# 惡意軟體即服務 Black Rose Lucy 現蹤

資安業者 Check Point 近期於官網發布訊息，發現一個名為 Black Rose Lucy 的全新惡意軟體即服務(Malware-as-a-Service，MaaS)，由 The Lucy Gang 俄國團隊所開發，雖然尚在發展的早期階段，但是 Check Point 認為，只需要一些時間，Black Rose Lucy 便能發展成網路攻擊的瑞士刀。

近年來網路犯罪逐漸走向專業化，在網路雇用傭兵或是購買 MaaS，作為進行惡意攻擊的一種手段已漸成常態。Check Point 表示，許多有心人士傾向雇用小型擁有特殊專業技能的團隊，而非具備攻擊技能組合完整的全功能團隊，而這些有心人士以類似購買雲端服務的方式，購買這些惡意軟體服務。這個 MaaS 乍看之下是一個惡意套件工具包，包含了遠端控制儀表板 Lucy Loader，用來控制整個殭屍網路的受駭裝置和主機，還可用來部署其他的惡意負載(Payload)，另一個工具則是 Black Rose Dropper，針對 Android 裝置設計來收集裝置資料、監聽遠端命令、控制 C&C 伺服器，並且安裝來自 C&C 伺服器發送的惡意軟體。

在 Check Point 發現的 Lucy Loader 實體中，系統正控制著位於俄羅斯的 86 台裝置，感染日期顯示為 2018 年 8 月初，Lucy Loader 儀表板還有世界地圖介面，為駭客顯示殭屍網路的地理位置概覽，駭客可以透過儀表板介面上傳惡意軟體，並將其推送至整個殭屍網路中。而 Black Rose Dropper 會偽裝成 Android 系統升級或圖片檔案，Check Point 所收集到的樣本，則會利用系統的無障礙服務來安裝有效負載，過程完全不需要用戶參與，並且會形成自我保護的機制。

Black Rose Dropper 安裝完成後，會立刻隱藏其圖標，並且向系統註冊監控服務，在 60 秒後，監控服務會向用戶顯示警示訊息，聲稱受害者裝置有安全危機，要求使用者替名為系統安全的應用程式啟用 Android 無障礙功能，而事實上這個系統安全應用程式正是 Black Rose Dropper，他會不停地要求受害者

授予權限，直到達成目的。只要 Black Rose Dropper 取得無障礙功能權限後，就能給予自己系統管理員權限，以便能在其他應用程式畫面前顯示視窗，並且忽略 Android 電池最佳化權限，以避免被節電政策消滅。監視服務會在每次使用者關閉和開啟螢幕時重新啟動，以確保惡意軟體服務總是有效的。Check Point 表示，目前這個階段，監控服務的行為主要都是從 C&C 伺服器獲取 APK 檔案後安裝，並將日誌檔案送回 C&C 伺服器，內容包括裝置狀態、Black Rose 執行的狀態以及任務執行的狀態資料。

由於 Android 的無障礙服務可以模擬使用者點擊螢幕事件，而這是 Black Rose 之所以能夠執行惡意活動的關鍵因素，一旦無障礙功能啟動後，Black Rose 便會透過切換螢幕模擬使用者點擊事件，迅速的授予自己系統管理員權限。在部分 Black Rose 的樣本中存在自我保護機制，會積極的檢測系統是否存在安全工具，在必要的時候停用這些應用程式。在 Check Point 整個調查過程中，Black Rose Lucy 還推出了新版本，顯示 The Lucy Gang 團隊正積極地維護並改進這個工具。新版本 Black Rose Dropper 加強了控制通訊能力，新版本的 Lucy Loader 儀表板則將殭屍網路改採用 DEX 負載而非 APK，強化惡意軟體入侵能力。

目前 Black Rose Dropper 支援英語、土耳其語和俄語使用者介面，且儀表板中顯示，模擬的受害者位在法國、以色列和土耳其。Check Point 認為駭客已經在這些地方向有興趣的買家進行了展示，因此 Black Rose Lucy 目標的範圍應該不只俄羅斯，而且由於 Black Rose Lucy 還對小米手機進行特殊邏輯處理，其中的自我保護機制還特別針對中國安全和系統應用進行特化，因此下一個目標是中國的可能性非常大。