Habilitar categoria de segurança de domínios vistos recentemente no Umbrella

Contents

Introdução

Este documento descreve a categoria de segurança "Domínios vistos recentemente" (NSD) no Cisco Umbrella.

Informações de Apoio

O NSD (Newly Seen Domains, Domínios recém-visualizados) é uma categoria de segurança que identifica domínios consultados pela primeira vez nas últimas 24 horas por qualquer usuário do serviço DNS do Cisco Umbrella (incluindo o serviço OpenDNS gratuito para usuários domésticos). Essa categoria de segurança funciona de forma idêntica a qualquer outra Categoria de segurança e pode ser ativada como parte de uma configuração de segurança existente ou de uma nova. Os domínios permanecem na lista por um período de 24 horas.

Como o Cisco Umbrella define um domínio como "visto recentemente"

Novos domínios são frequentemente criados como parte de novas campanhas de malware. Agentes mal-intencionados por trás dessas campanhas usam novos domínios porque os métodos tradicionais baseados em assinatura não os reconhecem por bloquear sites mal-intencionados conhecidos. Por exemplo, uma campanha de phishing pode criar um novo domínio para acompanhar uma grande campanha de spam, incentivando os usuários a clicar em um link. O link ainda não é conhecido por fazer parte desta campanha e não é bloqueado por listas padrão de domínios mal-intencionados conhecidos. Antes que o link seja adicionado a essas listas, os criminosos têm tempo suficiente para extrair dados, instalar malware e obter acesso à rede.

A Categoria de Segurança de Domínios Recentemente Vistos (NSD) opera verificando os logs de DNS em busca de pesquisas de domínios que nunca foram vistos anteriormente. Devido ao

volume de consultas inválidas, para que um domínio seja marcado como visto recentemente, a consulta do cliente deve receber uma resposta adequada. Quando um domínio é visto pela primeira vez, ele é adicionado a uma lista por 24 horas. Após esse período, o domínio não será mais visto recentemente e será removido da lista.

Um relatório registra a categoria em que um domínio estava no momento em que foi consultado. Portanto, se um domínio tiver sido categorizado como visto recentemente quando consultado, ele será relatado como tal no relatório Pesquisa de atividade ou Atividade de segurança. No entanto, uma vez que o domínio expira da lista, o deslocamento desse domínio em relação aos dados atuais sobre ele (especialmente usando os relatórios Destinos ou Identidades, o Console de investigação ou a API de investigação) não mostra mais esse domínio como visto recentemente. Resumindo, revisitar um domínio vários dias depois não pode mais mostrá-lo como visto recentemente no Umbrella. Isso é por design, mas pode levar a alguma confusão inicial.

A única definição de um domínio visto recentemente é exatamente a seguinte: é visto recentemente. Como resultado, uma parte significativa dos domínios categorizados como recém-vistos não é mal-intencionada, e espera-se que ocorram detecções de domínios legítimos com essa categoria de segurança. Precauções contra essa ocorrência foram implementadas, especialmente para certos serviços e CDNs como Akamai e Cloudfront que geram subdomínios aleatórios para servir conteúdo. Garantias tradicionais contra domínios altamente populares, como Facebook e Google, também têm sido usadas para garantir que eles não sejam incluídos.

Além disso, apenas nomes de domínio totalmente qualificados (domínio de segundo nível ou um subdomínio de um domínio de segundo nível) são considerados domínios que são vistos recentemente. Os domínios de nível superior e os domínios de nível superior com código de país não são incluídos em Domínios vistos recentemente para evitar o bloqueio de grandes agrupamentos de domínios.

Notas importantes sobre implementação

Como algumas detecções indesejadas podem ser esperadas, o Cisco Umbrella recomenda que você comece a usar esse relatório no modo de auditoria ou no modo somente detecção sem bloquear ou executar qualquer ação. Por padrão, qualquer usuário com esta categoria disponível em suas configurações de segurança vê Domínios vistos recentemente como detecções nos relatórios. Isso significa efetivamente que o recurso está habilitado sem nenhum bloqueio por padrão. Na maioria dos casos, os usuários devem usar relatórios para ver qual tráfego corresponde à categoria e usar essas informações para pesquisar esses domínios mais detalhadamente para determinar se eles podem representar uma ameaça à segurança em vez de bloquear automaticamente.

Outra advertência importante é que a primeira consulta ao domínio é permitida. Isso ocorre porque o Cisco Umbrella nunca viu uma consulta a esse domínio anteriormente e, como tal, ele não foi processado pelos sistemas de registro para ser incluído como parte da categoria Domínios recentemente vistos. O intervalo de tempo entre quando um domínio é consultado pela primeira vez e antes de aparecer na lista de domínios que correspondem à categoria é de

aproximadamente cinco minutos, mas pode se estender além disso porque o Cisco Umbrella não processa necessariamente 100% dos logs de consulta DNS (devido ao tempo e volume de processamento).

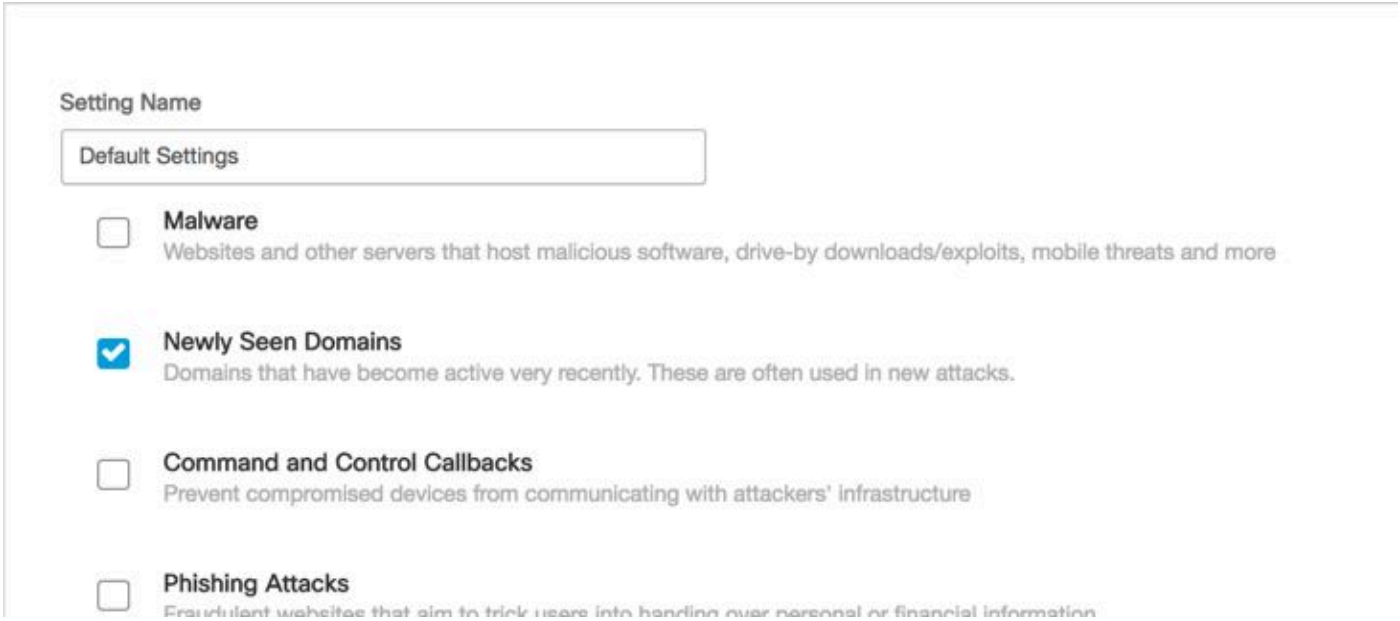
Uso de proxy em domínios vistos recentemente

Os clientes que utilizam o Umbrella Intelligent Proxy também observam que alguns domínios na categoria NSD recebem proxy. Isto é por projeto. A equipe da Umbrella Labs usa os dados coletados por meio do proxy desses novos domínios para determinar se eles podem ser adicionados às categorias de malware imediatamente. Um efeito colateral disso é que o tráfego fora do padrão enviado a um Domínio visto recentemente que também está recebendo proxy é descartado no nível de proxy. O Proxy Inteligente só faz o proxy das portas 80 e 443, as portas tradicionalmente usadas para o tráfego da Web. Isso acontece automaticamente quando o proxy é habilitado, independentemente da categoria estar bloqueada. Para evitar que um único domínio visto recentemente seja submetido a proxy, adicione-o à lista de permissões apropriada.

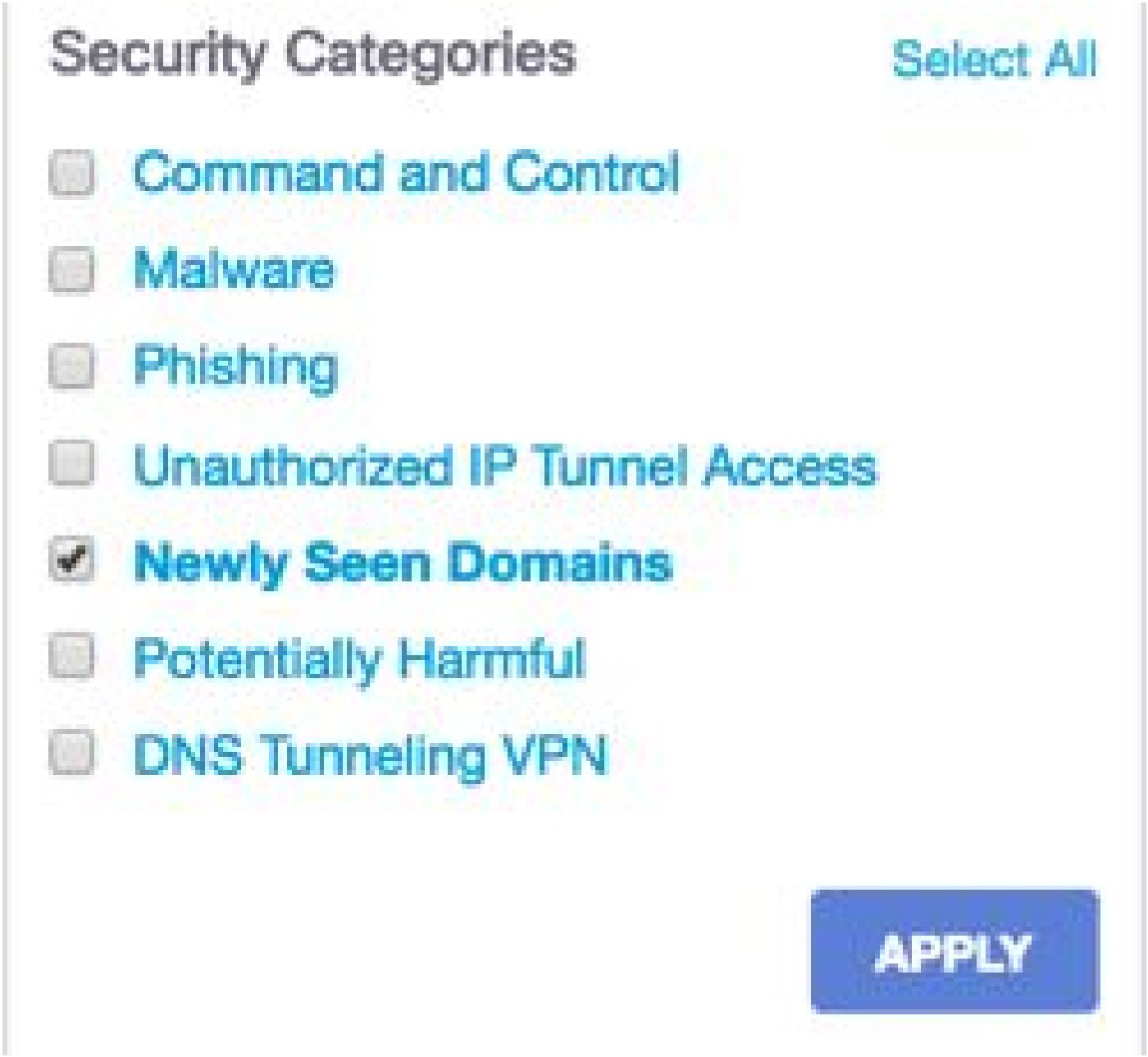
Mais informações sobre o Intelligent Proxy podem ser encontradas em nossa documentação Enable the Intelligent Proxy.

Habilitar Domínios Recentemente Vistos

A categoria de segurança Domínio Visto Recentemente pode ser habilitada como qualquer outra em Políticas > Configurações de Segurança e, em seguida, editar uma configuração de segurança existente. Como alternativa, ela pode ser feita no próprio Assistente de Configuração de Política.



Os domínios vistos recentemente também podem ser filtrados em determinados relatórios, como Pesquisa de atividades.



115015007423

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.