保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

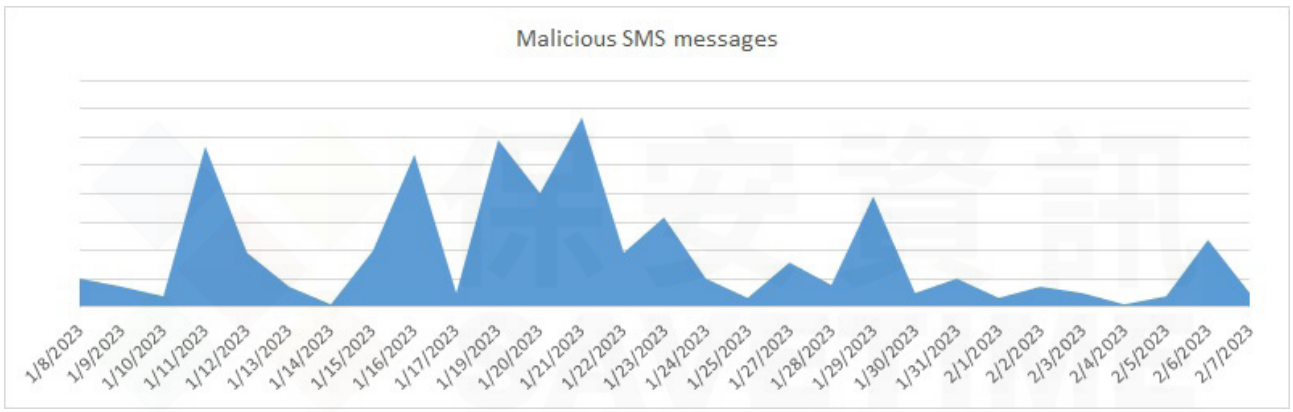
手機行動惡意軟體以日本為目標

2023 年 2 月 13 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

在過去的幾個月裡，針對日本手機用戶實施 (包括消費者和企業) 攻擊行動不斷，其中含針對安卓 (Android) 的惡意軟體和針對 iPhone 的網路釣魚。

攻擊行動的方法保持不變，攻擊者繼續使用惡意簡訊作為感染手段，並利用免費的動態 DNS 代管服務 Duck DNS 使用子網域。被這些簡訊引誘的安卓用戶會被重導向假冒的 Softbank 和 KDDI 網站，並被提示下載假冒的手機安全 APP。iPhone 用戶被重導向到一個虛假的電子帳單系統網站。下面是過去一個月的攻擊模式，每個峰值代表一個新的活動。



在這兩種平台 (Android 和 iPhone)，重新轉導向到的最終的網域會有所不同，顯然該攻擊行動比想像的更複雜。以下是常見的接收到的詐騙簡訊內容的樣本 :

* 【国税庁】重要なお知らせ、必ずお読みください
* 【国税庁 18:30】未払い税金お支払いのお願い。詳細はこちら【TT499】
* 【重要なお知らせ】未払い税金お支払いのお願い。ご確認ください【TQ177】
* 【重要なお知らせ HD474】SoftBank未払い料金お支払いのお願い
* 【12月6日利用停止予告】SoftBank未払い料金お支払いのお願い
* 【要確認】SoftBank重要なお知らせ、必ずお読みください
* 【ソフトバンク】お支払期限を過ぎた利用料金があります〔12月9日〕
* 【利用停止予告】KDDI未払い料金お支払いのお願い

本月初所發起的新一輪攻擊涉及 757 個使用 [10randomletters][.]duckdns[.]org 規則組合的 Duck DNS 子網域。偽裝成來自 Softbank 和 KDDI 的安全軟體的 Android 惡意軟體具有以下功能 :

- 更改內定的簡訊APP
- 收集聯絡人、已安裝的APP、電話號碼和簡訊並將它們轉發送到遠端伺服器
- 未經用戶同意發送簡訊
- 如果偵測到特定組合規則的網域，則修改或刪除簡訊內容

從本質上來講，這種惡意軟體能夠操控受害者的手機使其成為魁儡／機器人，也能夠進一步傳播感染源和／或發動以受害者手機電話簿上的聯絡人及其他收集到的電話號碼來進行詐騙行動。此外，歹徒還可以存取透過簡訊發送的機敏雙重驗證／兩步驟驗證 (2FA) 驗證碼。這對消費者和企業都有極大的風險。

日本是擁有大量智慧型手機用戶的科技先進國家，當然也是網路駭客認為最有利益可圖的目標，歹徒企圖入侵行動手機裝置以竊取敏感資訊並進一步傳播他們的惡意軟體。這些類型的攻擊只會日益增加。

賽門鐵克已經於第一時間提供多種有效保護 (**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- AdLibrary:Generisk
- AppRisk:Generisk

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

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。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。