張貼日期：2019/11/26

【資安攻擊預警】駭客利用惡意檔案竊取臉書帳號資訊

主旨：駭客利用惡意檔案竊取臉書帳號資訊

說明：

- 內容說明
  - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-ANA-201912-0001
  - 駭客散佈含有木馬的惡意PDF reader檔案，引誘使用者下載執行後，會從瀏覽器的SQL Lite DB中竊取使用者的Facebook sessions cookies並利用此sessions cookies連線至臉書，獲取使用者Ads Manager 帳戶的敏感資訊，藉以散佈廣告或不實訊息等惡意攻擊。
  - IOCs
    1. 可疑網址與IP:
       - smartpdfreader.com, pdfaide.com, pdfguidance.com, ytbticket.com, videossources.com
       - www.ipcode.pw, www.gaintt.pw
       - 185.130.215.118, 155.138.226.36
    2. 可疑檔案:
       - d56e00af1562ee3890a132cde6a9b8f8a7b68d73c1532ab5dad046c7cf5c20f3
       - ede475db32026a207a54ed924aa6e2230911dc1cce95fb0aa3efbdfd5f4de9e1
       - a415624fe4fbce9ba381f83573d74f760197ad2371d4e4a390ea5722fad755cb
       - 25c60987a0148c19477196257478f14c584600acd742369cb8859256ff005400
- 影響平台: Windows
- 建議措施:
  1. 勿隨意點擊下載/執行 來源不明的檔案
  2. 防毒軟體定期掃描更新
  3. 根據 IOCs 阻擋/偵測異常連線，並檢查電腦系統是否存在惡意程式
- 參考資料:
  1. https://www.bleepingcomputer.com/news/security/facebook-ads-manager-targeted-by-new-info-stealing-trojan
  2. https://twitter.com/malwrhunterteam/status/1201552349715673088

計算機與通訊中心
網路系統組 敬啟