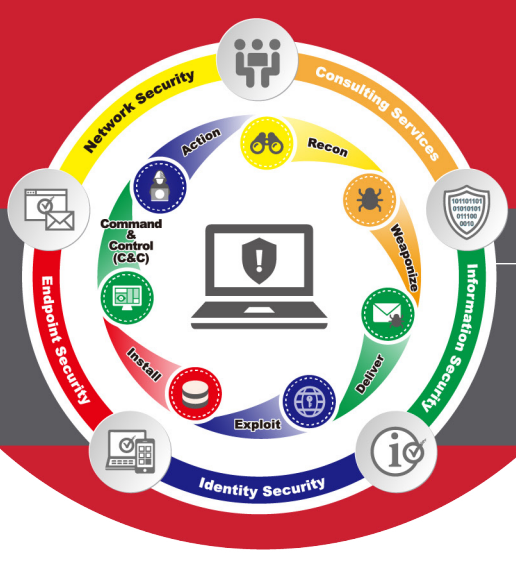


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

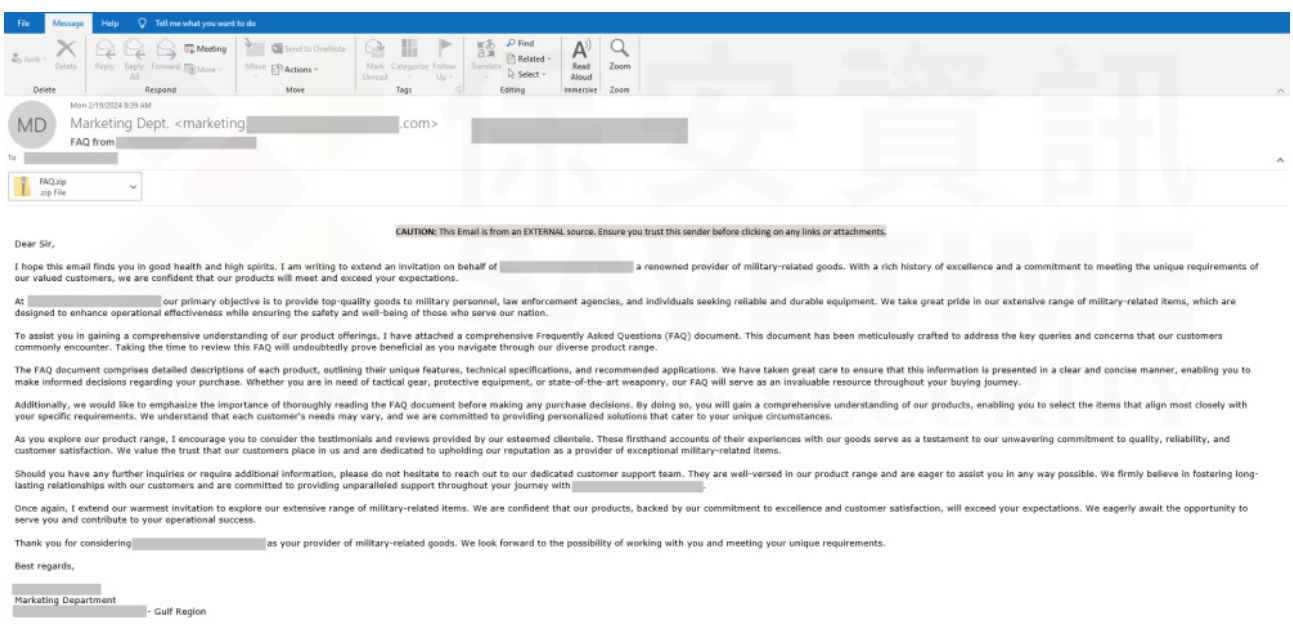
針對中東各國政府的網路攻擊

2024 年 3 月 6 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

在東歐和中東持續不斷的衝突中，一個網路惡棍一直在策劃針對中東各國政府的網路間諜行動。這些網路威脅行動利用該地區因長期衝突而加劇的恐懼和緊張局勢。這些惡意行動只會加劇對受影響政府及其人民的干擾，對該地區的穩定和安全構成更大的威脅。

攻擊行動是透過精心設計過的魚叉式網路釣魚電子郵件發起，攻擊者冒充一家信譽良好的美國航太和國防公司。這些精心製作的電子郵件大多以軍事和執法勤務裝備機具為主要誘餌。實際上，攻擊者誘使用戶存取他們偽造的常見問題 (FAQ) 檔案。在該檔案中，除了提供每種產品的獨特屬性、技術規格和推薦應用外，還提供詳細的說明。



CAUTION: This Email is from an EXTERNAL source. Ensure you trust this sender before clicking on any links or attachments.

Dear Sir,

I hope this email finds you in good health and high spirits. I am writing to extend an invitation on behalf of [redacted] a renowned provider of military-related goods. With a rich history of excellence and a commitment to meeting the unique requirements of our valued customers, we are confident that our products will meet and exceed your expectations.

At [redacted] our primary objective is to provide top-quality goods to military personnel, law enforcement agencies, and individuals seeking reliable and durable equipment. We take great pride in our extensive range of military-related items, which are designed to enhance operational effectiveness while ensuring the safety and well-being of those who serve our nation.

To assist you in gaining a comprehensive understanding of our product offerings, I have attached a comprehensive Frequently Asked Questions (FAQ) document. This document has been meticulously crafted to address the key queries and concerns that our customers commonly encounter. Taking the time to review this FAQ will undoubtedly prove beneficial as you navigate through our diverse product range.

The FAQ document comprises detailed descriptions of each product, outlining their unique features, technical specifications, and recommended applications. We have taken great care to ensure that this information is presented in a clear and concise manner, enabling you to make informed decisions regarding your purchase. Whether you are in need of tactical gear, protective equipment, or state-of-the-art weaponry, our FAQ will serve as an invaluable resource throughout your buying journey.

Additionally, we would like to emphasize the importance of thoroughly reading the FAQ document before making any purchase decisions. By doing so, you will gain a comprehensive understanding of our products, enabling you to select the items that align most closely with your specific requirements. We understand that each customer's needs may vary, and we are committed to providing personalized solutions that cater to your unique circumstances.

As you explore our product range, I encourage you to consider the testimonials and reviews provided by our esteemed clientele. These firsthand accounts of their experiences with our goods serve as a testament to our unwavering commitment to quality, reliability, and customer satisfaction. We value the trust that our customers place in us and are dedicated to upholding our reputation as a provider of exceptional military-related items.

Should you have any further inquiries or require additional information, please do not hesitate to reach out to our dedicated customer support team. They are well-versed in our product range and are eager to assist you in any way possible. We firmly believe in fostering long-lasting relationships with our customers and are committed to providing unparalleled support throughout your journey with [redacted].

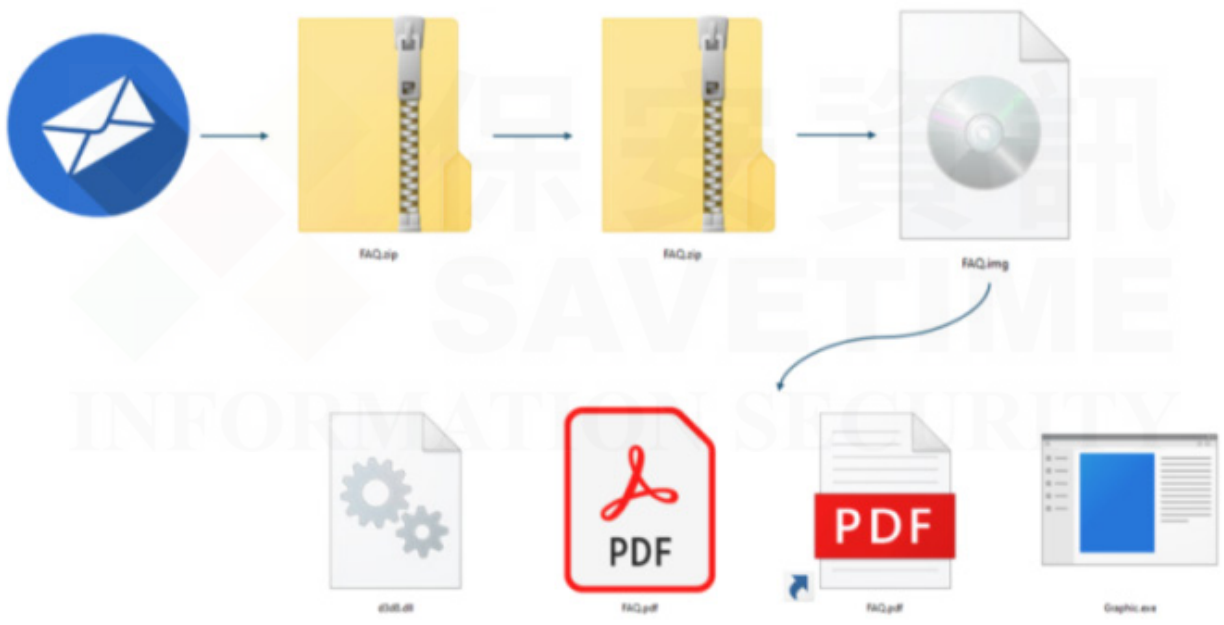
Once again, I extend our warmest invitation to explore our extensive range of military-related items. We are confident that our products, backed by our commitment to excellence and customer satisfaction, will exceed your expectations. We eagerly await the opportunity to serve you and contribute to your operational success.

Thank you for considering [redacted] as your provider of military-related goods. We look forward to the possibility of working with you and meeting your unique requirements.

Best regards,

[redacted]
Marketing Department
[redacted] - Gulf Region

如果用戶不疑有他被誘騙開啟所附的 ZIP 檔 (FAQ.zip)，就會遇到另一個同名的 ZIP 檔 (FAQ.zip)，其中包含一個 IMG 壓縮檔 (FAQ.img)。第二個壓縮檔包含一個 PDF 誘餌 (FAQ.pdf)，以及惡意捷徑檔 .LNK (FAQ.pdf.lnk)、EXE (Graphic.exe) 和 DLL (d3d8.dll) 等檔案。



執行後，惡意 .LNK 捷徑檔將啟動 PDF 誘餌，同時在後臺執行 EXE 檔。此外，DLL(d3d8.dll) 會使用搜尋序劫持技術載入。然後，該 DLL 會載入解密後的後門程式碼，進而啟動系統指紋識別，並開始對主機進行 C&C 註冊，分配亂數 ID，這些 ID 處於待機狀態，以接收和執行進一步命令。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Backdoor Trojan

基於機器學習的防禦技術：

- Heur.AdvML.C

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

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)。

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security 內建的預設強化政策，即能保護 MS Office 應用程式。
- DCS 可防止 MS Office 應用程式將命令直譯器 (包括 cmd.exe、powershell.exe 或 winrar.exe／winzip.exe 作為子程序) 啟動。
- DCS 將阻止任何可執行檔在該威脅的攻擊鏈上進一步執行。
- 為了提供更進一步的保護，客戶可以設定 DCS 網路規則，為特權服務和應用程式設置網路存取權限。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲深入瞭賽門鐵克端點安全完整版的調適型防護 (Adaptive Protection) 功能，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲瞭解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。

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**。