Bevorstehende Verbesserungen bei Umbrella Security - Neu erkannte Domänen

Inhalt

Einleitung

In diesem Dokument werden bevorstehende Sicherheitserweiterungen der NSD-Kategorie (Newly Seen Domains) der Secure Access- und Umbrella-Services beschrieben.

Überblick

Wir freuen uns, Sie über eine wichtige Erweiterung der Kategorie der neu erkannten Domänen (NSD) informieren zu können, einem zentralen Aspekt unserer Services für sicheren Zugriff und Umbrella, die vom Talos Threat Research Team angeführt werden.

Was machen wir?

In unserem ständigen Bemühen, Ihre Sicherheit zu erhöhen, führen wir ein aktualisiertes System für NSD ein, das auf Version 2 (NSDv2) umgestellt wird. Diese neue Iteration erweitert die Quelldaten erheblich, da sie nun den vollständigen Satz unseres passiven DNS umfasst, der unser Produkt Investigate (800 B Abfragen/Tag) antreibt, eine Verbesserung gegenüber der statistischen Sampling-Methodik der aktuellen neu gesehenen Domänen.

Mit NSDv2 haben wir den Datensatz verfeinert, um Kundenfeedback und -nutzung sowie die Datenanalyse des Vorfalls bis zur Verurteilung durch unser Talos Threat Research Team genauer widerzuspiegeln. Der neue Algorithmus konzentriert sich auf die Erkennung neuer Domänen auf registrierter Ebene und reduziert das "Rauschen" mehrerer Subdomänen, die ein gemeinsames übergeordnetes Element verwenden.

Warum tun wir das?

Wir hörten Kundenfeedback und analysierten Daten, die zeigten, wie NSD die Kategorisierung von Domänen mit geringem Volumen verzögern könnte, was unerwartete Ergebnisse und Unterbrechungen von Domänen zur Folge hätte, wenn sie plötzlich populärer würden. Darüber hinaus können Änderungen an Domänen mit hohem Datenvolumen zu unerwarteten

Verschiebungen führen, z. B. wenn ein Netzwerk zur Inhaltsbereitstellung Änderungen an seinem Namensschema einführt.

Das Team von Talos Threat Research hat NSDv2 in Zusammenarbeit mit Umbrella entwickelt, um diese Probleme zu beheben und ein zuverlässigeres und präziseres System zur Identifizierung neu erkannter Domänen bereitzustellen.

Wie profitieren Sie davon?

Die NSDv2-Erweiterung wurde im Hinblick auf Sicherheit und Betriebseffizienz entwickelt:

- Verbesserte Bedrohungserkennung: NSDv2 bietet eine mindestens 45%ige Verbesserung bei der Geschwindigkeit der Identifizierung von Domänen, die sich später als schädlich erweisen.
- Weniger Fehlalarme: Mit einem präziseren Targeting-System kommt es zu weniger Unterbrechungen durch falsch gekennzeichnete Domänen, die regelmäßig verwendet werden.
- Optimierte Leistung: Der optimierte Datensatz ermöglicht nicht nur eine schnellere Veröffentlichung, sondern ermöglicht auch unserem Support-Team, Probleme schnell zu beheben, falls sie auftreten.
- Best Practice bei der Durchsetzung: Diese Kategorie ist konsistenter und relevanter und ermöglicht eine bessere Anpassung an die Erwartungen der Branche und des Kunden.
- Erweiterte Berichtsdaten: Der verbesserte Kontext und die verbesserte Abdeckung mit NSDv2 reichern die Daten in Berichten an.
- Verbesserte Vorhersage: Dieses Update unterstützt den Intelligent Proxy bei der Ermittlung riskanter Domänen, die eine eingehendere Prüfung erfordern.
- Keine Kundeninteraktion erforderlich: Dies ist ein Update unserer Pipelines für eine dynamische Kategorisierung und erfordert keine Migration oder Richtlinienänderungen für unsere Kunden. Dies ist eine vollkommen transparente Verbesserung für Administratoren und Endbenutzer.

Die Änderungen an dieser Kategorie sollen am 13. August ^{2024} implementiert werden. Wir sind dankbar für Ihr anhaltendes Vertrauen in unsere Services und freuen uns darauf, Ihnen diese wichtigen Sicherheitsverbesserungen bieten zu können.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.