2023 年 2 月

2023 年 2 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 （1 ページ）
- マニュアルのアップデート （2 ページ）

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。

- Agent Tesla
- BlackHat Ad
- LNKR
- Remcos

また、既存の脅威検出のインジケーターも更新しました。

Agent Tesla

Agent Tesla は .NET ベースのリモートアクセス型トロイの木馬であり、多くの場合、攻撃対象のネットワークに足掛かり（TA0001）を確立し、さらなる感染のために第 2 段階のペイロード（T1105）を展開するために使用されます。ドロッパーとして使用されるだけでなく、感染したデバイスから情報（T1005）を盗むこともできます。その後、すでに確立されている C2 チャネル（T1041）を介して盗んだデータを盗み出します。多くの場合、さまざまなテーマのフィッシングメール（T1566）を介して配布されます。

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

BlackHat Ad

Black Hat Ad キャンペーンは、Web サイトに感染してトラフィックのリダイレクトに使用し、ユーザーを侵害された Web サイトに誘導します（T1204.001）。リダイレクトには複数のレイ

ヤがあり、ユーザーを望ましくないサービスやアプリケーションに誘導する可能性があります。また、情報窃取プログラムなどのより重大なマルウェア（T1105）のインストールにつながる可能性もあります。侵害された Web サイトでは、シンプルスクリプトインジェクションと難読化スクリプトインジェクションの 2 種類の JavaScript インジェクション（T1059.007）が確認されています。

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

LNKR

LNKR（Linker）は、ユーザーのコンピュータに広告を表示するように設計されたアドウェアの一種です。通常、ユーザーの Web ブラウザ（T1185）をハイジャックし、ページがロードされている間に広告をページに挿入します。また、検索エンジンの結果を関連サイトにリダイレクトし、データを収集してサードパーティに送信することもできます。LNKR は漏洩（T1041）が可能で、悪意のあるブラウザ拡張機能（T1204.002）によって配布されます。

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

Remcos

Remcos は元々、Breaking Security によって、軽量、高速、高度にカスタマイズ可能なリモート管理ツールとして開発されました。その後、攻撃者によって改変され、リモートアクセス型トロイの木馬として使用されました。無料版とプロフェッショナル版の両方があり、スクリーンキャプチャ（T1113）、ファイル転送（T1105）、キーロガー（T1056.001）、カメラ/マイクの制御（T1125）などのさまざまな機能を備えています。さまざまなプロセス（T1055）に自身を挿入し、攻撃者が攻撃対象の環境へのアクセスを維持できるようにします。

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

マニュアルのアップデート

2021 年 6 月に REST API が新しく導入されたことに伴い、STIX/TAXII API はサポートされなくなったため、このユーザーガイドから STIX/TAXII サービスの章が削除されました。

- 新しい REST API にアクセスするには、https://api.cta.eu.amp.cisco.com [英語] を参照してください。
- 詳細については、「global threat alerts REST API is now released!」を参照してください。
- サポートが必要な場合は、cognitive-api-support@cisco.com までお問い合わせください。

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。