2023 年 5 月

2023 年 5 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。

- DarkCrystal RAT
- Fabookie
- Nemesis Project
- TrueBot

また、既存の脅威検出のインジケーターも更新しました。

DarkCrystal RAT

DarkCrystal RAT（別名 DCRAT）は、攻撃対象のデバイスを制御して情報を盗むことができるリモートアクセス型のトロイの木馬です。フィッシング（T1566）、その他のローダー（PrivateLoader など）、または偽のソフトウェアのクラックやアップデート（T1036）を介して配布されます。モジュール型マルウェアであるため、キーロギング（T1056.001）を実行し、感染したデバイスから Cookie、ログイン情報、およびその他の情報を盗むことができます。情報が収集されると、コマンドアンドコントロール通信（T1041）を介して漏洩します。

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

Fabookie

Fabookie は、感染したデバイスからログイン情報（特に Facebook ログイン情報）を盗むことを目的とした情報窃取プログラムです。Fabookie は通常、SmokeLoader、PrivateLoader、Nullmixer などの他のマルウェアによって配布されます。Fabookie がデバイスにインストールされると、

保存されているログイン情報（T1552）を検索し、システムにインストールされているソフトウェアに関する情報を収集します（T1518）。ログイン情報を取得すると、Facebook API とやり取りし、コマンドアンドコントロールサーバー（T1071）と通信します。

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

Nemesis Project

Nemesis Project は、ダークネットフォーラムで販売されている情報窃取プログラムです。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。また、Dave や Minodo Loader などの他のマルウェアとともに配布される可能性もあります。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、Nemesis Project 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し、DNS 要求（T1071.004）を活用できます。情報窃取プログラムは、VPN とブラウザを標的とし、攻撃対象システムから入力アクション（T1056）とスクリーンショット（T1113）をキャプチャできます。Nemesis Project マルウェアは、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。

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

TrueBot

TrueBot（サイレンスとも呼ばれる）は、攻撃対象デバイスで追加のペイロードを取得して実行できるダウンローダーマルウェアです。これは、以前の感染（T1105）を介して、または一般向けアプリケーション（T1190）をエクスプロイトすることによって展開できます。TrueBot は、Grace（S0383）、Clop（S0611）、CobaltStrike（S0154）などのマルウェアやツールを展開することが知られています。TrueBot 感染は、ローダーとダウンローダーの 2 つのモジュールで構成されます。ローダーが復号化すると（T1140）、追加のペイロードを取得するためにダウンローダーをドロップします。TrueBot は、スケジュールされたタスク（T1053.005）とレジストリ実行キー（T1547.001）によって永続性を維持します。感染チェーンの後半で関連するマルウェアが使用されているため、TA505（G0092）の一部であると想定されています。

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