2023 年 6 月

2023 年 6 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。

- AMOS
- JackalControl
- RMS
- Satacom
- UNC4841

また、既存の脅威検出のインジケーターも更新しました。

AMOS

AMOS は Atomic macOS Stealer とも呼ばれ、Apple MacOS を標的とする情報窃取プログラムです。キーチェーンパスワード（T1555.001）、暗号ウォレット、システムデータ、ローカルファイル、さらには OS ログイン情報のダンプ（T1003）など、さまざまなタイプの情報のキャプチャに焦点を当てています。データを収集すると（T1560）、コマンドアンドコントロールチャネル（T1041）を介してデータを盗み出します。

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

JackalControl

JackalControl は、攻撃者が攻撃対象デバイスを制御できるようにする、GoldenJackal APT によって使用されるトロイの木馬です。JackalControl は、偽の Skype インストーラまたは添付ファイルとして配布される MS Word ドキュメントを介して配布されます。スケジュールされたタス

ク（T1053.005）、レジストリキー（T1547.001）、または Windows サービス（T1543.003）を作成することで、JackalControl は永続性を得ることができます。JackalControl は、感染したデバイス（T1082）に関する情報を収集し、HTTP POST 要求（T1071.001）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するために使用されるボット ID を生成します。

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

RMS

RMS（Remote Manipulator System）は、RuRat および Gussdoor とも呼ばれ、Microsoft Windows および Android デバイスのリモート管理のために TektonIT によって開発された正規のツールです。このツールは、ペイロード配布の手段としてフィッシングメールを使用した TA505 やその他の攻撃者によって実行されたキャンペーンで確認されています（T1566.001）。RMS がインストールされると、攻撃者は、コマンドアンドコントロール（T1071.001）を介した機密データの漏洩や追加のマルウェアの展開などの悪意のあるアクティビティのために、侵害されたデバイスに対する不正なリモートアクセスと制御を取得します。

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

Satacom

LegionLoader とも呼ばれる Satacom は、主に暗号通貨を盗むように設計されたブラウザ拡張機能（T1176）を配布するマルウェアです。このマルウェアは、違法コピーされたソフトウェアを配布するサードパーティの Web サイトを介して拡散し、その後、Satacom インストーラを含む zip ファイルをホストしている Web サイトに攻撃対象をリダイレクトします。攻撃対象がリダイレクションリンク（T1204.001）にアクセスすると、悪意のあるファイル（T1204.002）がダウンロードされ、実行されます。このファイルによって、ビットコインウォレットに関連するデータが収集され、コマンドアンドコントロールチャネル（T1041）経由でデータが流出します。Satacom によって配信される悪意のあるブラウザ拡張機能は、Coinbase、Bybit、KuCoin、Huobi、および Binance のユーザーをターゲットにしていることが確認されています。2FA をバイパスして、攻撃対象のビットコインアドレスと通貨を盗むことができます。

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

UNC4841

UNC4841 は、スパイ活動を目的としたキャンペーンを実行している疑いがある攻撃者です。このグループは、南北アメリカ、ヨーロッパ、およびアジア太平洋地域の公共部門と民間部門のさまざまな組織を対象としています。UNC4841 は、ゼロデイ脆弱性をエクスプロイトすることが確認されています。UNC4841 によってエクスプロイトされる脆弱性の 1 つは、Barracudo Email Security Gateway（ESG）の CVE-2023-2868 です。このグループは、フィッシング電子メールの添付ファイルを使用してマルウェア（T1566.001）を配布し、Saltwater、Seaside、SeaSpy、SkipJack などのバックドアを含めて、さまざまなマルウェアファミリを展開できます。一部のマルウェアは、Barracuna ESG をエクスプロイトするように特別に設計されています。

お使いの環境でUNC4841アクティビティが検出されたかどうかを確認するには、[UNC4841アクティビティ脅威の詳細（UNC4841 Activity 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。