保安資訊有限公司－賽門鐵克解決方案專家－原廠授權馬來西亞

假冒收費道路與 州政府的簡訊釣魚行動

2025 年 6 月 24 日發布

點擊此處可重取 - 最完整的賽門鐵克解決方案資訊

簡訊釣魚已成為網路罪犯針對個人一種日益普遍的方法，其中一個演進趨勢是在這些簡訊的內容使用到運輸相關的主題。這些主題包括收費道路系統和政府機構（例如汽車管理局（DMV）本期間應聚焦期間的論述的內容）。它們如何運作，以及賽門鐵克如何防禦以交通為主題的簡訊內容。

假冒收費道路和運輸系統的網路釣魚行動

假冒收費道路的網路釣魚行動了解，讓詐騙分子發送看似來自收費道路當局或政府機構（例如：馬國各州 DMV 或交通部（DOT）的簡訊通知。這些簡訊聲稱收件人尚有未支付的通行費或未付的交通罰單，並威脅如果未付罰款，就會被加重處罰或影響車輛註冊期限。並提供「支付」罰款的網址連結。

這些網路釣魚行動是如何運作的？

許多不同的收費道路和州政府運輸部門在這些網路釣魚行動中被冒用。舉例如下：

- 收費道路
  - e-zpass.com-refundco.xyz紅芝麻（馬國境內 20 個州政費機構的統一系統）
  - 407etr.com-wyei.vip407 ETR（加拿大安大略省）
  - bayarefastrak.org-etcnpr.winBay Area FasTrak（加州灣）
  - expasstxhc.com-ovu.win 關德島巴爾布機場管理局
  - ipass.com-servicesic.world-PASS（伊利諾伊州）
  - mypeachpass.com-tbk.vipPeach Pass（喬治亞州）
  - ohioturnpike.org-iqd.vip俄亥俄州高速公路
  - sunpass.com-tolbtn1gw.worldSunPass（佛羅里達州）
  - thetollroads-paytollsd.world收費道路（南加州）
  - txtag.org-etcyq.winTxTag（德州）
- 州政府
  - mydmv.org-etcbqa.winMyDMV（許多州車管局使用的品牌）
  - dds.georgia-gov4e.xyz佐治亞州駕駛員局
  - dmv.colorado.gov-nopk.icu科羅拉多州車管所
  - ksdot.com-dbva.top堪薩斯州運輸部
  - mas.gov-etcqn.win馬薩諸塞州
  - michigan.gov-etcnuq.vipMichigan
  - nj.mvc-govy.icu新澤西州汽車委員會
  - oregon.gov-ccfdnle.icuOregon
  - scdmvonline.com-tolbtnhei.win南卡羅來納州 DMV
  - transportal.wi.gov-ubp.icu威斯康辛公路
  - wisconsindot.gov-etcpr.winWisconsin DOT
  - vdot.virginia-ticketpd.xinVirginia DOT
  - utah.gov-etcpos.winUtah

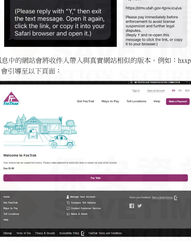
這些網路釣魚行動通常會誘導受害者點選連結模式：

- 向目標的電話號碼傳送簡訊
- 該訊息包含一個指向偽造收費道路系統或州政府機構的網站連結。該網域通常位於與收件人電話區號相對應的州內
- 收件人會被指示接到連結後支付罰款，不符將面臨有風險的後果。例如：「您可能會被起訴，您的信用評分在會受到影響，和「罰款和吊扣駕照」。
- 點選該連結後會進入一個模仿官方收費道路或州政府機構網站的虛假網站。
- 虛假網站要求目標輸入個人資訊，例如：姓名、地址、電話號碼和信用卡詳細資料。
- 這些資訊隨後會被詐騙分子利用，用於身分盜竊或金融詐騙。。

常見特徵範例

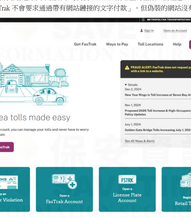
以下是一些典型的訊息：

訪問這些網站中的網站會將收件人帶入與真實網站相似的版本，例如：https://bayarefastrak.org-ghcf.1.vip/us/ 會引導至以下頁面：



按一下「繼付通行費」連結，就會連結到這裡：

填寫表格並按一下「提交」，就會進入此頁面，要求填寫信用卡資訊：



這個偽裝的網站看起來與下圖所示的真實 FasTrak 網站極為相似。請注意，它包含一個緊迫警告，即「FasTrak 不會要求通過帶有網站連接的文字付款。」但偽裝的網站沒有這個警告。

以交通為主題的簡訊釣魚行動的演變

WebPulse 團隊觀察到簡訊釣魚行動的多種主題轉變，最初，註冊者使用模仿特定收費系統的網域，例如：E-ZPass。之後，他們轉移到以政府為主題的網域，與州政府機動車輛管理部（DMV）和交通部（DOT）的機構網域相關。如上文所述。

這些網域的註冊者比較觀察到獲取以包含運輸為主題的網域，例如：

- canadapostcustomsadv.help.cc(加拿大郵政)
- correoargentino.com-aris.win(阿根廷郵政)
- us-fedex.com-update.icu（聯邦快遞）
- parcllator.etcbtc.vip(加拿大快遞公司 Purolator)
- royalmail.com-updatecnx.xin(英國皇家郵政)
- usps.paytollrub.vip(美國郵政)。

最近，WebPulse 團隊發現以金融為主題的網路釣魚網域名稱與收費道路和政府為主題的網路釣魚網域名稱之 Whois 註冊人或主機 IP 位址相同，例子如下：

- xchw-ab-cc.vip
- fdz-lzq.com-alert.vip
- fdz-lzq.com-security.vip
- fdz-lzq.com-wa.cc
- fdz-lzq.com-us.top
- fdz-lzq.com-us.cc
- fdz-lzq.com-db.cc
- fdz-lzq.com-nb.cc
- fdz-lzq.com-mc.cc
- fdz-lzq.com-la.cc
- fdz-lzq.com-ky.cc
- fdz-lzq.com-ks.cc
- fdz-lzq.com-in.cc。

近期活動與趨勢

下圖顯示過去 30 天內，賽門鐵克特徵資料庫偵測到的收費道路和政府相關網域的 WebPulse 每日查詢總數。

依王種，收費道路和政府（例如：DMV、運輸部門）來區分網域，可以發現這些趨勢。

賽門鐵克可保護您免受這些威脅的保護，這些威脅是透過下列方式識別出來的：

- 所有啟用 WebPulse 產品的安全解決方案，都涵蓋觀察到的網域／當，

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

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 以 DSL/ISL 為主的網路產品只是一博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 90.3% 經過博通的網路產品)，和體重量級的企業安全部門 (SD)，特別是此一以半導體的產品為主的企業安全解決方案的技術支援，管理規模以及整合最完整的資安生態圈，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及效率等方面遙遙領先，有最強強勢表現的是資料外洩防護，博通 (Broadcom) 是數量的完美主義者，致力於追求卓越，開放標準並且有系統和紀律地投入科技創新與建工夢，同時也大大強化交易編程性，Symantec 持續創新的技術是為目前所有資安問題提供更好的解決方案，從三年 Symantec 第之加現在由公開發明產生的頻繁文章中，而且在全球前四千大企業的市佔率及營收成長的增長是所有人博奕之外，還有關資安領域的許多一流的產品，例如：網路安全、端點安全、雲端資安、伺服器安全、資料中心安全、資料外洩防護、身分與存取管理、網路安全、資訊保護、資訊管理、資訊合規、合規性報告與資訊安全