2023 年 7 月

2023 年 7 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。

- Aurora
- GCleaner
- Kelihos
- Mystic
- RedDriver

また、既存の脅威検出のインジケーターも更新しました。

Aurora

Aurora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）を標的とする情報窃取マルウェアです。2022年以降、ロシア語を話すハッキングフォーラムで人気を集めました。これは、検索エンジンの結果で、SEOに毒された、偽の、クラックされたソフトウェアを介して配信されます（T1189）。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。被害デバイスでの動作中に WMI（T1047）と PowerShell（T1059.001）を使用します。Golang で記述されています。

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

GCleaner

GCleaner（別名 G-Cleaner または Garbage Cleaner）は、Windows デバイスを高速化および最適化するための正規のツールとして宣伝されているアプリケーションです。ただし、GCleanerは悪意のある PPI（Pay-Per-Install）ローダーであり、Azorult、Stealc、Vidar などの他のマルウェアを配信できます。これは、アプリケーションや違法コピーされたソフトウェアを共有する Web サイト（T1189）を介して配布されます。GCleaner は、本物の最適化ツールを装ってシステムに侵入し（T1036）、悪意のあるペイロードを実行します。GCleanerは、地理位置情報ベースのコマンドアンドコントロールインフラストラクチャを利用します。つまり、ローダーと後続のマルウェアのダウンロード（T1105）の動作は、被害者の IP アドレスの場所に依存します。

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

Kelihos

Kelihos（別名 Hlux）は、スパム電子メールの配信、機密情報の窃取、分散型サービス妨害（DDoS）（T1498）の実行、ビットコインのマイニングなど、さまざまな悪意のあるアクティビティを実行するピアツーピアのボットネットです。Kelihos は、添付ファイル（T1566.001）またはペイロード（T1566.002）のインストールにつながるリンクを含む悪意のある電子メールキャンペーンを介して配布されます。また、ユーザーが侵害された Web サイトにアクセスしたときに、ドライブバイダウンロードを使用して配布することもできます（T1189）。システムが侵害されると、マルウェアはコマンドアンドコントロールサーバーに接続してコマンドを受信し、追加のコンポーネントをダウンロードします（T1105）。

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

Mystic

Mystic は、ローダー機能（T1105）も備えた情報窃取マルウェアです。2023 年 4 月からダークウェブでアドバタイズされており、システムホスト名、ユーザー名、GUID などの情報を収集します（T1082）。また、キーボードレイアウトを使用してユーザーの地理位置情報を特定することもできます。この窃取マルウェアは、さまざまな Web ブラウザ、ブラウザ拡張機能、暗号通貨アプリケーション、MFA およびパスワード管理プログラム、Steam および Telegram のログイン情報を標的としています。ブラウザ履歴、自動入力データ、ブックマーク、Cookie、およびその他の保存されたログイン情報をブラウザからキャプチャできます（T1555.003）。Mystic は、コマンドアンドコントロール通信（T1095）に TCP を介したカスタムバイナリプロトコルを使用し、感染したデバイスからデータを盗み出す（T1041）ために使用されます。Mystic は、感染したデバイスの情報をディスクに保存せずにその場で送信します。

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

RedDriver

RedDriverは、中国のユーザーを対象としたドライバベースのブラウザハイジャッカー（T1185）です。これは、一般的なエンドポイントアプリケーションを模倣した実行ファイルとして配布

されます（T1036）。これには2つのDLLが含まれており、後でブラウザセッションへのリフレクティブコードのロード（T1620）に使用されます。同じ実行ファイルは、悪意のあるドライバ（T1105）をダウンロードするためにも使用され、被害システムのリスニングポートを介してブラウザトラフィックをリダイレクトします（T1557）。HookSignTool を使用するため、Windows ドライバ署名ポリシーをバイパスできます。

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