中國平價手機遭預裝惡意程式，20 多萬台設備受影響

中國平價手機廠商深圳傳音控股（TRANSSION）遭爆，於旗下品牌 Tecno 系列智慧型手機中安裝惡意程式，該惡意程式會在未經使用者允許的狀況下訂閱付費服務，截至目前已有 20 多萬台的設備出現可疑交易。

中國廠商傳音控股所生產的行動裝置傳音手機，靠著價格低廉的政策，以及為族群量身打造的功能，在開發中國家受民眾廣泛支持。根據 IDC 的調查，在東非國家中，傳音控股旗下品牌的市場佔有率高達 6 成以上，而其業務也逐漸遍及中東、南亞等國家。

根據海外科技媒體 TechRadar 報導，行動裝置資安廠商 Upstream，在中國平價手機品牌傳音所生產的設備上，發現被預先安裝的惡意後門軟體 Triada。這個後門軟體會導致使用者一旦啟用裝置並連接網際網路，將會在使用者不知情的情況下訂閱付費服務，用以竊取使用者的預付通話費。

Triada 是一種針對 Android 環境開發的木馬程式，一旦被安裝在設備上，將會以 ROOT 的權限來存取系統檔案與更改其設定，而攻擊者

可以透過C&C Server（命令控制伺服器），在受害設備上下載並安裝任意應用程式、存取設備檔案及簡訊，甚至訂閱付費服務。在安裝後，Triada會修改系統檔案及開機程序，將自身隱藏成系統應用程式，讓使用者無法移除該木馬程式。即使使用者將設備回復原廠設定，仍無法移除Triada木馬。

由於在中國、非洲及南亞等開發中國家，使用者必須預付款項於門號中，才能使用通話、行動網路等電信服務，而門號上的預付款在許多開發中國家也是唯一的電子支付方式。使用者在訂閱電信商或應用程式的付費服務時，通常需要使用簡訊來驗證，而Trida木馬程式能自動接收簡訊並傳送至攻擊者端，導致使用者在不知情的情況下，消耗預存通話費訂閱服務。根據報導，至今已經發現了20萬支行動設備上，共1,920萬筆的可疑交易，受害者遍佈全球19個國家。

儘管如此，傳音控股的行為卻未被Android系統開發商Google所譴責，相反地，Google在其安全團隊的部落格中表明，認為這些惡意程式的存在是源於上游供應商，而手機生產商只是誤用了含有惡意軟體的第三方元件。

※ 本文轉載於台灣電腦網路危機處理暨協調中心
彰化監獄政風室 關心您