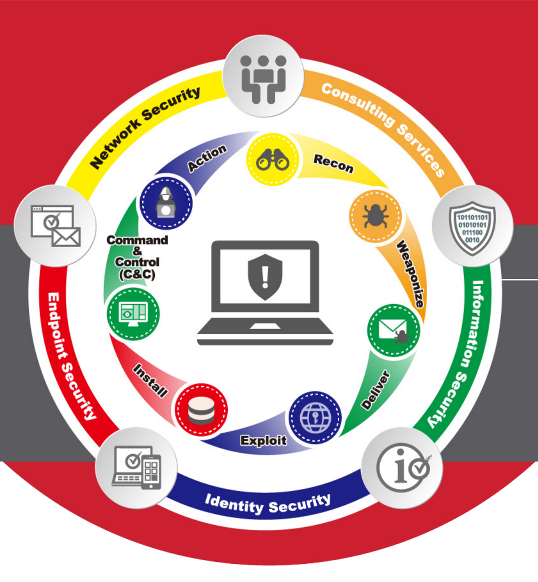


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

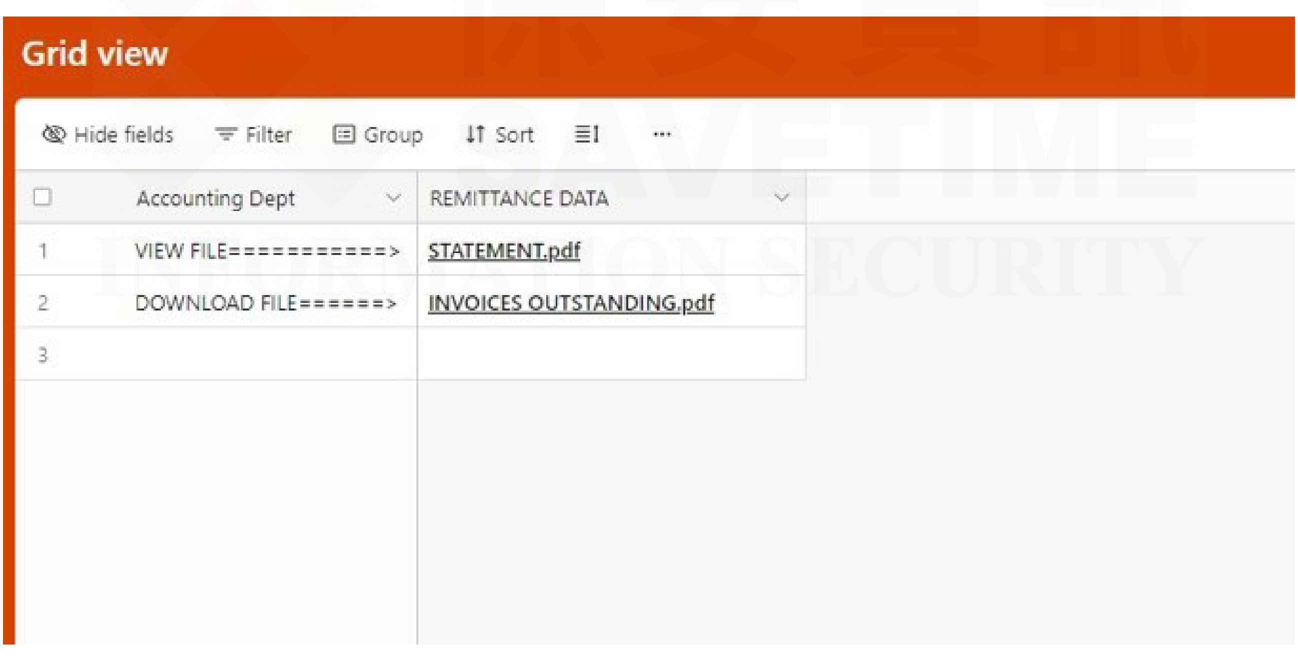
賽門鐵克的網頁生態即時分類系統--WebPulse 持續偵測到唯妙唯肖的釣魚、詐騙網站

2024 年 10 月 15 日發布

點擊此處可獲取--**最完整的賽門鐵克解決方案資訊**

賽門鐵克的網頁生態即時分類系統--WebPulse 持續偵測到可能來自俄羅斯 Microsoft Outlook 主題網路釣魚活動的內容。惡意網域名稱及遭濫用網際網路服務上的某些子網域 (例如：page[.]dev 和r2[.]dev) 傳回的內容包含指向其他網域的連接，這些網域傳回 Microsoft Outlook 的偽裝內容，然後該內容被有關汽車收藏的引誘內容所取代。

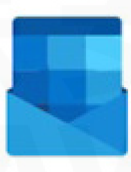
例如：hxxps://airtable[.]com/appCFZIhXR4xkRsBW/shrBlLd0rIPEHc6VC/tblHMgIOgYgGhRnt2 傳回以下內容：


Grid view

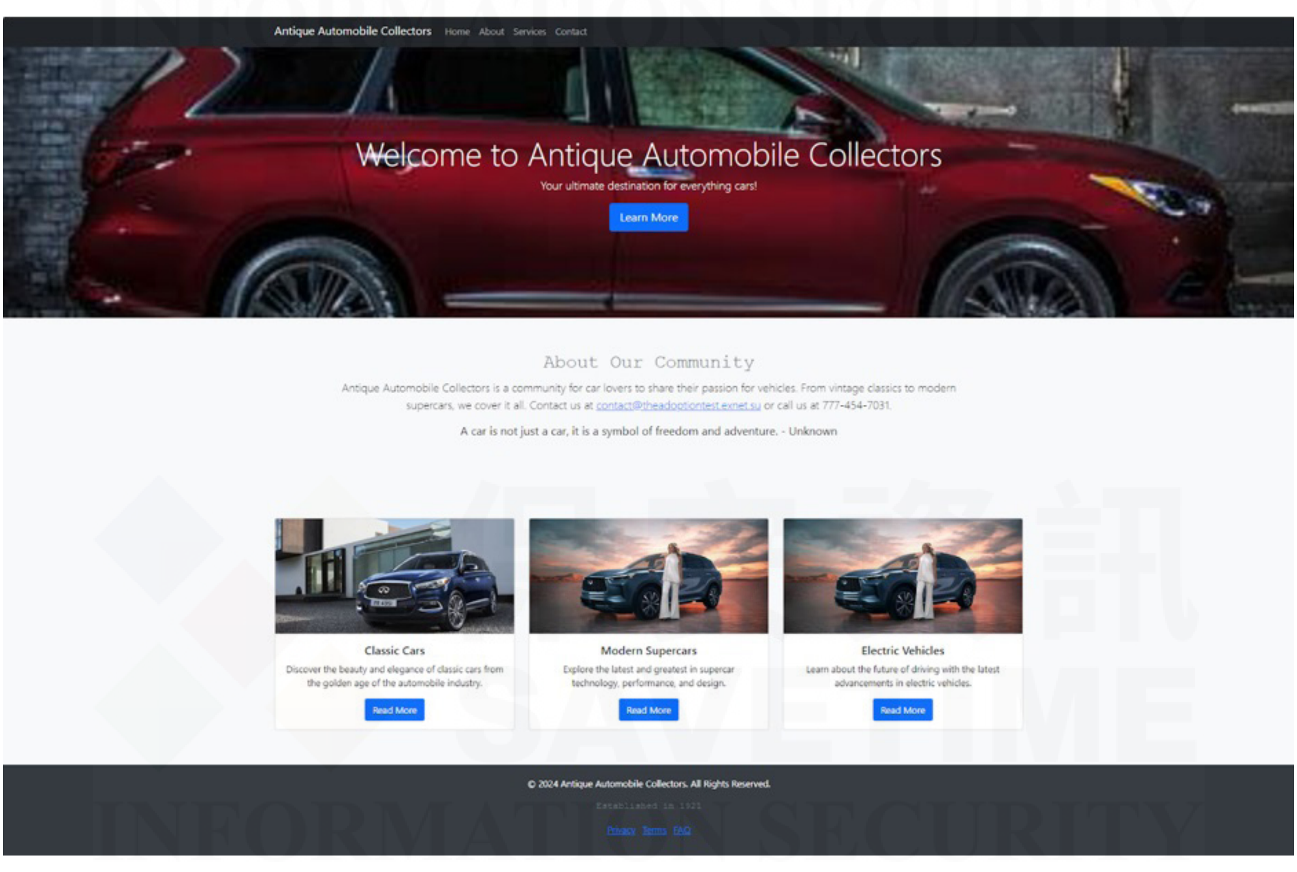
Hide fields · Filter · Group · Sort

	Accounting Dept	REMITTANCE DATA
1	VIEW FILE===========>	STATEMENT.pdf
2	DOWNLOAD FILE=======>	INVOICES OUTSTANDING.pdf
3		

兩個 .pdf 檔名都會連結到 hxxps://shopzingr[.]bir[.]ru/eXgHl/，該鏈結隱藏在 CLOUDFLARE 的「CAPTCHA」辨認人類與機器人的驗證系統驗證碼複選框後面。勾選該方塊後，會短暫顯示此 Microsoft Outlook 圖示：



然後它會被一個有關汽車收藏的詐騙網站所取代。在此範例中，詐騙網站的標題是『Antique Automobile Collectors*古董車收藏網站』並顯示以下內容：


Antique Automobile Collectors Home About Services Contact

Welcome to Antique Automobile Collectors

Your ultimate destination for everything cars!

Learn More

About Our Community

Antique Automobile Collectors is a community for car lovers to share their passion for vehicles. From vintage classics to modern supercars, we cover it all. Contact us at contact@theadoptiontest.exnet.su or call us at 777-454-7031.

A car is not just a car, it is a symbol of freedom and adventure. - Unknown

Classic Cars

Discover the beauty and elegance of classic cars from the golden age of the automobile industry.

Read More

Modern Supercars

Explore the latest and greatest in supercar technology, performance, and design.

Read More

Electric Vehicles

Learn about the future of driving with the latest advancements in electric vehicles.

Read More

© 2024 Antique Automobile Collectors. All Rights Reserved.

Established in 1921

Privacy Terms FAQ

WebPulse 偵測到此活動並即時回應到 WebPulse 的網頁分類平台並歸為釣魚網頁。自 2024 年 9 月 10 日到 10 月 10 日，WebPulse 偵測到 1,106 個獨立網域。下圖顯示與此活動相關的新網域首次搜尋的計數：

獨立的網域使用以下 TLD／ccTLD (註：頂級網域／國家或地區的頂級網域)：

- .ru (520)
- .com (102) (註：包括 sa[.]com 和 za[.]com 上託管的許多子網域)
- .dev (86) (註：主要被濫用的pages[.]dev 和r2[.]dev 服務)
- .site (72)
- .pl (69)
- .de (58)
- .id (32)
- .shop (25)
- .moscow (25)
- .su (24) (註：莫斯科地區的網域名稱)
- .pro (22)
- .sbs (13)
- .uk (12)
- .top (10)
- .buzz (8)
- .cyou (7)
- .online (6)
- .store (4)
- .space (3)
- .ua (2)
- .me (2)
- .art (2)
- .hu (1)
- .cfd (1)

偵測到的網域範例包括：

Domains／網域

- 0700ihrenummer[.]msk[.]ru
- 1349653976[.]my[.]id
- bytevault[.]com[.]de
- bytevault[.]ru
- cloudcogmputing[.]ru
- digitalbuzztechmo[.]ru
- digitalgroovetechieno[.]shop
- enterlifegrooved[.]com[.]pl
- entertaintechtrendsro[.]ru
- fggiggle[.]site
- gadgetgroovees[.]shop
- payment-to-your-bank-urska-zupanc-lasic-hidrotehnik-si[.]dynamictooilngsolutionsinc[.]com
- pulsesagego[.]top
- quickbooksboose[.]ru
- techlifegrooveeo[.]ru
- trenddigitalgadgetcx[.]ru

遭濫用服務的子網域

- 11299onedrive84899nhfhjke3hdhhdd[.]pages[.]dev
- accessdocumentfile[.]pages[.]dev
- aldkdlkdkdkdkdldlkdljdkskdjsdjsnmdkskddskdkekdksdk[.]pages[.]dev
- fsafacbcvbcxbdsfafafsf[.]pages[.]dev
- graves-construction-llc[.]pages[.]dev
- lively-crystal-reward[.]glitch[.]me
- pagemicrorofimicrsftonininecheckverf-portal-secure-logon[.]us-east-1[.]linodeobjects[.]com
- pub-80ebf6b7d8e54c738b0717427e3e131c[.]r2[.]dev
- pub-e0deb07b5eea4ed5b7ab525b4d87d2a8[.]r2[.]dev
- sharepointrickdirkse[.]pages[.]dev
- sj84848383voicena0mprdooooprodoutlookcommmailpppprotection[.]pages[.]dev

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：

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。

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。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

關於賽門鐵克 (Symantec)

Symantec
A Division of Broadcom

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
KEEPSAFE
INFORMATION SECURITY

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，以及基於比原廠更熟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**。