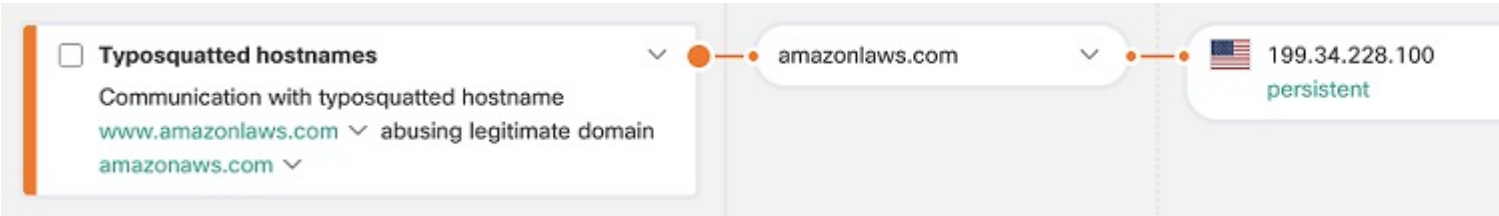
2021 年 3 月

2021 年 3 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

新しいタイポスクワッティング分類子

タイポスクワッティングとは、ユーザが Web ブラウザに URL を入力する際の入力ミス（タイプミス）を利用する URL ハイジャックの一種です。これにより、ユーザは攻撃者が所有する別の Web サイトに誘導されます。タイポスクワッティング URL は、次のように、正規の URL に視覚的に似ています。

図 *1*：例：余分な文字が追加されたタイポスクワッティングのホスト名



通常、タイポスクワッティング URL は、広告から利益を得るために使用される広告ページや、ユーザから情報を盗むために使用されるフィッシングページなどのオンライン詐欺に誘導します。

図 *2 :* 例：*Amazon AWS* にアクセスしようとするユーザをターゲットとする広告ページ

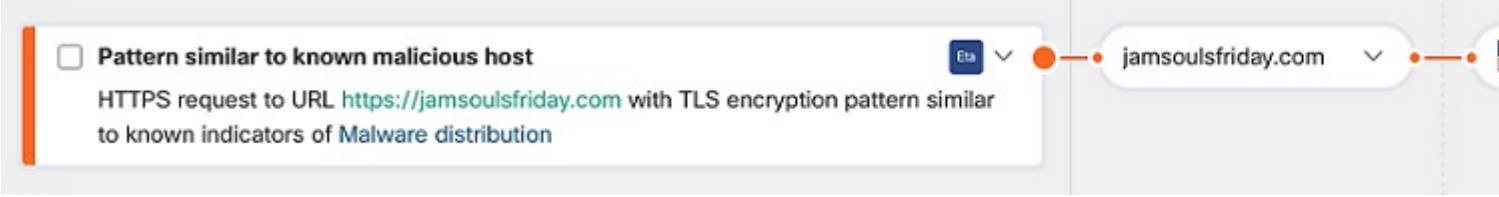
新しい分類子は、最も一般的なドメインをターゲットとするタイポスクワッティングドメインからユーザを保護することを目的としています。分類子は、ドメインの類似性を計算することで、最も一般的なドメインに類似するドメインを効率的に識別します。その後、タイポスクワッティング ドメインの運用期間などの追加パラメータに基づいて脅威の重大度を決定します。

これは、**[アラート（Alert）]**> **[アラート詳細（Alert detail）]**>**[セキュリティイベント（Security events）]** で確認できます。

新しい TLS パターン分類子

新しい分類子は、Transport Layer Security（TLS）フィンガープリントテクノロジーの上に構築されています。https://en.wikipedia.org/wiki/Transport_Layer_Security暗号化トラフィック分析（ETA）からの TLS ヘッダーと追加のグローバルおよびローカルコンテキストの機能を考慮して、分類子は TLS フットプリントに基づいて疑わしいアプリケーションおよび悪意のあるアプリケーションを検出します。https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.html分類子は、暗号化された通信を分析することで、HTTP で通信する脅威を対象としたモデルの機能を拡張します。

図 *3 :* 例：悪意のあることが知られているホストに類似した *TLS* パターン



これは、**[アラート（Alert）]**> **[アラート詳細（Alert detail）]**>**[セキュリティイベント（Security events）]** で確認できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。