Activer la catégorie de sécurité Domaines récemment vus dans Umbrella

Table des matières

Introduction

Ce document décrit la catégorie de sécurité « Nouveaux domaines visibles » (NSD) dans Cisco Umbrella.

Informations générales

Newly Seen Domains (NSD) est une catégorie de sécurité qui identifie les domaines interrogés pour la première fois au cours des dernières 24 heures par tout utilisateur du service Cisco Umbrella DNS (y compris le service OpenDNS gratuit pour les utilisateurs à domicile). Cette catégorie de sécurité fonctionne de manière identique à toute autre catégorie de sécurité et peut être activée dans le cadre d'un paramètre de sécurité existant ou d'un nouveau paramètre. Les domaines restent dans la liste pendant une période de 24 heures.

Comment Cisco Umbrella définit un domaine comme « nouveau »

De nouveaux domaines sont souvent créés dans le cadre de nouvelles campagnes contre les programmes malveillants. Les acteurs malveillants derrière ces campagnes utilisent de nouveaux domaines car les méthodes traditionnelles basées sur les signatures ne les reconnaissent pas pour bloquer les sites Web malveillants connus. Par exemple, une campagne d'hameçonnage peut créer un nouveau domaine pour accompagner une campagne de spam majeure incitant les utilisateurs à cliquer sur un lien. Le lien ne fait pas encore partie de cette campagne et n'est pas bloqué par les listes standard de domaines malveillants connus. Avant que le lien ne soit ajouté à ces listes, les criminels disposent de suffisamment de temps pour exfiltrer les données, installer des programmes malveillants et accéder au réseau.

La catégorie de sécurité Nouveaux domaines (NSD) fonctionne en recherchant dans les journaux

DNS des recherches de domaines qui n'ont jamais été vus auparavant. En raison du volume de requêtes non valides, pour qu'un domaine soit marqué comme nouvellement vu, la requête du client doit recevoir une réponse appropriée. Une fois qu'un domaine est vu pour la première fois, il est ajouté à une liste pendant 24 heures. Après cette période, le domaine n'est plus visible et est supprimé de la liste.

Un rapport enregistre la catégorie dans laquelle se trouvait un domaine au moment de l'interrogation. Par conséquent, si un domaine a été classé comme nouvellement vu lors de l'interrogation, il est signalé comme tel dans le rapport Activity Search ou Security Activity. Cependant, une fois que le domaine expire de la liste, le pivotement sur ce domaine par rapport aux données actuelles le concernant (en particulier à l'aide des nouveaux rapports Destinations ou Identities, la console Investigate ou l'API Investigate) n'affiche plus ce domaine comme nouvellement vu. En bref, le fait de revisiter un domaine plusieurs jours plus tard ne peut plus le montrer comme nouveau vu dans Umbrella. C'est intentionnel, mais cela peut conduire à une certaine confusion initiale.

La seule définition d'un domaine nouvellement vu est exactement celle-ci : c'est nouveau. Par conséquent, une grande partie des domaines classés comme nouvellement vus ne sont pas malveillants et des détections de domaines légitimes sont attendues avec cette catégorie de sécurité. Des précautions ont été mises en oeuvre contre cet événement, en particulier pour certains services et CDN comme Akamai et Cloudfront qui génèrent des sous-domaines aléatoires pour servir le contenu. Les garanties traditionnelles contre les domaines très populaires, comme Facebook et Google, ont également été utilisées pour s'assurer que ceux-ci ne sont pas inclus.

En outre, seuls les noms de domaine complets (domaine de second niveau ou sous-domaine d'un domaine de second niveau) sont considérés comme des domaines nouvellement visibles. Les domaines de premier niveau et les domaines de premier niveau de code de pays ne sont pas inclus dans les domaines nouvellement vus pour éviter de bloquer de grands regroupements de domaines.

Remarques importantes sur la mise en oeuvre

Étant donné que certaines détections indésirables peuvent être attendues, Cisco Umbrella recommande fortement de commencer à utiliser ce rapport en mode audit ou en mode détection seule sans blocage ni action. Par défaut, tout utilisateur disposant de cette catégorie dans ses paramètres de sécurité voit les domaines nouvellement vus comme des détections dans les rapports. Cela signifie que la fonctionnalité est activée par défaut sans blocage. Dans la plupart des cas, les utilisateurs doivent utiliser des rapports pour voir quel trafic correspond à la catégorie et utiliser ces informations pour effectuer des recherches plus approfondies sur ces domaines afin de déterminer s'ils peuvent représenter une menace pour la sécurité plutôt que de les bloquer automatiquement.

Une autre mise en garde importante est que la première requête au domaine est autorisée. En effet, Cisco Umbrella n'a jamais vu de requête pour ce domaine auparavant et, en tant que tel, il n'a pas été traité par les systèmes de journalisation pour être inclus dans la catégorie Domaines

nouvellement vus. L'intervalle de temps entre le moment où un domaine est interrogé pour la première fois et le moment où il apparaît dans la liste des domaines correspondant à la catégorie est d'environ cinq minutes, mais il peut s'étendre au-delà, car Cisco Umbrella ne traite pas nécessairement 100 % des journaux de requêtes DNS (en raison du temps et du volume de traitement).

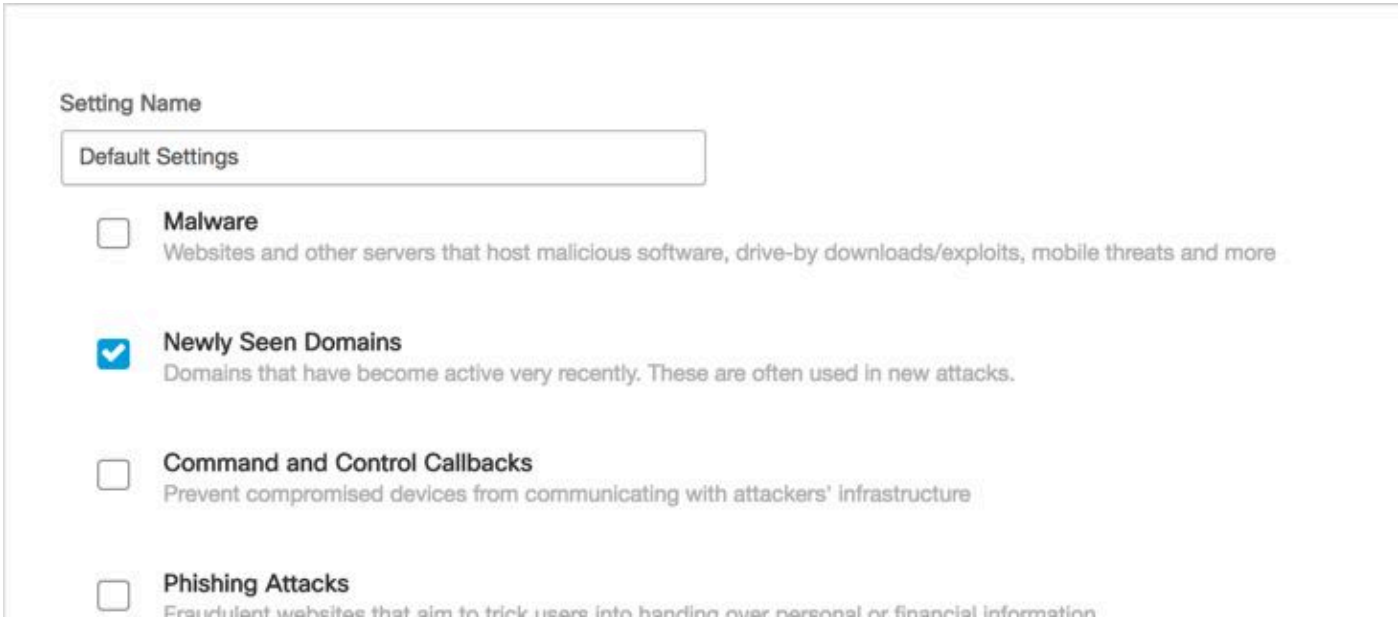
Proxy des domaines récemment vus

Les clients qui utilisent le proxy intelligent Umbrella observent également que certains domaines de la catégorie NSD sont mis en proxy. C'est intentionnel. L'équipe d'Umbrella Labs utilise les données collectées via le proxy de ces nouveaux domaines pour déterminer s'ils peuvent être ajoutés immédiatement aux catégories de programmes malveillants. Un effet secondaire de cette situation est que le trafic non standard envoyé à un domaine nouvellement vu qui est également mis en proxy est abandonné au niveau du proxy. Le proxy intelligent n'utilise que les ports proxy 80 et 443, les ports traditionnellement utilisés pour le trafic Web. Cela se produit automatiquement lorsque le proxy est activé, que la catégorie soit bloquée ou non. Pour empêcher qu'un seul domaine nouvellement détecté soit mis en proxy, ajoutez-le à la liste d'autorisation appropriée.

Pour plus d'informations sur le proxy intelligent, consultez notre documentation Enable the Intelligent Proxy.

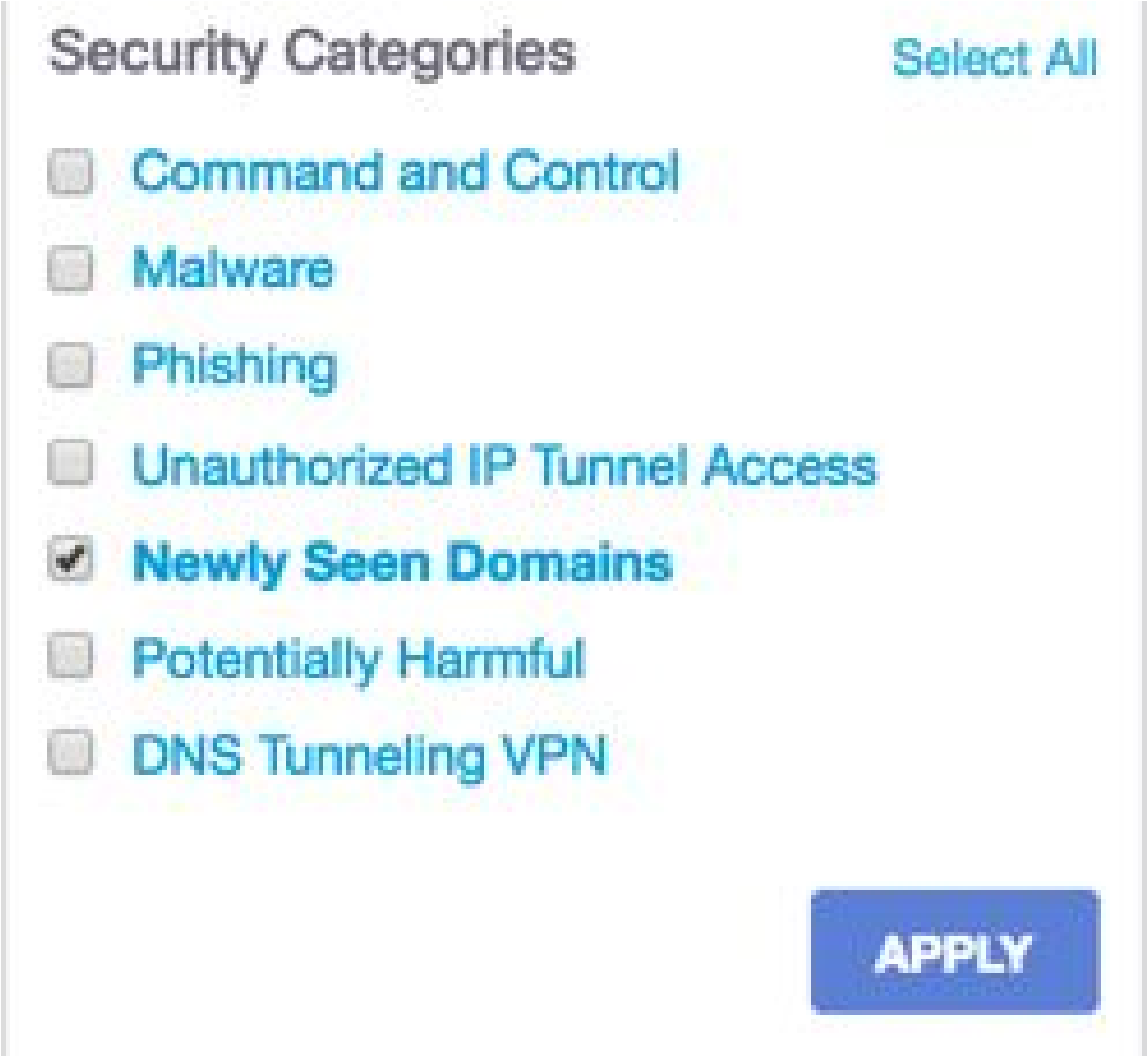
Activer les domaines récemment vus

La catégorie de sécurité Domaine récemment vu peut être activée comme n'importe quelle autre catégorie sous Stratégies > Paramètres de sécurité, puis en modifiant un paramètre de sécurité existant. Vous pouvez également le faire dans l'Assistant Configuration de stratégie lui-même.



115014822286

Les domaines récemment vus peuvent également être filtrés pour certains rapports, tels que la recherche d'activité.



115015007423

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.