資安事件應變方法-智慧手機惡意程式

＃資料來源：CERT SOCIETE GENERALE http://cert.societegenerale.com/en/publications.html

摘要

這份 IRM 小抄，專給想要精確調查安全事件的事件處理者們

誰應該要使用 IRM 小抄呢

- 管理者
- 安全營運中心
- 資訊安全總監與代理人
- 電腦緊急應變中心

記住：面對事件時，跟著 IRM 的流程，記下記錄不要驚慌。如果需要請立刻聯絡你的電腦緊急應變中心。

事件處理步驟

處理安全事件六個步驟

準備：準備好處理事件

確認：調查事件

封鎖：限制事件的影響

修正：移除威脅

復原：復原到正常階段

後續情況：制訂並改進流程

IRM 裡提供每個步驟的詳細資訊

一、 準備

目標：建立聯繫、確定程序、收集資料以達到在被攻擊時節省時間的目的。

- 行動服務平台必須定義一套程序來應對可疑的惡意軟體感染：將該用戶的智慧型手機替換成一支新的，並且將可疑的設備隔離並交由鑑識人員來分析。
- 對智慧型手機平常的活動有良好的知識是值得讚賞的(在上面運行的預設及其他的工具)，智慧型手機的支援專家對於協助取證調查會有幫助。
- 監控應該要確認不尋常的用戶帳單或網路活動。

二、 確認

目標：檢測事件、決定其範圍並連絡相關單位。

可疑智慧型手機的通知重點：

- 防毒發出警報
- 不尋常的系統活動，異常緩慢的系統。
- 不尋常的網路活動，非常緩慢的網路連線。
- 系統在沒有理由的情況下重新開機或關機。
- 一些應用程式發生非預期的崩潰。
- 使用者收到一個或多個簡訊，有些可能含有不尋常字元(SMS，MMS，藍芽訊息等。)
- 在不尋常的時間、日期有不尋常的通話到不尋常的手機號碼。
- 網站網址這些證據需要被收集。
- 詢問使用者他平常使用手機的活動：上哪些網站、安裝那些額外的應用程式。這些資訊可以選擇性地與公司的政策做交叉驗證。

三、 封鎖

目標：採取行動阻止攻擊

- 確認使用者被給予了一個暫時或新的永久裝置來避免時間對於調查的限制。
- 備份智慧型手機資料。
- 移除電池來阻擋任何活動(wifi、藍芽等)
- 使用防毒軟體來檢查曾與該智慧型手機進行同步以及連接的電腦。
- 將可疑的智慧型手機以及適當的配件(SIM 卡、電池、電源線、記憶卡)到你的安全事件處理團隊。這個團隊會幫忙隔離惡意的內容，並且將之送到防毒軟體公司。

四、 修正

目標：採取行動來移除威脅，並且避免未來再次發生。

如果有一些加密或密碼存取被設定，嘗試找出一個方法來取得這些儲存的檔案，如果這是不可能的，那麼調查會受到很大的限制。

你們的事件處理團隊應該要使用特定來工具來對智慧型手機進行採證調查。

僅是提供資訊，這邊有簡短的清單列有一些好用的工具：

免費工具：XDA Utils (Windows Mobile)、MIAT (Mobile Internal Acquisition Tool–Symbian、Windows Mobile)、TULP2G、Blackberry Desktop Manager

商業軟體：XRY、Cellebrite、Paraben

採取的行動：

- 移除智慧型手機的 SIM 卡，如果還沒這樣做。
- 復原手機歷史紀錄、網頁紀錄以及所有可用的紀錄檔。
- 如果可以，復原伺服器連接記錄檔。
- 辨識並移除手機上的威脅。
- 如果威脅與某個已經安裝的應用軟體有關，辨識出它的在網路上的位置並移除它。

五、 復原

目標：將系統回復為正常。

如果使用者需要從感染支援中回復，定義一個隔離期間以及適當的防毒檢驗，如果可能的話，確定沒有任何東西會傷害使用者以及公司的系統。

復原先前存放在可以信任來源的資料到目標裝置上。

一旦調查結束，清除被感染的智慧型手機(如果有可能的話)並且還原到有最原始韌體以及檔案系統的原廠狀態，以讓人可以再次使用。

六、 後續情況

目標：將事件的詳細內容文件化、討論在事件所學到的事情以及調整計畫及防禦。

報告

需要寫一份事件報告並且所以的參與者都可以取得。

以下是一些需要被描述到的議題：

- 最初的偵測
- 採取的措施以及時間軸
- 哪些事情做對了
- 哪些事情做錯了
- 事件造成的花費

讓使用者聽取報告以提升使用者對於安全問題的意識。