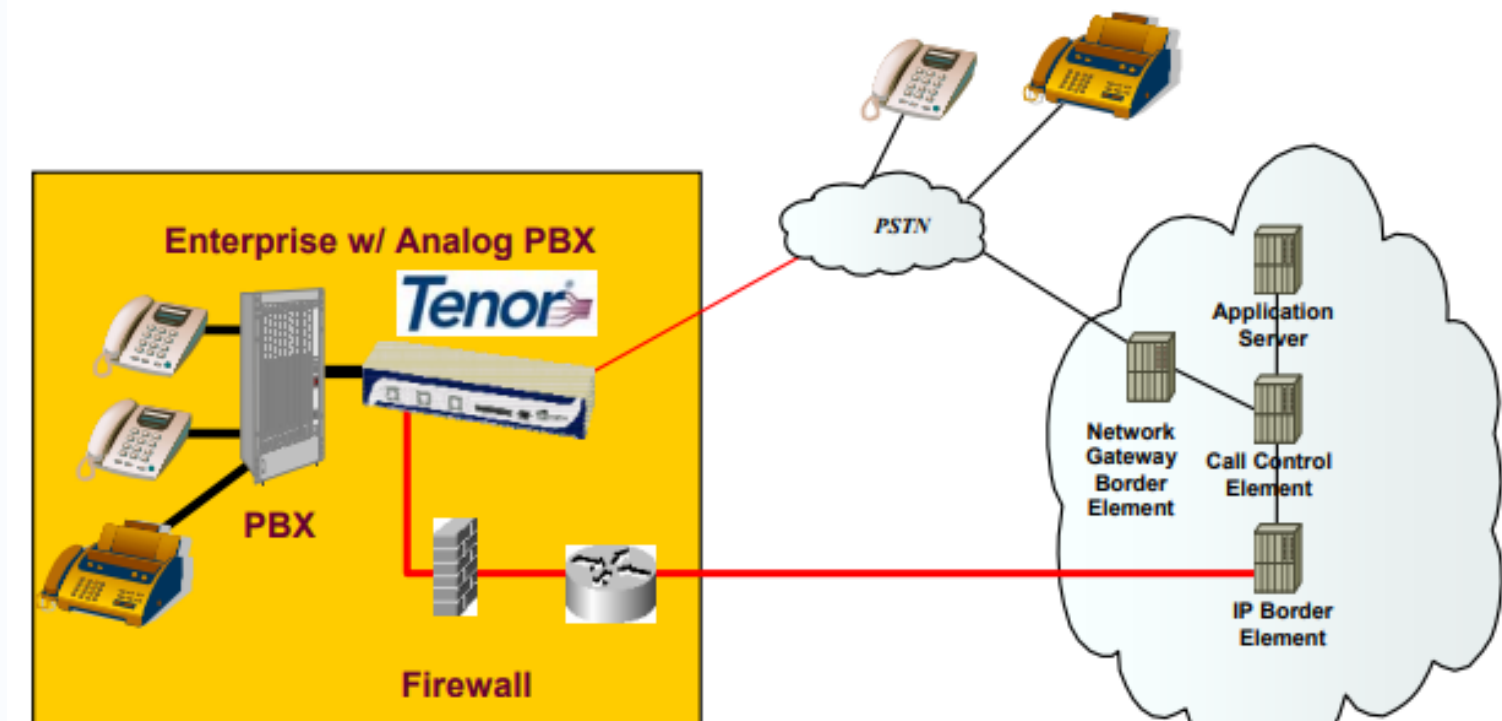
```
boot device      : emac
unit number      : 0
processor number  : 0
host name        : host
file name        : file
inet on ethernet (e) : 192.168.1.150:FEFF00
gateway inet (g)   : 211.1.1.254
user (u)         : g
ftp password (pw) : g
flags (f)         : 0x8
other (o)         : emac
```

```
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。



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20日 第2次通報

- 第2次通報A-ISAC與N-ISAC。



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

THANK YOU

限閱：行政院資安會報第44次委員會-會前公開簡報

