2024 年 2 月

2024 年 2 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。

追加の脅威検出

新しい脅威検出をポートフォリオに追加しました。

- Coyote
- Donut Loader
- RisePro

また、既存の脅威検出のインジケーターも更新しました。

Coyote

Coyuteは、主にラテンアメリカのユーザーを標的とするバンキング型トロイの木馬で、支払請求書を装った電子メールによるフィッシング手法（T1566.001）を利用します。このマルウェアは、配布に Squirrel インストーラを使用します。Coyute は NodeJS や Nim などのプログラミング言語を使用して作成されていて、このマルウェアの適応性と回避能力を示しています。このトロイの木馬は、検出を回避するために、文字列難読化技術（T1027）と AES暗号化を組み合わせて使用しています。被害者のシステムにインストールされた Coyute は、コマンドアンドコントロール（C2）サーバー（TA0011）との通信を確立して、スクリーンショットを要求したり、キーロギングを実行したりします。

お使いの環境で Coyote が検出されたかどうかを確認するには、[Coyote脅威の詳細（Coyote Threat Detail）] をクリックして、グローバル脅威アラートで詳細を表示します。

Donut Loader

Donut Loader は、スクリプトやアセンブリをメモリ内で実行するための高度なツールキットであり、悪意のある目的にも使用されます（T1055.009）。ステルス Windows プロセスインジェクション（T1055）用に暗号化されたシェルコード（T1027）を生成します。このマルウェア

は、Chaskey 暗号を使用して暗号化されたペイロードをシェルコード内に埋め込むか、URL からダウンロードすることによって（T1105）ステージレスに動作します。実行されると、メモリトレースを消去し（T1070）、新しいアプリケーションドメインでペイロードを分離することで検出を回避します。

お使いの環境で Donut Loader が検出されたかどうかを確認するには、[Donut Loader脅威の詳細（Donut Loader Threat Detail）] をクリックして、グローバル脅威アラートで詳細を表示します。

RisePro

RisePro は、Telegram で販売されている情報窃盗マルウェアであり、Private Loader マルウェアによって配布されます。RisePro は、感染したデバイスからデータを収集したり（TA0009）、スクリーンショットをキャプチャしたりできます（T1113）。RisePro は、ブラウザのログイン情報、暗号資産ウォレット（アドレスと秘密キー）、およびクレジットカード情報を読み取って盗むことができます。RisePro によって収集されたデータは、zip ファイルに圧縮され、HTTP メッセージで盗み出されます（T1071.001）。この窃盗マルウェアは、コマンドアンドコントロール（C2）（T1041）を使用して構成を取得し、他のマルウェアをロードすることもできます。

お使いの環境で RisePro が検出されたかどうかを確認するには、[RisePro脅威の詳細（RisePro Threat Detail）] をクリックして、グローバル脅威アラートで詳細を表示します。

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。