Futuras melhorias de segurança de guarda-chuva - Domínios vistos recentemente

Contents

Introdução

Este documento descreve os futuros aprimoramentos de segurança para a categoria de Domínios recém-vistos (NSD) dos serviços de Acesso seguro e guarda-chuva.

Overview

Estamos muito animados em informar você sobre uma melhoria importante na categoria de Domínios recentemente vistos (NSD), um aspecto importante dos nossos serviços de acesso seguro e guarda-chuva, liderados pela equipe de pesquisa de ameaças da Talos.

O que estamos fazendo?

Em nossos esforços contínuos para reforçar sua segurança, estamos implementando um sistema atualizado para NSD, fazendo a transição para a versão 2 (NSDv2). Essa nova iteração expande significativamente os dados de origem, pois agora inclui o conjunto completo de nosso DNS passivo que alimenta nosso produto Investigate (800B consultas/dia), uma melhoria sobre a metodologia de amostragem estatística dos Domínios Recentemente Vistos atuais.

Com o NSDv2, refinamos o conjunto de dados para refletir melhor o feedback e o uso do cliente, bem como a análise de dados da ocorrência até a condenação pela nossa equipe de pesquisa de ameaças da Talos. O novo algoritmo focaliza na descoberta de novos domínios de nível registrado e reduz o "ruído" de vários subdomínios que compartilham um pai comum.

Por que estamos fazendo isso?

Ouvimos o feedback do cliente e analisamos os dados que mostram como o NSD pode retardar a categorização de domínios de baixo volume, causando resultados inesperados e interrupção dos domínios se eles experimentarem um aumento repentino na popularidade. Além disso, alterações em domínios de alto volume podem observar mudanças inesperadas, por exemplo, quando uma rede de fornecimento de conteúdo introduziu alterações em seu esquema de nomenclatura.

A equipe da Talos Threat Research desenvolveu o NSDv2 em conjunto com a Umbrella para resolver esses problemas, fornecendo um sistema mais confiável e preciso para identificar domínios recém-vistos.

Como isso beneficia você?

O aprimoramento do NSDv2 foi projetado considerando a segurança e a eficiência operacional:

- Detecção aprimorada de ameaças: O NSDv2 apresenta uma melhora de no mínimo 45% na taxa de identificação de domínios que mais tarde se revelaram mal-intencionados.
- Diminuição de falsos positivos: Com um sistema de direcionamento mais preciso, você enfrenta menos interrupções de domínios sinalizados incorretamente que estão em uso regular.
- Desempenho otimizado: O conjunto de dados simplificado não só permite uma publicação mais rápida, como também permite que nossa equipe de suporte resolva rapidamente qualquer problema, se ele surgir.
- "Práticas recomendadas" de aplicação: Essa categoria é mais consistente e relevante e permite um melhor alinhamento com as expectativas do setor e do cliente.
- Dados de relatório aprimorados: O contexto e a cobertura aprimorados com o NSDv2 enriquecem os dados nos relatórios.
- Previsão aprimorada: Essa atualização auxilia o Proxy Inteligente na determinação de domínios de risco que exigem inspeção mais profunda.
- Não é necessária interação com o cliente: Essa é uma atualização de nossos pipelines para uma categorização dinâmica e não requer nenhuma migração ou alteração de política para nossos clientes. Essa é uma melhoria completamente transparente para administradores e usuários finais.

As mudanças nessa categoria serão implantadas em 13 de agosto de 2024. Agradecemos sua confiança contínua em nossos serviços e estamos ansiosos para fornecer essas melhorias significativas de segurança.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.