2023 年 12 月

2023 年 12 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。

- Agniane Stealer
- Pikabot
- SectopRAT

また、既存の脅威検出のインジケーターも更新しました。

Agniane Stealer

Agnianeは、ブラウザ、パスワード、暗号通貨ウォレット、およびRDPログイン情報（T1005）を標的とする窃取マルウェアです。2023 年以降、Malware-as-a-Service モデルを通じて人気を得ています。他の多くの窃取マルウェアと同様に、ファイルを収集して侵入し（T1041）、追加のペイロードを展開（T1105）できるグラバーおよびローダーモジュールが含まれています。WMI（T1047）、PowerShell（T1059.001）、および ConfuserEx 難読化ツール（T1027）を使用して保護されている .NET 実行可能ファイルを使用します。

お使いの環境で窃取マルウェア Agniane が検出されたかどうかを確認するには、[Agniane Stealer 脅威の詳細（Agniane Stealer 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。

Pikabot

Pkabotは、ローダーとコアペイロードで構成されるモジュール型マルウェアです。C/C++で記述されていて、被害者のシステムに他のマルウェアを展開するためによく使用されます（T1105）。CIS 諸国のメンバーはターゲットリストから除外され、多くの場合、悪意のある添付ファイルを含むフィッシングメール（T1566.001）で配信されます。そのコアモジュール

は、多くの場合、ファイルのダウンロードやさまざまなペイロードの実行（TA0002）など、複数の段階を介して展開されます。Pkabotは回避能力が非常に高く、VM対策/デバッグ（T1622）技術と難読化された文字列（T1027）を活用して検出を回避します。これは Qakbot（S0650）や DarkGate などのマルウェアと同様の動作を示します。

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

SectopRAT

SectopRAT（別名 ArechClient2）は、正規のソフトウェアを装った悪意のあるリンク（T1204.001）によって配布される、.NET リモートアクセス型トロイの木馬です。SectopRAT には複数の機能があります。感染したデバイスからオペレーティングシステムやハードウェア情報などの詳細情報を抽出したり（T1082）、保存されているログイン情報を窃取したり（T1552.001）、非表示のブラウザセッションを起動したりできます。アプリケーション層プロトコル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（T1071）、非標準ポート（T1571）を使用して他のペイロードをダウンロードし、情報を盗み出します。SectopRATには、マルウェア対策ソリューションを無効にし、サンドボックスの実行を回避するためのさまざまな機能があります。

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