



2023 年 9 月

2023 年 9 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 \(1 ページ\)](#)

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。

- Andariel
- PurpleFox

また、既存の脅威検出のインジケータも更新しました。

Andariel

Andariel は、韓国の機関や企業を標的とした攻撃者です。これは、北朝鮮ベースの高度で永続的な脅威である Lazarus (G0032) と関係があることが知られています。Andariel は、(T1105) リモートアクセス型トロイの木馬、ローダー、リバースシェルなど、独自の手段を使用することが知られています。ツールを開発しながら、Go、Rust、.NET フレームワークを活用します (T1587.001)。スパイフィッシング (T1566.001)、ドライブバイダウンロード (T1189)、および一般向けアプリケーションのエクスプロイト (T1190) によって拡散します。

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

PurpleFox

PurpleFox は、自己拡散機能を備えたドロPPERマルウェアです。攻撃対象に感染した後、PurpleFox はこれを使用してインターネットをスキャンし、公開されている脆弱なサーバー (T1595.001) を探します。侵害されたデバイス (T1584.004) は、キルチェーンの初期ペイロードをホスト (T1105) するために使用されます。DLL と非表示のルートキット (T1014) を含む MSI ファイル (T1204.002) を活用することが確認されています。DLL の名前を正規のシス

テムリソースに変更し、svchostのネットワークサービスグループを介して実行されるようにします (T1543.003)。ホストのローカルファイアウォールポリシーを変更して (T1562.004)、同じデバイスの再感染を防ぎます。

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