2023 年 3 月

2023 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。

追加の脅威検出

以下の新しい脅威検出をポートフォリオに追加しました。

- Amadey
- BatLoader
- Retadup
- Stealc
- ViperSoftX

また、既存の脅威検出のインジケーターも更新しました。

Amadey

Amedy は、データを盗み、他のマルウェアを展開することで知られるトロイの木馬ボットです。フィッシング（T1566）電子メールを介して配信されるか、他のマルウェアファミリによって展開されます。レジストリエントリ（T1547.001）とスケジュールされたタスク（T1053.005）を介して、攻撃対象のデバイスでの永続性を維持します。コマンドアンドコントロールサーバーと通信する前に、攻撃対象のデバイス（T1005）からドメイン名、ユーザー名、コンピュータ名、OSバージョンなどのさまざまなデータを収集します。収集されたデータの漏洩（T1041）後、エクスプロイトキット、情報窃盗、ランサムウェアなどのマルウェアをダウンロード（T1105）およびインストールできます。

お使いの環境でAmadeyが検出されたかどうかを確認するには、[Amadey脅威の詳細（Amadey 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。

BatLoader

BatLoader は、情報窃盗マルウェア、バンキング型トロイの木馬、ランサムウェア、およびその他のローダーなど、さまざまなマルウェアを攻撃対象のデバイスにインストールするモジュラーダウンローダーです。BatLoader は、クラックされたソフトウェア（T1204.001）を使用して配布されます。特に、Adobe、AnyDesk、CCleaner、TeamViewer、Zoom になりすますことが確認されています。攻撃対象が MSI ファイル（T1204.002）をダウンロードして実行すると、さらなる感染のためにカスタムアクションを介して Powershell（T1059.001）ペイロードを実行します。その後、攻撃対象のデバイスは、コマンドアンドコントロールサーバー（T1071.001）に接続し、他のペイロード（T1105）をダウンロードします。

お使いの環境で GootLoader が検出されたかどうかを確認するには、[BatLoader脅威の詳細（BatLoader 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。

Retadup

Retadup は、自己複製機能を備えた Monero マイナーです。攻撃対象のデバイス（T1091）の使用可能なすべての外部ドライブに LNK ファイルをコピーします。その後、悪意のある AutoIt でコンパイルされたスクリプト（T1204.002）を実行し、ホスト名や OS バージョンなどのエンコードされたホスト情報（T1132.001）をコマンドアンドコントロール サーバーにエクスポートします。スティーラーやランサムウェアなどの追加のマルウェア（T1105）を展開できます。2019 年にテイクダウンされたにもかかわらず、特に中南米のデバイスをターゲットにしたネットワークで引き続き確認されています。多くの場合、ペイロード名は、正規のソフトウェアや、Google や Microsoft などの企業を模倣します（T1036.005）。

お使いの環境で Retadup が検出されたかどうかを確認するには、[Retadup脅威の詳細（Retadup 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。

Stealc

Stealc は、ダークネットフォーラムで販売されている情報窃取型マルウェアです。フィッシングメール（T1566.001）、悪意のあるオンライン広告、および偽のソフトウェアのダウンロード（T1036）を介して配布されます。コマンドアンドコントロール サーバーと通信するために、Stealc は HTTP や HTTPS（T1071.001）などのアプリケーション層プロトコルを使用できます。また、DNS 要求（T1071.004）を活用し、攻撃対象のデバイスから入力アクション（T1056）またはスクリーンショット（T1113）をキャプチャすることもできます。Stealc は、Web サービス（ T1567 ）または FTP や SMTP などの代替プロトコル（ T1048 ）を使用して、盗んだデータをコマンドアンドコントロール サーバーに送信します。https://attack.mitre.org/versions/v12/techniques/T1567https://attack.mitre.org/versions/v12/techniques/T1048

お使いの環境で Stealc が検出されたかどうかを確認するには、[Stealc脅威の詳細（Stealc 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。

ViperSoftX

ViperSoftX は、VenomSoftX と呼ばれる Chrome ブラウザ拡張機能を展開するマルウェアです。マルウェアは、クラッキングされたソフトウェアまたはトレントダウンロード（T1036）を使用して配布されます。暗号化されたバイナリ（T1027）、Powershell ペイロード（T1059.001）、およびブラウザ拡張機能（T1176）を活用してタスクを実行できます。HTTP または HTTPS

（T1071）を使用してコマンドアンドコントロール サーバーと通信します。このマルウェアは、暗号通貨ウォレット（T1496）の窃取、クリップボードデータの収集（T1115）、コマンドの実行（TA0002）、およびその他のタスクを実行できます。

お使いの環境で ViperSoftX が検出されたかどうかを確認するには、[ViperSoftX脅威の詳細（ViperSoftX 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。