Aankomende Umbrella-beveiligingsverbeteringen - nieuw bekeken domeinen

Inhoud

Inleiding

In dit document worden aankomende beveiligingsverbeteringen beschreven voor de categorie Newly Seen Domains (NSD) van de Secure Access- en Umbrella-services.

Overzicht

We zijn verheugd u te informeren over een belangrijke verbetering van de categorie Newly Seen Domains (NSD), een belangrijk aspect van onze Secure Access- en Umbrella-services, onder leiding van het Talos Threat Research-team.

Wat zijn we aan het doen?

In onze voortdurende inspanningen om uw beveiliging te versterken, implementeren we een bijgewerkt systeem voor NSD, overgaand naar versie 2 (NSDv2). Deze nieuwe iteratie breidt de brongegevens aanzienlijk uit, omdat het nu de volledige set van onze Passive DNS bevat die ons Investigate-product (800B-query's / dag) aanstuurt, een verbetering ten opzichte van de statistische steekproefmethodologie van de huidige Newly Seen Domains.

Met NSDv2 hebben we de dataset verfijnd om de feedback en het gebruik van klanten beter weer te geven, evenals de gegevensanalyse van het optreden tot veroordeling door ons Talos Threat Research Team. Het nieuwe algoritme richt zich op het ontdekken van nieuwe domeinen op geregistreerd niveau en vermindert de "ruis" van meerdere subdomeinen die een gemeenschappelijke ouder delen.

Waarom doen we dit?

We hebben geluisterd naar feedback van klanten en gegevens geanalyseerd die laten zien hoe NSD de categorisatie van domeinen met een laag volume kan vertragen, waardoor onverwachte

resultaten en verstoring van domeinen worden veroorzaakt als ze een plotselinge toename in populariteit ervaren. Bovendien kunnen wijzigingen in domeinen met een hoog volume onverwachte verschuivingen zien, bijvoorbeeld wanneer een netwerk voor de levering van inhoud wijzigingen in hun naamgevingsschema introduceerde.

Het Talos Threat Research-team heeft NSDv2 in samenwerking met Umbrella ontwikkeld om deze problemen op te lossen en een betrouwbaarder en nauwkeuriger systeem te bieden voor het identificeren van nieuw geziene domeinen.

Hoe komt het u ten goede?

De NSDv2-uitbreiding is ontworpen met het oog op uw beveiliging en operationele efficiëntie:

- Verbeterde detectie van bedreigingen: NSDv2 biedt een verbetering van minimaal 45% in het aantal identificerende domeinen die later kwaadaardig blijken te zijn.
- Verminderde false positives: met een nauwkeuriger targetingsysteem ervaart u minder verstoringen van onjuist gemarkeerde domeinen die regelmatig worden gebruikt.
- Geoptimaliseerde prestaties: de gestroomlijnde dataset maakt niet alleen snellere publicatie mogelijk, maar stelt ons supportteam ook in staat om snel eventuele problemen aan te pakken.
- Handhaving "Best practice": deze categorie is consistenter en relevanter en maakt een betere afstemming op de verwachtingen van de industrie en de klant mogelijk.
- Verrijkte rapportagegegevens: De verbeterde context en dekking met NSDv2 verrijkt de gegevens in rapporten.
- Verbeterde voorspelling: deze update helpt de Intelligente proxy bij het bepalen van risicovolle domeinen die een diepere inspectie rechtvaardigen.
- Geen interactie met de klant vereist: dit is een update van onze pijpleidingen voor een dynamische categorisatie en vereist geen migratie of beleidswijzigingen voor onze klanten. Dit is een volledig transparante verbetering voor beheerders en eindgebruikers.

De wijzigingen in deze categorie worden op 13 augustus 2024 doorgevoerd. We zijn dankbaar voor uw voortdurende vertrouwen in onze diensten en staan te popelen om u te voorzien van deze aanzienlijke verbeteringen in de beveiliging.

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.