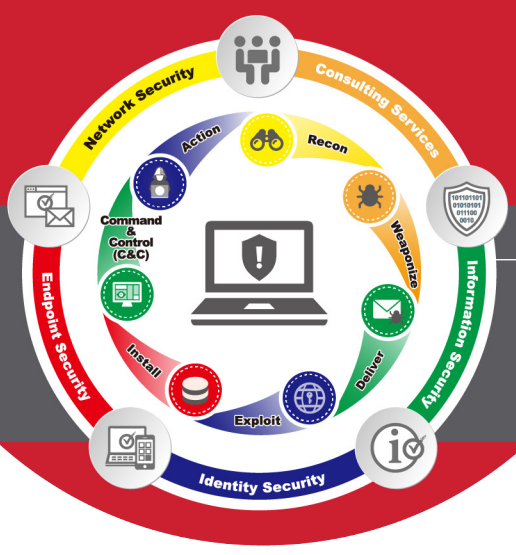


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

補足EMM不足，賽門鐵克行動威脅防禦(MTD)有效保護Microsoft身分識別平台內的識別碼權杖實例

2024 年 11 月 19 日發布

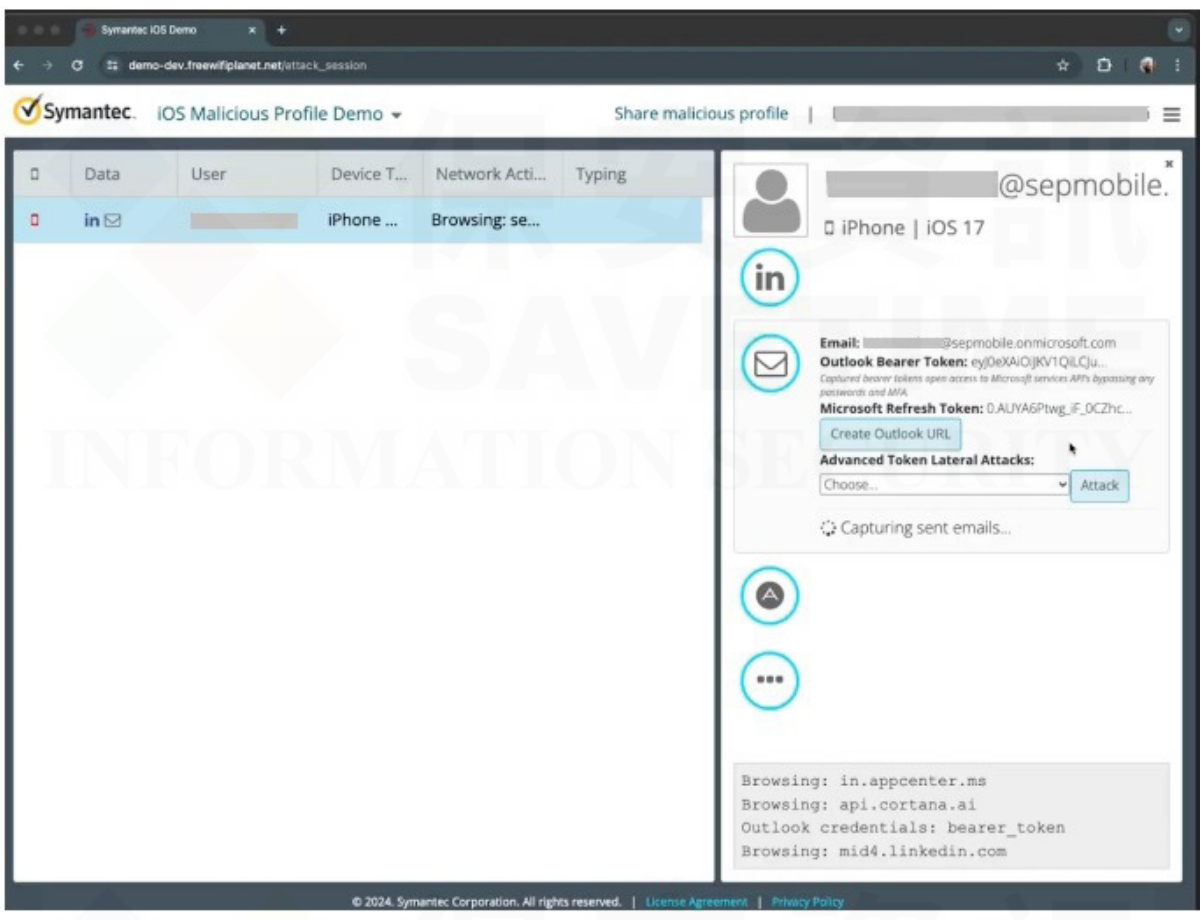
點擊此處可獲取--最完整的賽門鐵克解決方案資訊

當今的組織通常依賴一套被稱為企業行動管理解決方案 (Enterprise Mobility Management，EMM) 的政策與程序來監控與管理企業與員工的行動裝置。賽門鐵克最近檢視一家現實世界財富 500 大企業的行動裝置相關聯事件，該企業在全球擁有超過 400,000 名員工。我們團隊研究那些原本僅依賴 EMM 面對威脅的不堪一擊，與賽門鐵克行動威脅防禦 (MTD：Symantec Mobile Threat Defense) 保護所阻止攻擊形成的強烈對比。

拆解攻擊與解析 MTD 的防禦能力

其中一個攻擊媒介是利用惡意的 iOS 設定檔，透過中間人 (MiTM) 攻擊攔截 Microsoft 身分識別平台內的識別碼權杖。攻擊者以公司的 Active Directory 為目標，目的是繞過多因素驗證 (MFA) 來取得這些權杖--實際上就是存取公司資源的「通行天國之鑰」。

威脅者從公開和／或暗網收集員工聯絡資訊後，先發送大量的網路釣魚簡訊，偽裝成 IT 更新的訊息。當點選這些訊息時，就會下載惡意設定檔並安裝到員工的 iOS 裝置上。這些設定檔會重新路由和解密加密流量，讓攻擊者攔截敏感資料和存取公司資源 (例如：Outlook 和 Intune) 所需的憑證權限。



攻擊者如何存取使用者 Outlook 帳戶的範例

攻擊者濫用盜取的權杖，在網路中進行橫向移動，取得不受限制的存取權限，卻沒有觸發任何記錄或警示。所幸有使用賽門鐵克行動威脅防禦 (MTD：Symantec Mobile Threat Defense)，在端點識別並阻 止了這個攻擊鏈。

總而言之

- 該財富 500 大企業中有 3% 使用者成為簡訊網路釣魚攻擊的目標，所幸受到 MTD 提供的安全保護。
- 400 位使用者安裝不受信任的設定檔，因為有 MDM 保護，所以無法存取公司內部服務和資料。
- 25% 使用者成為採用解密用戶端流量的中間人 (MiTM) 攻擊之潛在目標。賽門鐵克 MTD 在攻擊者有機會存取公司內部服務和資料之前，就已識別並阻擋這些潛在攻擊。

如需關於行動平台上的攻擊和防護策略的更多深入見解，請參閱我們的白皮書《保護您的行動企業》：僅有 EMM 是不夠。

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 年起就全心全力專注在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使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。