Nuovi miglioramenti alla sicurezza Umbrella - Domini appena visti

Sommario

Introduzione

Questo documento descrive i prossimi miglioramenti alla sicurezza per la categoria Nuovi domini visti (NSD, Newly Seen Domains) dei servizi Secure Access e Umbrella.

Panoramica

Siamo lieti di informarvi su un importante miglioramento alla categoria NSD (Newly Seen Domains), un aspetto chiave dei nostri servizi Secure Access e Umbrella, promosso dal team di ricerca Talos Threat.

Cosa stiamo facendo?

Nell'ambito dei nostri continui sforzi per rafforzare la tua sicurezza, stiamo implementando un sistema aggiornato per NSD, in transizione alla versione 2 (NSDv2). Questa nuova iterazione espande in modo significativo i dati di origine, in quanto ora include l'intero set di DNS passivi che alimenta il nostro prodotto Investigate (800B query al giorno), un miglioramento rispetto alla metodologia di campionamento statistico degli attuali domini appena visti.

Con NSDv2, abbiamo perfezionato il set di dati per riflettere più da vicino il feedback e l'utilizzo dei clienti, così come l'analisi dei dati dell'occorrenza alla convinzione da parte del nostro team di ricerca Talos Threat. Il nuovo algoritmo si concentra sull'individuazione di nuovi domini a livello registrato e riduce il "rumore" di più sottodomini che condividono un elemento padre comune.

Perché stiamo facendo questo?

Abbiamo ascoltato i commenti dei clienti e analizzato i dati che mostrano come NSD potrebbe ritardare la categorizzazione dei domini a basso volume, causando risultati inattesi e interruzioni ai domini in caso di improvviso aumento della popolarità. Inoltre, le modifiche ai domini con volumi elevati possono comportare cambiamenti imprevisti, ad esempio quando una rete di distribuzione dei contenuti ha introdotto modifiche nello schema di denominazione.

Il team di Talos Threat Research ha sviluppato NSDv2 in collaborazione con Umbrella per risolvere questi problemi, fornendo un sistema più affidabile e accurato per l'identificazione dei nuovi domini visti.

Quali sono i vantaggi per voi?

Il miglioramento di NSDv2 è stato progettato tenendo presente la sicurezza e l'efficienza operativa:

- Rilevamento delle minacce migliorato: NSDv2 vanta un miglioramento minimo del 45% nella percentuale di identificazione dei domini che in seguito si riveleranno dannosi.
- Riduzione dei falsi positivi: Grazie a un sistema di destinazione più preciso, è possibile riscontrare un numero inferiore di interruzioni dovute a domini contrassegnati in modo errato e utilizzati regolarmente.
- Prestazioni ottimizzate: Il set di dati semplificato non solo consente una pubblicazione più rapida, ma consente anche al team di supporto di affrontare rapidamente eventuali problemi, se si verificano.
- Applicazione delle "migliori pratiche": Questa categoria è più coerente e pertinente e consente un migliore allineamento con le aspettative del settore e della clientela.
- Dati di reporting migliorati: Il contesto e la copertura migliorati con NSDv2 arricchiscono i dati nei report.
- Previsione migliorata: Questo aggiornamento aiuta il proxy intelligente a determinare i domini più rischiosi che richiedono un'ispezione più approfondita.
- Non è richiesta alcuna interazione da parte del cliente: Si tratta di un aggiornamento delle pipeline per una categorizzazione dinamica e non richiede alcuna migrazione o modifica delle regole per i clienti. Si tratta di un miglioramento completamente trasparente per gli amministratori e gli utenti finali.

Le modifiche a questa categoria saranno implementate il 13 agosto 2024. Ti ringraziamo per la tua costante fiducia nei nostri servizi e siamo ansiosi di offrirti questi significativi miglioramenti in termini di sicurezza.

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).