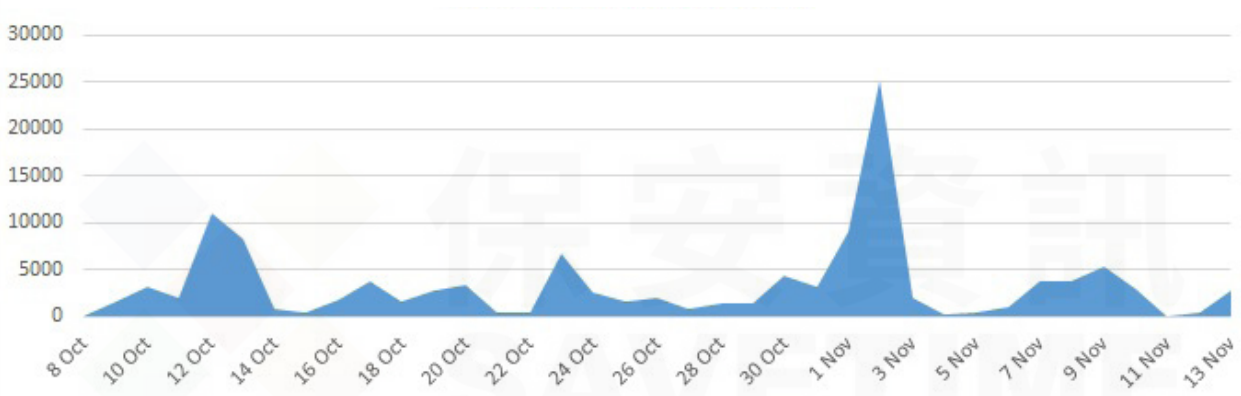
濫用Cloudflare物件儲存服務R2的網路釣魚威脅

2023 年 11 月 14 日發布

長期以來，發動網路釣魚的惡棍，無論是個人還是團體，都在持續嘗試各種可能的方法實施網路釣魚行動。星際檔案系統 (IPFS) 和 Cloudflare 物件儲存服務 R2 等內容存儲網路 (CDN) 是被濫用最多的網路釣魚網頁主機。我們最近發佈一份有關單個活動的防護公告，但在過去 30 天內，我們在全球觀察到更多的實例，主要是試圖竊取企業使用者的電子郵件憑據／帳密。

賽門鐵克所攔截到的上架在 Cloudflare R2 的網路釣魚郵件時序統計圖



我們可以認為，CloudFlare R2 日益被網路釣魚威脅者濫用的主要原因是其免費、易用性、良好聲譽和遍及全球的影響力。所有這些因素結合在一起，為他們提供一個強大的平臺來操弄社交工程伎倆，以達到一定程度的規避、韌性和匿名性來進行非法的勾當。

如前所述，所觀察到的大多數網路釣魚行動都以誘騙電子郵件憑證／帳密為目標，透過與帳戶相關問題 (密碼問題、終止、未讀郵件等)、帳單、警方警告和其他社交工程伎倆等相關的電子郵件來引誘使用者。這些電子郵件包含一個引導至網路釣魚頁面的惡意網頁鏈結，網頁鏈接的尾部是使用者的電子郵寄地址。因此，如果用戶被成功誘騙點擊 URL，假冒的登錄頁面就會在登錄欄位中顯示使用者的電子郵寄地址，使登錄過程看起來更加可信。

以下是一些惡意網頁鏈結的最新實例，這些惡意網頁鏈結會引導至上線在 CloudFlare R2 代管的釣魚網頁：

- hxxp[:]//pub-733372c603ef451496fbd54cfcb41576[.]r2[.]dev/93306DHI[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-be898b69352444c28d68f43e8725f2d1[.]r2[.]dev/godisalive[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-f4d1302dafbf4beeaf3e5e773e67edc4[.]r2[.]dev/allupdate[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-ad5b0662c2a54e5884a831384bd99913[.]r2[.]dev/pagefem345[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-ad60cadbed8e448499578f472c0a3183[.]r2[.]dev/af[.]html#[使用者的電子郵寄地址]
- hxxp[:]//pub-a8906372f15e4c3c9eeedea91a48a923[.]r2[.]dev/index[.]html#[使用者的電子郵寄地址]

賽門鐵克的多重防護技術已經於第一時間提供最有效的保護 (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

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**。