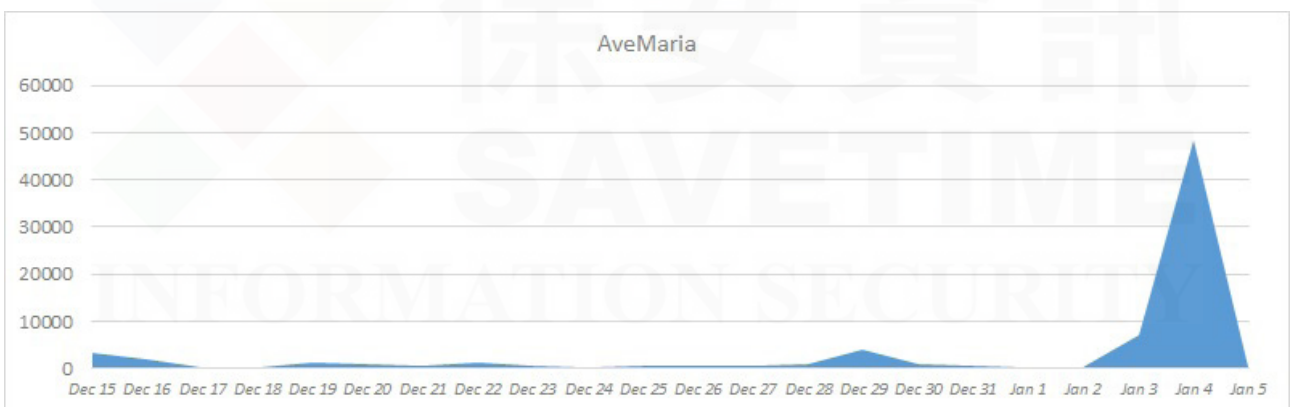
賽門鐵克多層次防護機制讓 AveMaria RAT 落荒而逃

2023 年 1 月 6 日發布

AveMaria (也稱為 Warzone RAT) 是一種遠端存取木馬 (RAT)，首次出現於 2018 年底前後，它具有從受害者那裡竊取資訊的能力，儘管某些變種還具有其他功能，例如：遠端桌面存取、提升用戶權限和啟動相機。它通常透過包含惡意附件的垃圾郵件“網路釣魚”行動傳播，或者在某些情況下鏈接到代管在合法雲端服務和檔案共享平台上的惡意檔案。相對於其他一些 RAT，AveMaria 沒有很流行，但它持續定期針對廣泛的商業部門發動垃圾郵件攻擊，雖然它似乎主要集中在 EMEA (歐洲、中東及非洲) 地區，但也包括在美國、中東和亞太地區的企業組織。

賽門鐵克安全機制應變中心，每天都會收到警報並調查涉及多種威脅的不同程度的威脅活動，但在 1 月 4 日至少有三種不同類型的防護技術同時偵測到，提醒我們留意 AveMaria 涉及的網路攻擊大幅增加。我們的 .NET 模擬器將其識別為 MSIL.Downloader!gen8，我們的機器學習技術將該攻擊識別為 Heur.AdvML.B，並且我們的一個啟發式技術權重機制將其歸類為 Scr.Malcode!gdn32。



值得注意的是，這種特殊的攻擊採用雙重副檔名伎倆，惡意郵件附件內含“.pdf.exe" 之.gz 格式的自解壓縮檔附件。

賽門鐵克擁有領先業界的 **零時差** 保護技術，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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Downloader!gen8
- Scr.Malcode!gdn32

基於機器學習的防禦技術：

- Heur.AdvML.B

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

要了解有關賽門鐵克雲端郵件安全服務的更多資訊，請點擊此處下載我們型錄及簡報檔。
要了解有關賽門鐵克安全(SEP/SESE/SESC)的更多資訊，請點擊此處下載我們型錄及簡報檔。

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**。