今後予定される包括セキュリティの機能拡張：新たに出現するドメイン

内容

はじめに

このドキュメントでは、Secure AccessおよびUmbrellaサービスの Newly Seen Domains(NSD)カテゴリに対する今後のセキュリティ拡張について説明します。

概要

Talos Threat Researchチームが率いる、セキュアアクセスおよびアンブレラサービスの重要な側面であるNewly Seen Domains(NSD)カテゴリの重要な機能強化についてお知らせします。

何してるの？

セキュリティ強化の取り組みの一環として、NSDの更新システムを実装し、バージョン2(NSDv2)に移行します。 この新しいイテレーションでは、ソースデータが大幅に拡張され、Investigate製品を強化するパッシブDNS（1日あたり800億件のクエリ）のフルセットが含まれるようになり、現在の新しく見られたドメインの統計サンプリング手法が改善されました。

NSDv2では、お客様のフィードバックと使用状況をより密接に反映するようにデータセットを調整し、Talos Threat Research Teamによる有罪判決の発生に関するデータ分析を行いました。新しいアルゴリズムは、新しい登録レベルのドメインの検出に重点を置いており、共通の親を共有する複数のサブドメインの「ノイズ」を軽減します。

なぜこんな事を？

お客様のフィードバックに耳を傾け、NSDが低容量ドメインの分類を遅らせ、急激な普及が進んだ場合に予期せぬ結果やドメインの混乱を引き起こす可能性があることを示すデータを分析しました。また、大容量ドメインに対する変更は、たとえばコンテンツ配信ネットワークの命名方式に変更が加えられた場合など、予期しない変化を示す可能性があります。

Talos Threat Researchチームは、これらの問題を解決するためにUmbrellaと連携してNSDv2を開発し、新たに検出されたドメインを特定するためのより信頼性の高い正確なシステムを提供して

います。

どのような利点がありますか。

NSDv2機能拡張は、セキュリティと運用効率を念頭に置いて設計されています。

- 脅威検出の向上：NSDv2では、後に悪意があると判明したドメインの特定率が45 %以上向上しています。
- 誤検出の減少：より正確なターゲットシステムを使用することで、通常の使用で誤ってフラグが設定されたドメインによる中断が減少します。
- パフォーマンスの最適化：合理化されたデータセットにより、迅速な公開が可能になるだけでなく、問題が発生した場合に迅速に対応できます。
- 適用の「ベストプラクティス」:このカテゴリはより一貫性があり、関連性が高く、業界および顧客の期待により適しています。
- 充実したレポートデータ：NSDv2の改善されたコンテキストとカバレッジにより、レポートのデータが強化されます。
- 予測の向上：この更新により、インテリジェントプロキシは、より深いインスペクションが必要なリスクの高いドメインを決定できるようになります。
- カスタマーインタラクションは不要：これは、動的なカテゴリ化のためのパイプラインの更新であり、お客様の移行やポリシーの変更は必要ありません。これは、管理者とエンドユーザにとって完全に透過的な改善点です。

このカテゴリの変更は、2024年8月13日に導入される予定です。引き続き、弊社のサービスに対する信頼をお持ちいただき、感謝しております。また、セキュリティの大幅な向上に努めております。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。