Abilita la categoria di sicurezza Domini appena visti in Umbrella

Sommario

Introduzione

Questo documento descrive la categoria di sicurezza "Nuovi domini visti" (NSD) in Cisco Umbrella.

Premesse

NSD (Newly Seen Domains) è una categoria di sicurezza che identifica i domini interrogati per la prima volta nelle ultime 24 ore da qualsiasi utente del servizio DNS Cisco Umbrella (incluso il servizio OpenDNS gratuito per gli utenti privati). Questa categoria di protezione funziona in modo identico a qualsiasi altra categoria di protezione e può essere abilitata come parte di un'impostazione di protezione esistente o nuova. I domini restano nell'elenco per un periodo di 24 ore.

Definizione di un dominio da parte di Cisco Umbrella come "appena visto"

I nuovi domini vengono spesso creati come parte di nuove campagne malware. Gli attori malintenzionati che si celano dietro queste campagne utilizzano nuovi domini perché i metodi tradizionali basati su firme non li riconoscono per il blocco di siti web dannosi noti. Ad esempio, una campagna di phishing può creare un nuovo dominio da affiancare a un'importante campagna di spam per incoraggiare gli utenti a fare clic su un collegamento. Il link non fa ancora parte di questa campagna e non è bloccato da elenchi standard di domini noti-dannosi. Prima che il link venga aggiunto a tali elenchi, i criminali hanno tempo sufficiente per esfiltrare dati, installare malware e ottenere accesso alla rete.

La categoria di sicurezza NSD (Newly Seen Domains) funziona controllando i registri DNS per individuare ricerche di domini che non sono mai state rilevate in precedenza. A causa del volume

di query non valide, affinché un dominio venga contrassegnato come appena visualizzato, è necessario che la query client riceva una risposta corretta. Una volta individuato, il dominio viene aggiunto all'elenco per 24 ore. Trascorso questo periodo, il dominio non viene più visualizzato e viene rimosso dall'elenco.

Un report registra la categoria sotto cui si trovava un dominio al momento della query. Pertanto, se un dominio è stato classificato come appena visualizzato quando è stato interrogato, viene segnalato come tale nel report Ricerca attività o Attività protezione. Tuttavia, una volta che il dominio scade dall'elenco, eseguendo il pivot su tale dominio in base ai dati correnti su di esso (in particolare utilizzando i nuovi report Destinazioni o Identità, Investigate Console, o Investigate API) non visualizza più tale dominio come appena visualizzato. In breve, rivisitare un dominio diversi giorni dopo non può più mostrarlo come appena visto in Umbrella. Questo è il progetto, ma può portare ad una certa confusione iniziale.

L'unica definizione di dominio appena visto è esattamente questa: è stato appena visto. Di conseguenza, una parte significativa dei domini classificati come nuovi visualizzati non sono dannosi e si prevede che il rilevamento di domini legittimi si verifichi con questa categoria di sicurezza. Sono state implementate precauzioni contro questo evento, soprattutto per alcuni servizi e CDN come Akamai e Cloudfront che generano sottodomini randomizzati per servire il contenuto. Anche le tradizionali garanzie contro i domini più popolari, come Facebook e Google, sono state usate per assicurarsi che questi non siano inclusi.

Inoltre, solo i nomi di dominio completi (dominio di secondo livello o sottodominio di secondo livello) sono considerati domini appena visualizzati. I domini di primo livello e i domini di primo livello con codice paese non sono inclusi nei Domini visualizzati di recente per evitare il blocco di grandi raggruppamenti di domini.

Note importanti sull'implementazione

Poiché è possibile prevedere alcuni rilevamenti indesiderati, Cisco Umbrella consiglia di iniziare a utilizzare questo report in modalità di controllo o di rilevare solo la modalità senza bloccare o intraprendere alcuna azione. Per impostazione predefinita, gli utenti con questa categoria disponibile nelle impostazioni di protezione visualizzano i nuovi domini visualizzati come rilevamenti nei report. Ciò significa che la funzione è abilitata senza alcun blocco per impostazione predefinita. Nella maggior parte dei casi, gli utenti devono utilizzare i report per verificare il traffico che corrisponde alla categoria e utilizzare le informazioni per eseguire ricerche più approfondite su questi domini e determinare se possono rappresentare una minaccia per la sicurezza, anziché bloccarli automaticamente.

Un'altra importante osservazione riguarda il fatto che è consentita la prima query sul dominio. Infatti, in precedenza Cisco Umbrella non aveva mai ricevuto una query su tale dominio e, pertanto, non è stata elaborata dai sistemi di log per essere inclusa nella categoria Nuovi domini visualizzati. L'intervallo di tempo tra il momento in cui un dominio viene interrogato per la prima volta e il momento in cui viene visualizzato nell'elenco dei domini corrispondenti alla categoria è di circa cinque minuti, ma può estendersi oltre, in quanto Cisco Umbrella non elabora

necessariamente il 100% dei log di query DNS (a causa del tempo di elaborazione e del volume).

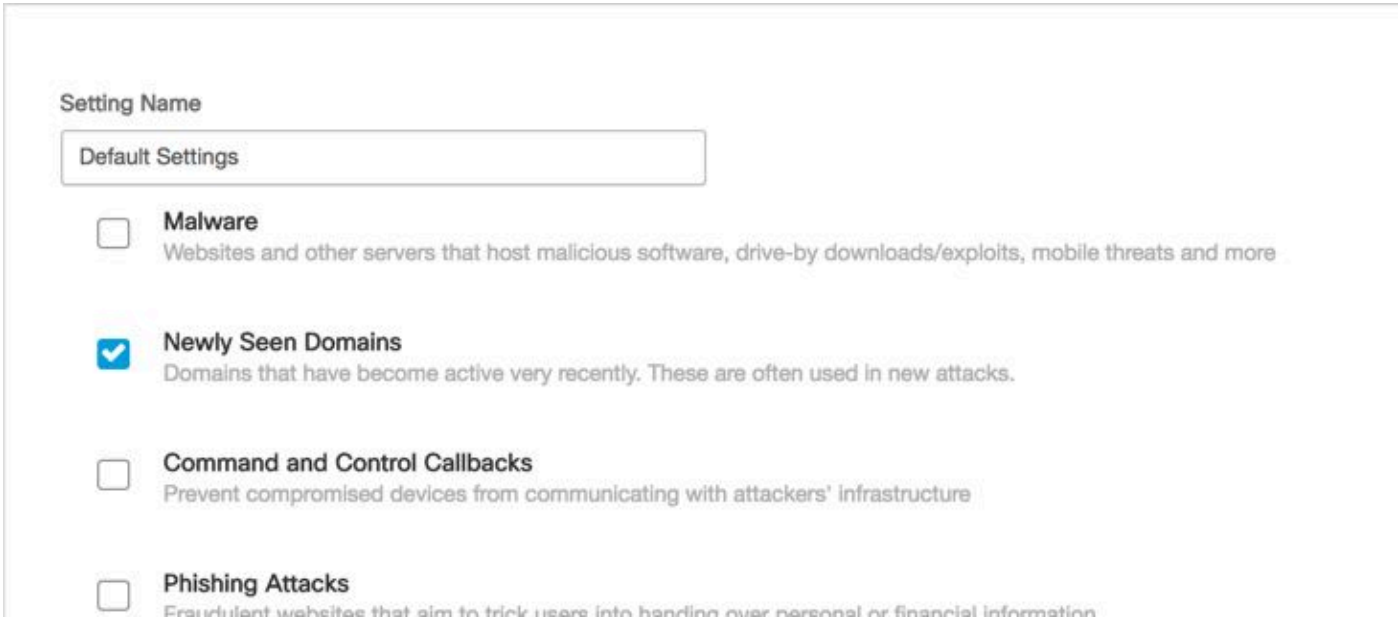
Proxy dei nuovi domini visualizzati

I clienti che utilizzano l'Umbrella Intelligent Proxy osservano anche che alcuni domini nella categoria NSD sono proxy. Questo è il risultato del progetto. Il team di Umbrella Labs utilizza i dati raccolti tramite l'inoltro di questi nuovi domini per determinare se possono essere aggiunti immediatamente alle categorie di malware. Un effetto collaterale di questo è che il traffico non standard inviato a un dominio appena visto che è anche in fase di proxy viene scartato a livello di proxy. Il proxy intelligente supporta solo le porte 80 e 443, le porte tradizionalmente utilizzate per il traffico Web. Questo si verifica automaticamente quando il proxy è attivato, indipendentemente dal fatto che la categoria sia bloccata o meno. Per impedire che un singolo dominio appena visto venga inserito nel proxy, aggiungerlo all'elenco degli oggetti autorizzati appropriato.

Per maggiori informazioni sul proxy intelligente, consultare la nostra documentazione Enable the Intelligent Proxy.

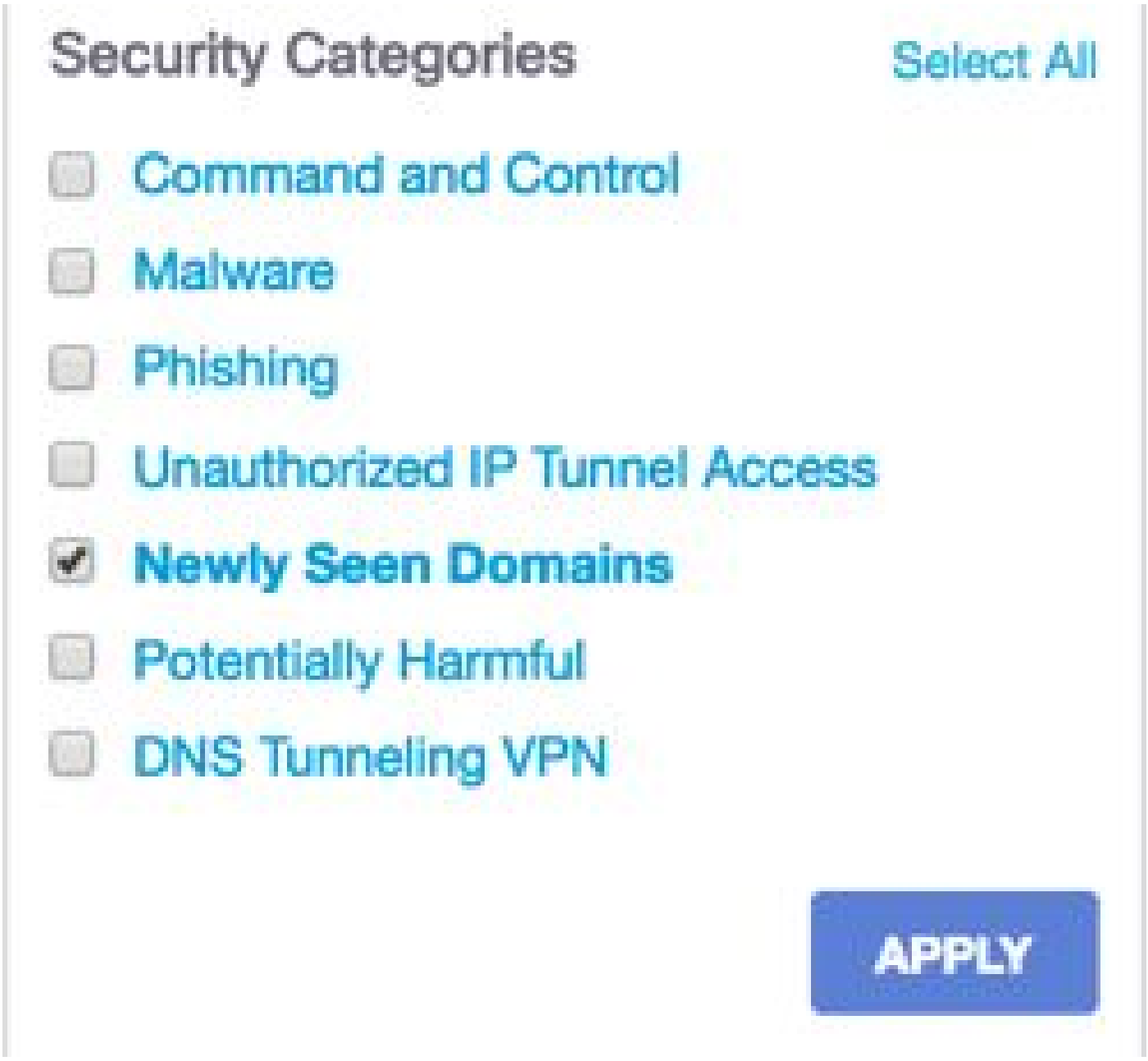
Abilita domini visualizzati di recente

La categoria di protezione Nuovo dominio visualizzato può essere abilitata come qualsiasi altra in Criteri > Impostazioni di protezione, quindi modificare un'impostazione di protezione esistente. In alternativa, è possibile eseguire questa operazione nella Configurazione guidata criteri stessa.



115014822286

I nuovi domini visualizzati possono essere filtrati anche in alcuni report, ad esempio Ricerca attività.



115015007423

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).