在Umbrella中啟用新看見的域安全類別

目錄

簡介

本檔案介紹Cisco Umbrella中的「新見域」(NSD)安全類別。

背景資訊

新見域(NSD)是一個安全類別，用於識別Cisco Umbrella DNS服務（包括家庭使用者的免費OpenDNS服務）的任何使用者在過去24小時內首次查詢的域。 此安全類別的功能與任何其他安全類別相同，並且可作為現有安全設定或新安全設定的一部分啟用。域在清單中保留24小時。

Cisco Umbrella如何將域定義為「新看到」

新域通常作為新惡意軟體活動的一部分而建立。這些攻擊背後的惡意攻擊者使用新的域，因為傳統的基於特徵碼的方法無法識別他們是否阻止已知的惡意網站。例如，網路釣魚活動可以建立一個新域來配合大型垃圾郵件活動，從而鼓勵使用者點選連結。該連結尚未被知為此活動的一部分，並且未被已知惡意域的標準清單阻止。在將連結新增到這些清單之前，犯罪分子有足夠的時間來竊取資料、安裝惡意軟體並獲得網路訪問許可權。

新發現的域(NSD)安全類別通過檢查DNS日誌來查詢以前從未見過的域來運行。由於無效查詢的數量，對於要標籤為新可見的域，客戶端查詢必須收到正確的答案。首次看到域後，會將其新增到清單中24小時。在此時間段之後，該域將不再可見，並且會從清單中刪除。

報告記錄域在查詢時所屬的類別。因此，如果某個域在查詢時被分類為新可見域，則此域將在活動搜尋或安全活動報告中進行報告。但是，一旦域從清單中到期後，根據有關該域的當前資料(特別是使用新的Destinations或Identities報告、Investigate Console或Investigate API)在該域上透視後，該域將不再顯示為最新顯示的域。簡而言之，幾天後重新訪問域無法再顯示為Umbrella中的新域。這是有意安排的，但可能會導致一些最初的混亂。

新發現的域的唯一定義是：這是新看到的。因此，被歸類為新發現的域中有很大一部分不是惡意域，並且合法域檢測預計會出現在此安全類別中。已針對此情況實施了預防措施，尤其是針對生成隨機子域為內容服務的某些服務和CDN（如Akamai和Cloudfront）。針對Facebook和Google等熱門

域名的傳統保證也被用於確保這些域不包括在內。

此外，只有完全限定域名（第二級域或第二級域的子域）被視為新發現的域。頂級域和國家代碼頂級域未包括在新建域中，以避免阻止域的大型分組。

關於實施的重要說明

鑑於可能會出現一些不需要檢測，Cisco Umbrella強烈建議開始在稽核模式或僅檢測模式下使用此報告，而不阻止或採取任何操作。預設情況下，其安全設定中帶有此類別的任何使用者都將在報告中將「新發現的域」視為檢測項。這實際上意味著該功能在預設情況下啟用時不會有任何阻塞。在大多數情況下，使用者必須使用報告來檢視哪些流量符合該類別，然後使用該資訊更深入地研究這些域，確定它們是否可能構成安全威脅而不是自動阻止。

另一個主要警告是允許對域執行第一個查詢。這是因為Cisco Umbrella以前從未看到對該域的查詢，因此日誌記錄系統沒有處理過該查詢，因此該查詢未被包含在Newly Seen Domains類別中。首次查詢域和出現在匹配類別的域清單之前的時間間隔大約為五分鐘，但可能超過此時間，因為Cisco Umbrella不一定處理100%的DNS查詢日誌（由於處理時間和流量）。

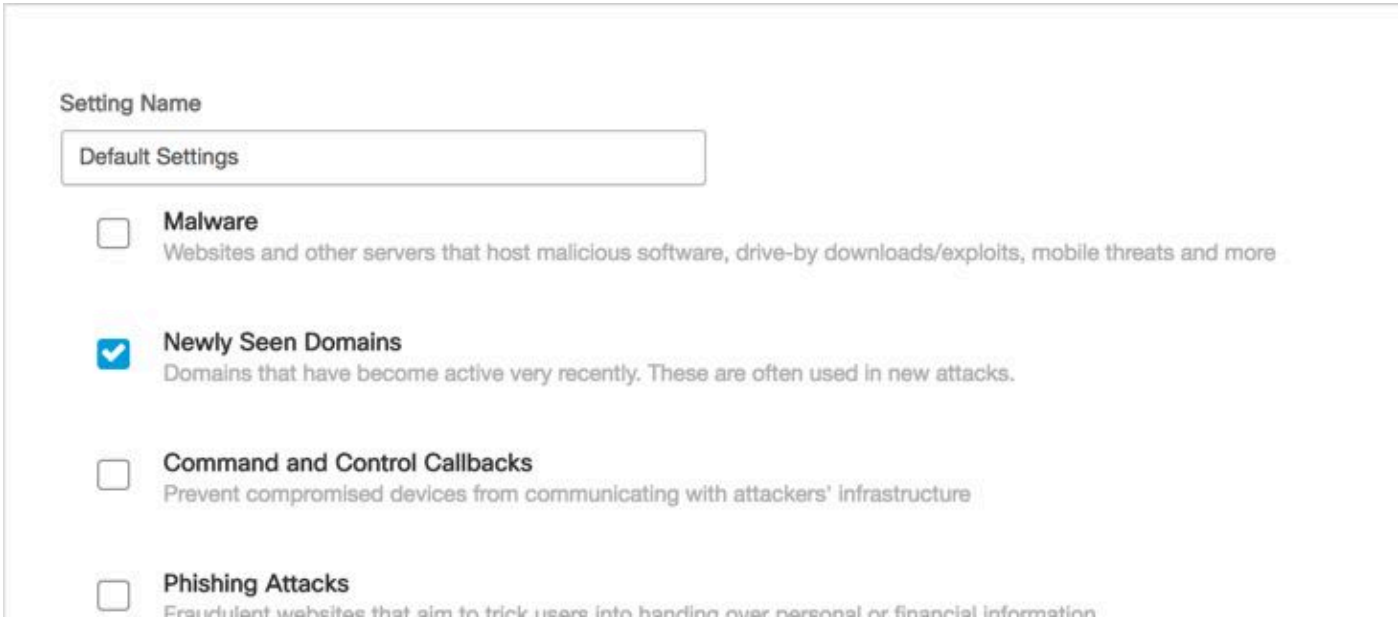
代理新發現的域

使用Umbrella智慧代理的客戶還發現NSD類別中的某些域是代理的。這是有計畫的。Umbrella Labs團隊使用通過代理這些新域收集的資料來確定是否可以立即將其新增到惡意軟體類別。此問題的一個副作用是，傳送到新發現的域（也正被代理）的非標準流量在代理級別被丟棄。智慧代理僅代理埠80和443，這些埠傳統上用於網路流量。無論類別是否遭封鎖，代理啟用後都會自動發生這種情況。要防止代理單個新顯示的域，請將其新增到相應的允許清單。

有關智慧代理的更多資訊，請參閱我們的啟用智慧代理檔案。

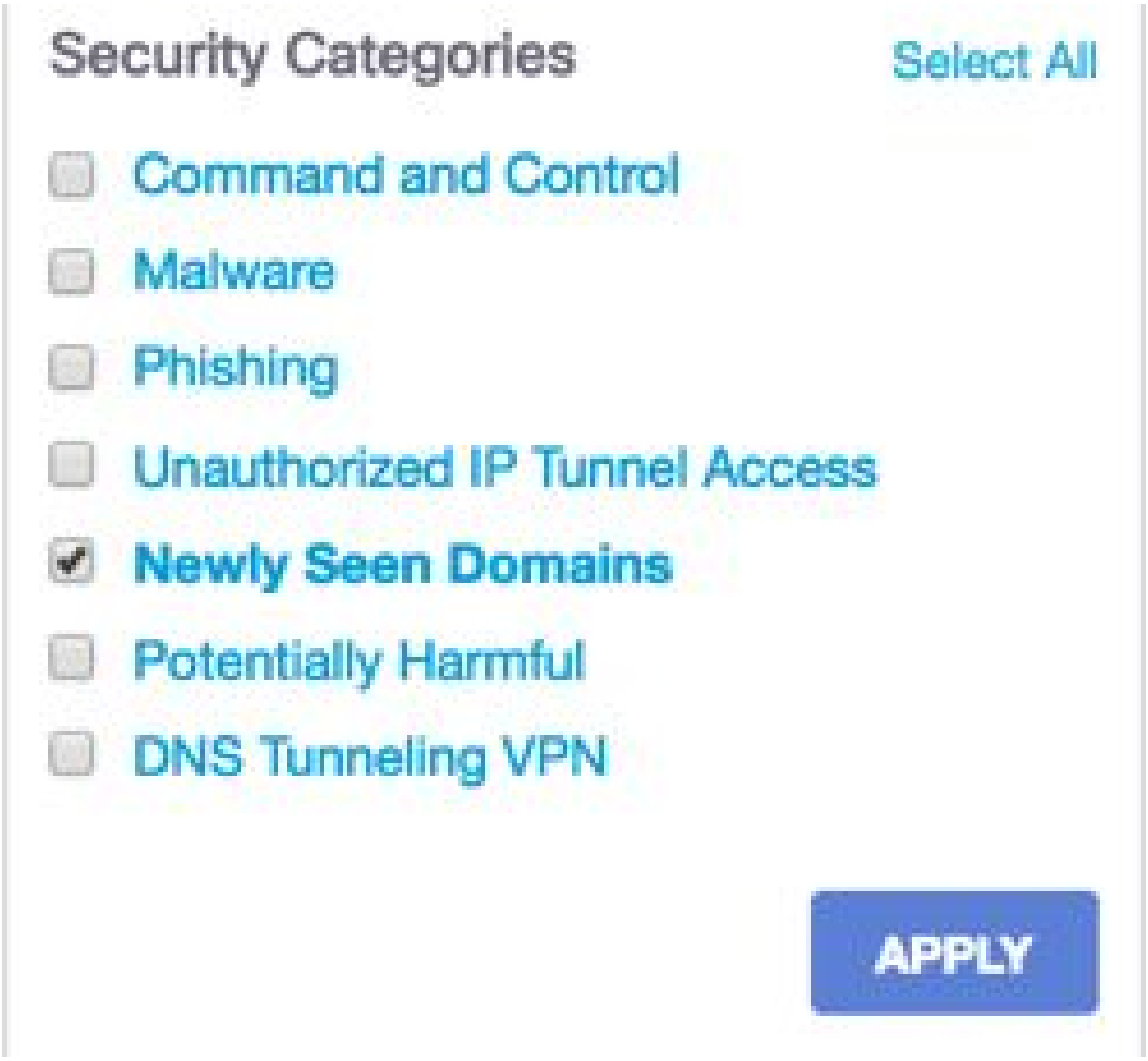
啟用新看見的域

可以像Policies > Security Settings下的任何其他類別一樣啟用Newly Seen Domain安全類別，然後編輯現有安全設定。或者，也可以在Policy Configuration Wizard本身內完成。



115014822286

在某些報告(如活動搜尋)中，也可以過濾新發現的域。



115015007423

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。