Habilitar la categoría de seguridad de dominios recién vistos en Umbrella

Contenido

Introducción

Este documento describe la categoría de seguridad "Dominios recién vistos" (NSD) en Cisco Umbrella.

Antecedentes

Dominios recién vistos (NSD) es una categoría de seguridad que identifica los dominios consultados por primera vez en las últimas 24 horas por cualquier usuario del servicio Cisco Umbrella DNS (incluido el servicio OpenDNS gratuito para usuarios domésticos). Esta categoría de seguridad funciona de forma idéntica a cualquier otra y se puede habilitar como parte de una configuración de seguridad existente o una nueva. Los dominios permanecen en la lista durante un período de 24 horas.

Cómo define Cisco Umbrella un dominio como "recién visto"

A menudo, se crean nuevos dominios como parte de nuevas campañas de malware. Los sujetos malintencionados detrás de estas campañas utilizan nuevos dominios porque los métodos tradicionales basados en firmas no los reconocen por bloquear sitios web malintencionados conocidos. Por ejemplo, una campaña de suplantación de identidad puede crear un nuevo dominio para acompañar a una campaña de spam importante que anime a los usuarios a hacer clic en un enlace. Aún no se sabe que el enlace forme parte de esta campaña y no está bloqueado por listas estándar de dominios malintencionados conocidos. Antes de agregar el enlace a dichas listas, los delincuentes disponen de tiempo suficiente para extraer datos, instalar malware y obtener acceso a la red.

La categoría de seguridad Dominios recién vistos (NSD) funciona comprobando los registros DNS para buscar dominios que no se hayan visto anteriormente. Debido al volumen de consultas no válidas, para que un dominio se marque como recién visto, la consulta del cliente debe recibir una

respuesta adecuada. Una vez que se ve un dominio por primera vez, se agrega a una lista durante 24 horas. Después de este período, el dominio ya no se ve recientemente y se elimina de la lista.

Un informe registra la categoría en la que se encontraba un dominio en el momento en que se realizó la consulta. Por lo tanto, si un dominio se categorizó como recién visto cuando se le consultó, se informa como tal en el informe Búsqueda de actividad o Actividad de seguridad. Sin embargo, una vez que el dominio expira de la lista, pivotando en ese dominio contra los datos actuales sobre él (especialmente usando los nuevos informes Destinos o Identidades, la Consola de Investigación o la API de Investigación) ya no muestra ese dominio como recién visto. En resumen, volver a visitar un dominio varios días después ya no puede mostrarlo como recién visto en Umbrella. Esto es por diseño, pero puede llevar a cierta confusión inicial.

La única definición de un dominio recién visto es exactamente eso: es de reciente aparición. Como resultado, una parte significativa de los dominios categorizados como recientemente vistos no son maliciosos, y se espera que se produzcan detecciones de dominios legítimos con esta categoría de seguridad. Se han implementado precauciones contra esta ocurrencia, especialmente para ciertos servicios y CDNs como Akamai y Cloudfront que generan subdominios aleatorios para servir contenido. Las garantías tradicionales contra dominios muy populares, como Facebook y Google, también se han utilizado para garantizar que no se incluyen.

Además, sólo los nombres de dominio completos (dominio de segundo nivel o un subdominio de un dominio de segundo nivel) se consideran dominios que se ven recientemente. Los dominios de nivel superior y los dominios de nivel superior de código de país no se incluyen en los dominios recién vistos para evitar el bloqueo de grandes agrupaciones de dominios.

Notas importantes sobre la implementación

Dado que cabe esperar algunas detecciones no deseadas, Cisco Umbrella recomienda encarecidamente empezar a utilizar este informe en modo auditoría o en modo solo detección sin bloquear ni realizar ninguna acción. De forma predeterminada, cualquier usuario con esta categoría disponible en su configuración de seguridad ve los dominios recién vistos como detecciones en los informes. Esto significa que la función está habilitada sin ningún bloqueo de forma predeterminada. En la mayoría de los casos, los usuarios deben utilizar informes para ver qué tráfico coincide con la categoría y utilizar esa información para investigar estos dominios con más profundidad para determinar si podrían representar una amenaza para la seguridad en lugar de bloquearlos automáticamente.

Otra advertencia importante es que se permite la primera consulta al dominio. Esto se debe a que Cisco Umbrella nunca ha visto una consulta a ese dominio anteriormente y, como tal, no ha sido procesada por los sistemas de registro para incluirla como parte de la categoría Dominios recién vistos. El intervalo de tiempo entre el momento en que se consulta un dominio por primera vez y el momento en que aparece en la lista de dominios que coinciden con la categoría es de aproximadamente cinco minutos, pero puede extenderse más allá, ya que Cisco Umbrella no procesa necesariamente el 100% de los registros de consultas DNS (debido al tiempo y volumen

de procesamiento).

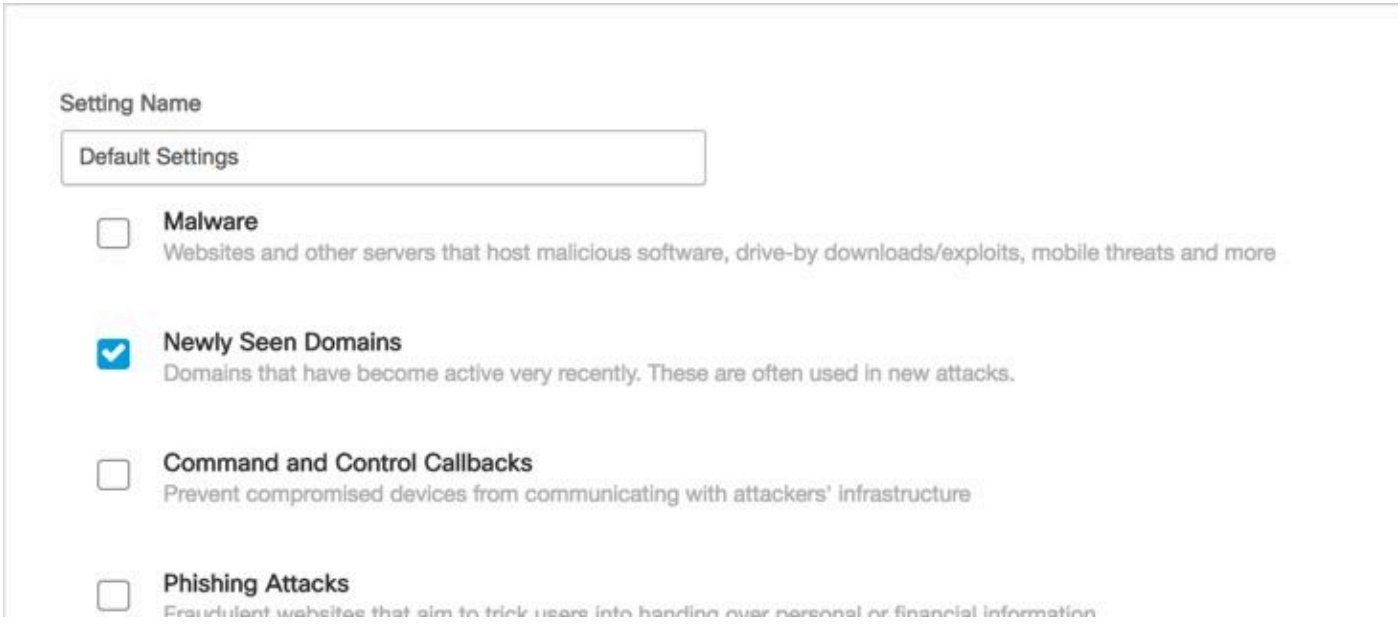
Proxying Dominios Recién Vistos

Los clientes que utilizan el proxy inteligente de Umbrella también observan que algunos dominios de la categoría NSD están proxy. Esto es por diseño. El equipo de Umbrella Labs utiliza los datos recopilados mediante el proxy de estos nuevos dominios para determinar si se pueden agregar a las categorías de malware inmediatamente. Un efecto secundario de esto es que el tráfico no estándar enviado a un dominio visto recientemente que también se está procesando como proxy se descarta en el nivel de proxy. El proxy inteligente sólo utiliza los puertos 80 y 443, los puertos que se utilizan tradicionalmente para el tráfico web. Esto sucede automáticamente cuando el proxy está habilitado, independientemente de si la categoría está bloqueada o no. Para evitar que un único dominio recién visto se convierta en proxy, agréguelo a la lista de permitidos correspondiente.

Puede encontrar más información sobre Intelligent Proxy en nuestra documentación Enable the Intelligent Proxy.

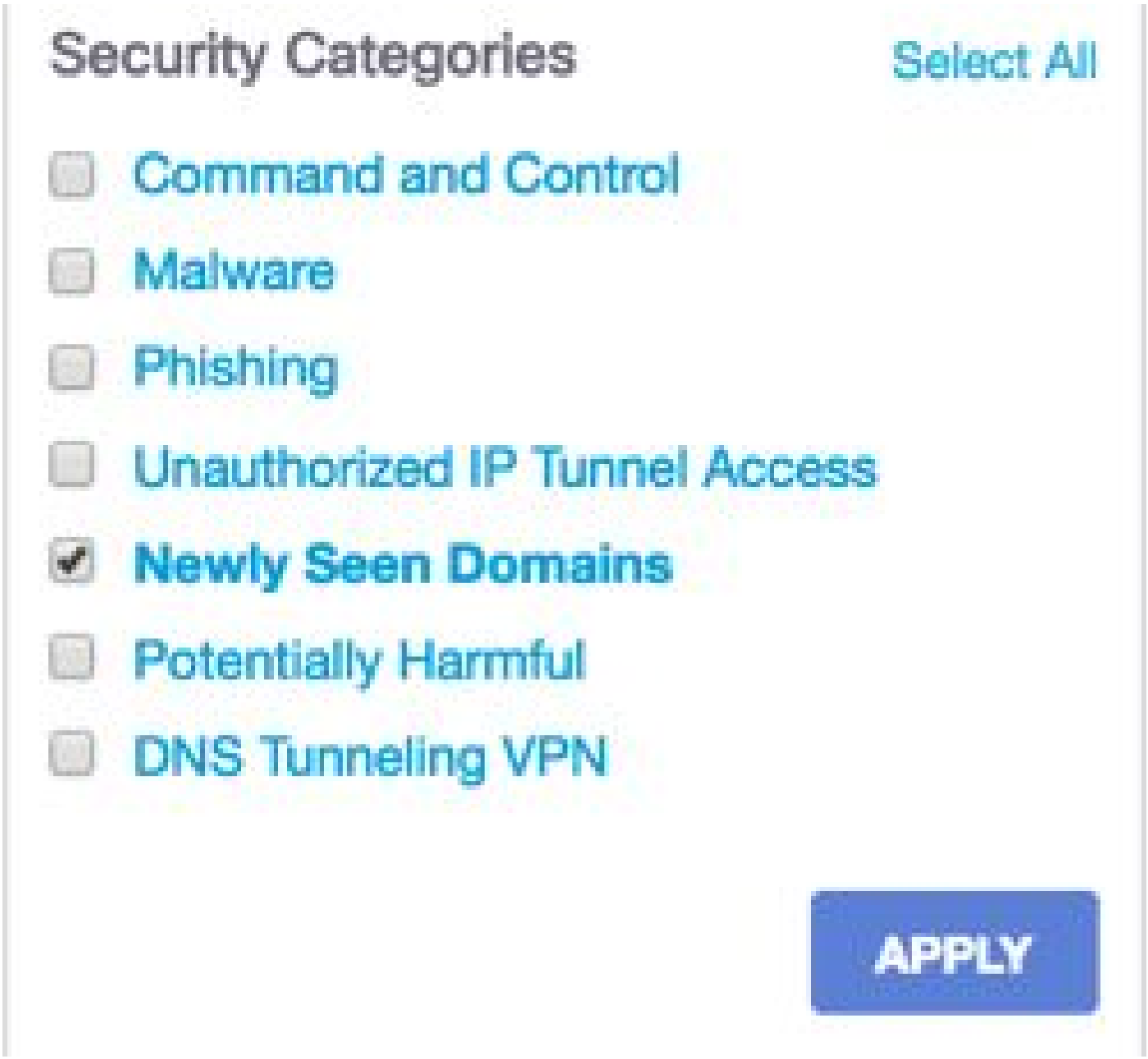
Habilitar dominios recién vistos

La categoría de seguridad Dominio Recién Visto se puede habilitar como cualquier otra en Políticas > Configuración de Seguridad, y luego editar una configuración de seguridad existente. Alternativamente, se puede hacer dentro del Asistente de Configuración de Políticas mismo.



115014822286

Los dominios recién vistos también se pueden filtrar en determinados informes, como Búsqueda de actividad.



115015007423

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).