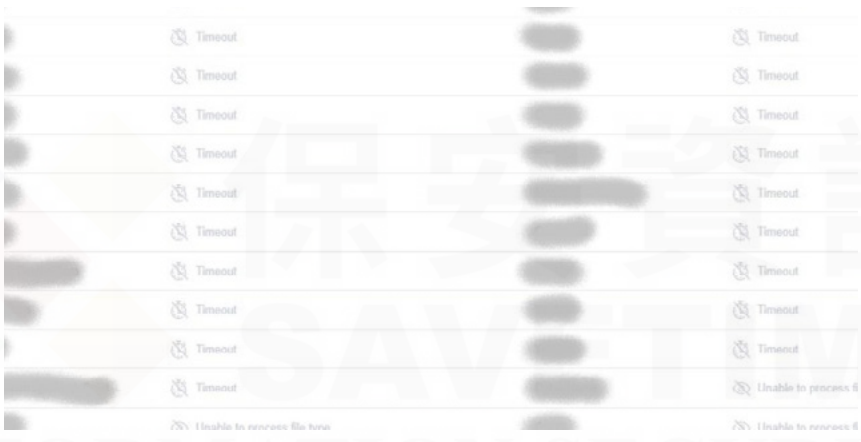
『模擬』Android阻斷服務攻擊 (DoS)

2023 年 5 月 15 日發布

在我們 7x24 的日常工作中，我們會不斷監控異常和跡象，這些異常和跡象可能顯示存在試圖逃避安全檢測的全新威脅或經過修改的威脅。我們的自動化系統最近提醒我們注意一個問題，即在檢測特定 Android 手動安裝包 .APK 的樣本時，我們的雲端掃描明顯變慢。快速瀏覽一下就會發現，幾個有問題的樣本也對更廣泛的自動化掃描系統效能產生輕微影響。

VirusTotal 其他供應商似乎受到的不利影響更大，在分析期間顯示逾時 (Timeout)，這實際上看起來像是一次行動裝置的分散式服務阻斷 (DDoS) 攻擊。



深入研究樣本顯示了以下特性：

- 每個容器樣本都包含大量（最多 32K）、很小的檔案
- 這些很小的檔案包含看起來像隨機字串的內容，並且似乎沒有被 APK 使用
- APK 本身似乎是自動化產成
- 手動安裝包名稱似乎也是隨機自動生成
  * hbjvuozxxuhpyfbnvxtd.dxgbesgyxlsvkccgozbi.deomdyhhwgeraghfzrds
  * dknmmohvktzcmopltehs.yrrnbpuvyctwiefeeycz.gtwxbuikrwakaehwpazg

透過行為分析，我們確定這些 APK 樣本主要是廣告軟體／灰色軟體，和其他可能不需要但不全然是惡意的程式，被統稱為潛在有害程式 (Potentially Unwanted Applications，PUAs)。其中某些連接到遠端伺服器以取得跟廣告相關的設定或與管理推送通知或位置服務的部份軟體開發套件 (SDK) 整合。

迄今為止，我們已經看到超過 11,000 個此類樣本（每個樣本包含超過 30,000 個檔案）。我們相信它們可能是某種測試--因此標題中使用『模擬』這個詞彙--但很難確定這種測試是由安全研究人員，還是有惡意意圖的人士所進行。

學習和適應的能力對於一家安全公司的成功非常重要，我們立即修改我們的自動化程序，以便更有效地分析這些樣本，有效地克服之前觀察到的處理性能下降。

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。

個別的內含在SES／SESC 賽門鐵克行動裝置威脅防禦型錄最新版下載，請點擊此處。