Nieuw bekeken domeinen inschakelen Beveiligingscategorie in paraplu

Inhoud

Inleiding

In dit document wordt de beveiligingscategorie "Nieuw gezien domeinen" (NSD) in Cisco Umbrella beschreven.

Achtergrondinformatie

Newly Seen Domains (NSD) is een beveiligingscategorie die domeinen identificeert die voor het eerst in de afgelopen 24 uur zijn opgezocht door een gebruiker van de Cisco Umbrella DNS-service (inclusief de gratis OpenDNS-service voor thuisgebruikers). Deze beveiligingscategorie functioneert identiek aan elke andere beveiligingscategorie en kan worden ingeschakeld als onderdeel van een bestaande of een nieuwe beveiligingsinstelling. Domeinen blijven in de lijst voor een periode van 24 uur.

Hoe Cisco Umbrella een domein definieert als "nieuw gezien"

Nieuwe domeinen worden vaak gemaakt als onderdeel van nieuwe malwarecampagnes. Kwaadwillende actoren achter deze campagnes gebruiken nieuwe domeinen omdat traditionele op handtekeningen gebaseerde methoden ze niet herkennen voor het blokkeren van bekende kwaadaardige websites. Een phishingcampagne kan bijvoorbeeld een nieuw domein maken om een grote spamcampagne te begeleiden en gebruikers aan te moedigen op een link te klikken. De link maakt nog geen deel uit van deze campagne en wordt niet geblokkeerd door standaardlijsten met bekende kwaadaardige domeinen. Voordat de link aan die lijsten wordt toegevoegd, hebben criminelen voldoende tijd om gegevens te exfiltreren, malware te installeren en netwerktoegang te krijgen.

De beveiligingscategorie Newly Seen Domains (NSD) werkt door DNS-logs te controleren op zoekopdrachten van domeinen die nog nooit eerder zijn gezien. Vanwege het aantal ongeldige query's moet de clientquery een juist antwoord krijgen om een domein als nieuw gezien te

markeren. Zodra een domein voor het eerst wordt gezien, wordt het gedurende 24 uur aan een lijst toegevoegd. Na deze periode is het domein niet meer nieuw gezien en wordt het verwijderd uit de lijst.

Een rapport registreert de categorie waarin een domein zich bevond op het moment dat het werd opgevraagd. Als een domein is gecategoriseerd als nieuw gezien tijdens het opvragen, rapporteert het als zodanig in het rapport Activiteit zoeken of Beveiligingsactiviteit. Zodra het domein echter uit de lijst is vervallen, wordt dat domein afgezet tegen de huidige gegevens over dat domein (met name met behulp van de nieuwe rapporten Bestemmingen of Identiteiten, de Onderzoeksconsole of Onderzoeken API). Kortom, een domein enkele dagen later opnieuw bezoeken kan het niet meer laten zien als nieuw gezien in Umbrella. Dit is door het ontwerp, maar kan leiden tot enige initiële verwarring.

De enige definitie van een nieuw gezien domein is precies dat: het is nieuw gezien. Als gevolg hiervan is een aanzienlijk deel van de domeinen die zijn gecategoriseerd als nieuw gezien niet kwaadaardig en wordt verwacht dat detecties van legitieme domeinen zullen plaatsvinden met deze beveiligingscategorie. Voorzorgsmaatregelen tegen deze gebeurtenis zijn geïmplementeerd, vooral voor bepaalde diensten en CDN's zoals Akamai en Cloudfront die gerandomiseerde subdomeinen genereren om inhoud te dienen. Traditionele garanties tegen zeer populaire domeinen, zoals Facebook en Google, zijn ook gebruikt om ervoor te zorgen dat deze niet worden opgenomen.

Bovendien worden alleen volledig gekwalificeerde domeinnamen (domein op het tweede niveau of een subdomein van een domein op het tweede niveau) beschouwd als domeinen die nieuw worden gezien. Topleveldomeinen en topleveldomeinen voor landcodes zijn niet opgenomen in Nieuw bekeken domeinen om te voorkomen dat grote groepen domeinen worden geblokkeerd.

Belangrijke opmerkingen over de implementatie

Aangezien sommige ongewenste detecties kunnen worden verwacht, raadt Cisco Umbrella ten zeerste aan om dit rapport in de auditmodus te gebruiken of alleen de modus te detecteren zonder te blokkeren of actie te ondernemen. Standaard ziet elke gebruiker met deze categorie die beschikbaar is in zijn beveiligingsinstellingen Nieuw bekeken domeinen als detecties in de rapporten. Dit betekent in feite dat de functie standaard is ingeschakeld zonder blokkering. In de meeste gevallen moeten gebruikers rapporten gebruiken om te zien welk verkeer overeenkomt met de categorie en die informatie gebruiken om deze domeinen diepgaander te onderzoeken om te bepalen of ze mogelijk een beveiligingsbedreiging kunnen vormen in plaats van automatisch te blokkeren.

Een ander belangrijk voorbehoud is dat de eerste zoekopdracht naar het domein is toegestaan. Dit komt omdat Cisco Umbrella nog nooit eerder een zoekopdracht naar dat domein heeft gezien en als zodanig niet is verwerkt door de logboeksystemen om te worden opgenomen in de categorie Nieuw gezien domeinen. Het tijdsverschil tussen het moment waarop een domein voor het eerst wordt opgevraagd en voordat het wordt weergegeven in de lijst met domeinen die overeenkomen met de categorie is ongeveer vijf minuten, maar kan verder gaan omdat Cisco

Umbrella niet noodzakelijkerwijs 100% van de DNS-querylogs verwerkt (vanwege de verwerkingstijd en het volume).

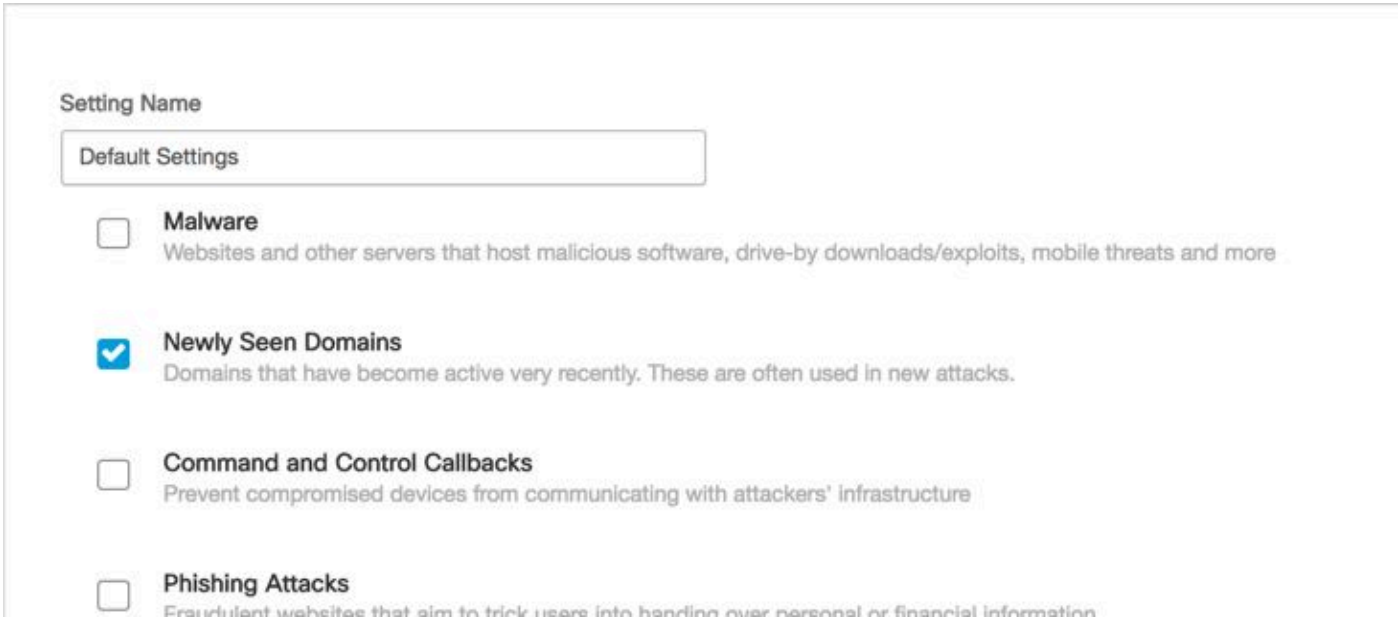
Nieuw gezien domeinen proxyeren

Klanten die de Umbrella Intelligent Proxy gebruiken, merken ook op dat sommige domeinen in de NSD-categorie worden benaderd. Dit is met opzet. Het Umbrella Labs-team gebruikt de gegevens die zijn verzameld door deze nieuwe domeinen te proxyen om te bepalen of ze onmiddellijk aan de malwarecategorieën kunnen worden toegevoegd. Een neveneffect hiervan is dat niet-standaard verkeer dat wordt verzonden naar een nieuw gezien domein dat ook wordt geproxied, op proxyniveau wordt verwijderd. De Intelligent Proxy alleen proxy poorten 80 en 443, de poorten traditioneel gebruikt voor webverkeer. Dit gebeurt automatisch wanneer de proxy is ingeschakeld, ongeacht of de categorie is geblokkeerd. Om te voorkomen dat een nieuw domein wordt geproxydeerd, voegt u het toe aan de juiste machtigingslijst.

Meer informatie over de Intelligente proxy kunt u vinden in onze documentatie De Intelligente proxy inschakelen.

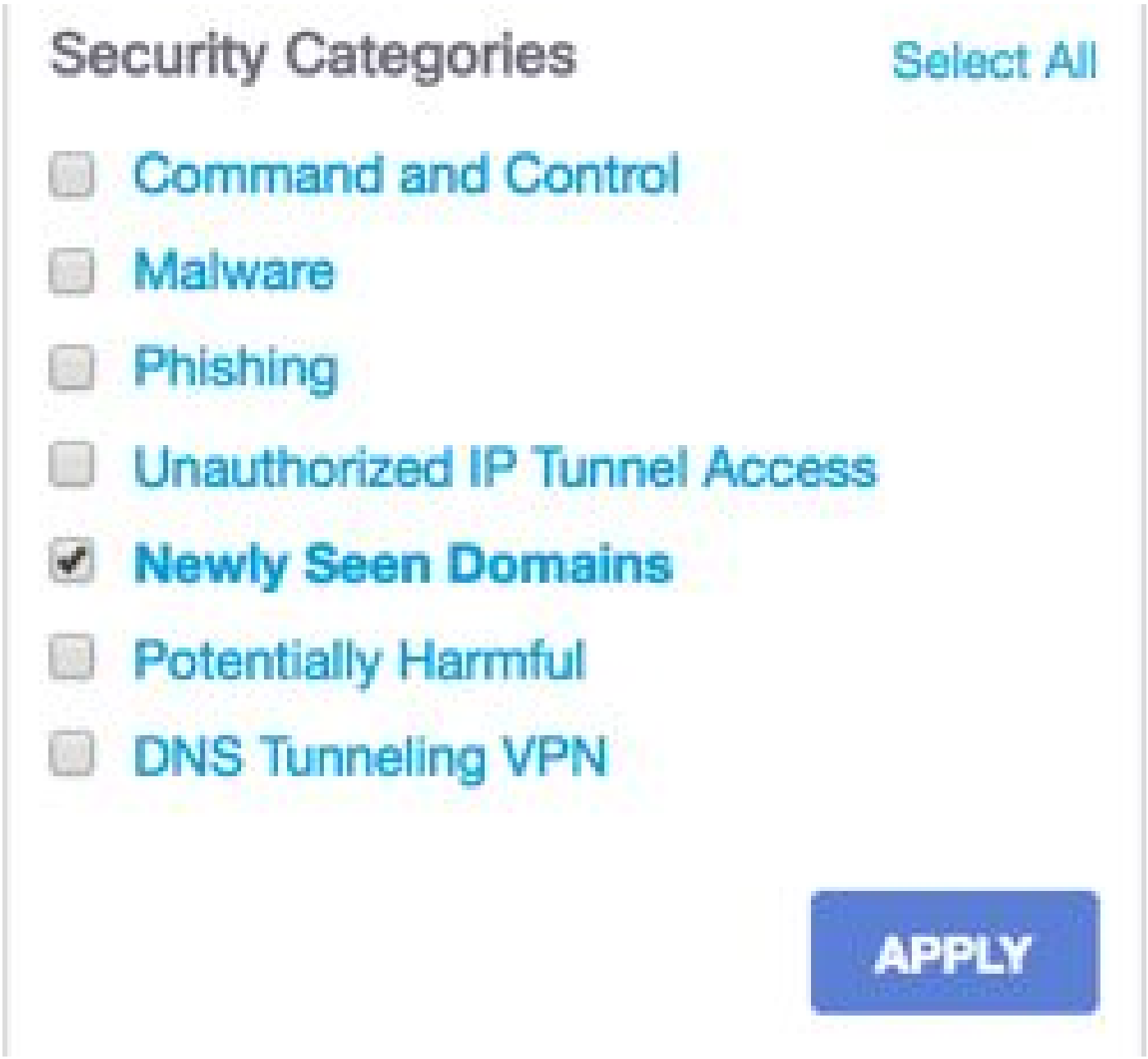
Nieuw bekeken domeinen inschakelen

De beveiligingscategorie Nieuw gezien domein kan worden ingeschakeld, net als alle andere categorieën onder Beleid > Beveiligingsinstellingen, waarna een bestaande beveiligingsinstelling wordt bewerkt. U kunt dit ook doen met de wizard Beleidsconfiguratie zelf.



115014822286

Nieuw bekeken domeinen kunnen ook worden gefilterd voor in bepaalde rapporten, zoals Activiteit zoeken.



115015007423

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.