2022 年 10 月

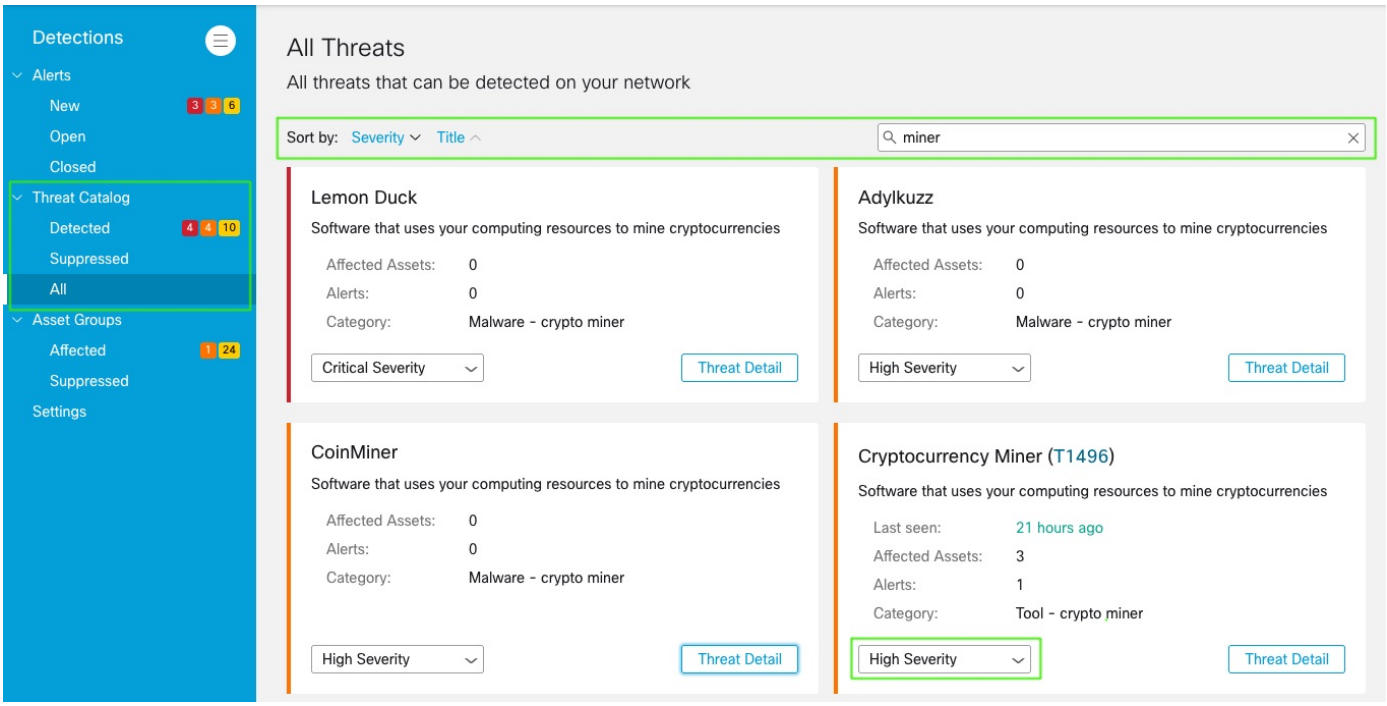
2022 年 10 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

脅威カタログ - すべて

グローバル脅威アラートダッシュボードには、新しいセクション [脅威カタログ（Threat Catalog）] > [すべて（All）] があります。

- 検出可能なすべての脅威を一覧表示します。
- 検索ボックスを使用してリスト（現在 300 を超えるアイテムが含まれています）をフィルタリングします。
- 検索を高速化または優先順位付けするには、リストを [重大度（Severity）] または [タイトル（Title）] で並べ替えます。
- 重大度のドロップダウンを使用して、脅威の重大度を調整し、アラートがトリガーされるたびにアラートの全体的なリスクスコアに影響を与えることができます。

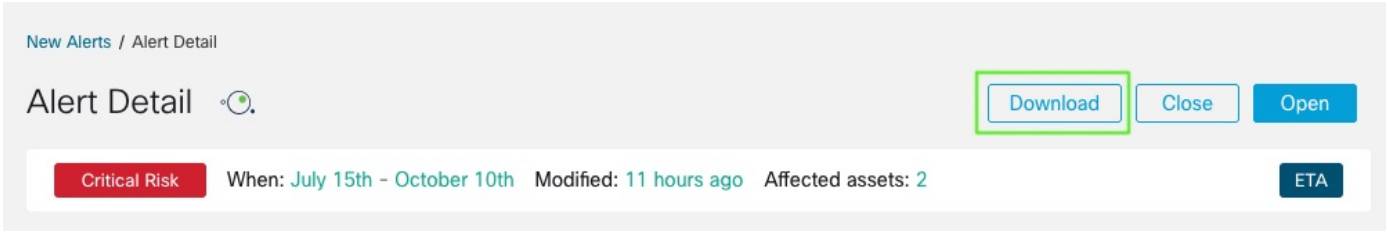
図 *1*:



アラート詳細のダウンロード

[アラート詳細（Alert Detail）] ビューで、すべてのアラートの詳細を CSV ファイルでコンピューターに [ダウンロード（Download）] できるようになりました。このオプションを使用すると、選択した表処理ツールですべてのアラートの詳細をすばやく表示できます。

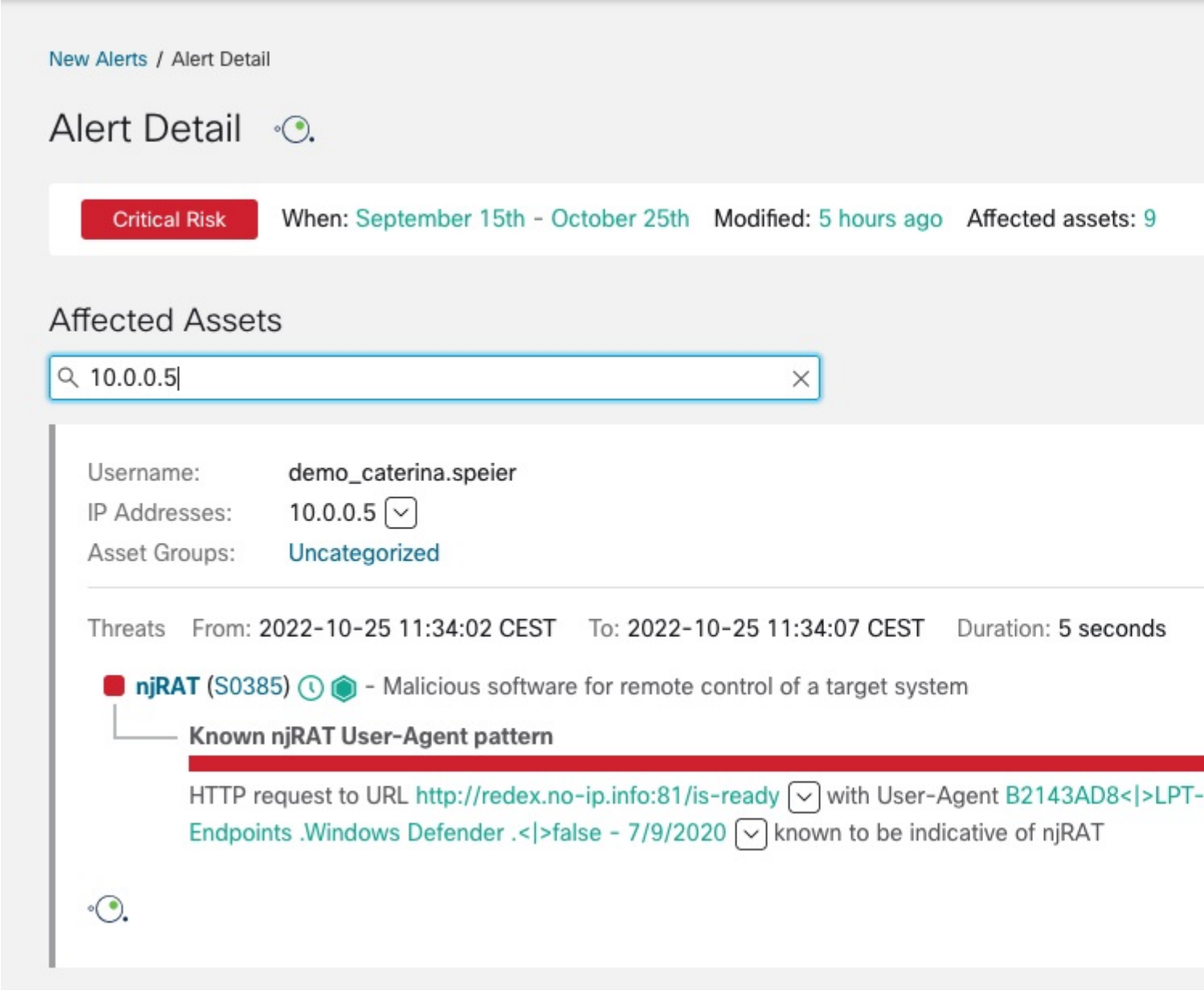
図 *2*:



アラート詳細で影響を受けるアセットのフィルタリング

[アラート詳細（Alert Detail）] ビューで、検索ボックスに IP アドレスまたはユーザー名を入力して、表示される [影響を受けるアセット（Affected Assets）] をフィルタリングできるようになりました。この機能は、選択した 1 つのアセットの詳細をすばやく見つけて集中することで、時間を節約するのに役立ちます。

図 *3 :*

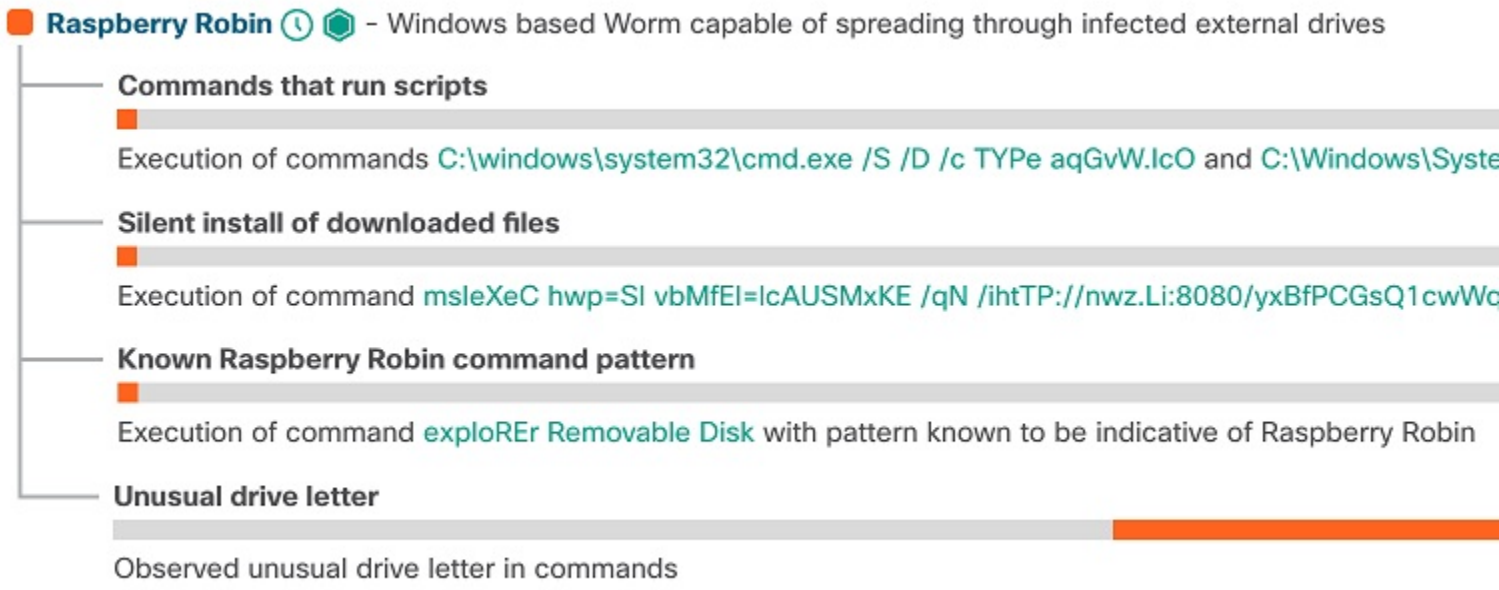


新たな検出

（注） 現在、これは Cisco Secure Endpoint ユーザーの早期アクセス機能としてのみ利用できます。オプトインしてこの検出を有効にするには、cognitive-feedback@cisco.com まで電子メールでお問い合わせください。

新しい検出パターンを追加するプロセスが簡素化されたおかげで、Raspberry Robin、Mozi、WPAD 攻撃などの脅威を検出するルールが追加されました。ルールでは、複数の TTP を 1 つの脅威に組み合わせることができます。

図 *4*:



さらに、検出された脅威のコンテキストを改善する新しい異常検出機能を追加しました。新しい異常検出機能は、DGA ファイル名、ブラウザに関連付けられていないユーザーエージェント、異常に長い URL などを持つファイルのダウンロードを識別できます。

可視性の拡張

グローバル脅威アラートエンジンによって提供されるコンテキスト情報を改善しました。訪問したドメインに基づいてオペレーティングシステム（OS）を検出する新しいアプローチを実装し、デバイス全体での OS 検出の範囲を改善しました。また、Android デバイスの検出機能も大幅に強化されました。 Android デバイスの数は約 3 倍に増加しました。

他のセキュリティ対策によってすでにブロックされている通信を検出して強調表示する方法を拡張しました。Cisco Secure Web Appliance（旧 Cisco Web セキュリティアプライアンス）プロキシによってエクスポートされる sc-filter-result フィールドのサポートを追加することで、検出を高度化しました。さらに、Cisco Secure Network Analytics（旧 Stealthwatch）フローでブロックされた通信のディテクタを展開しました。UI の特別なタグは、ブロックされた通信を強調表示します。

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。

- M0yv
- Metamorfo

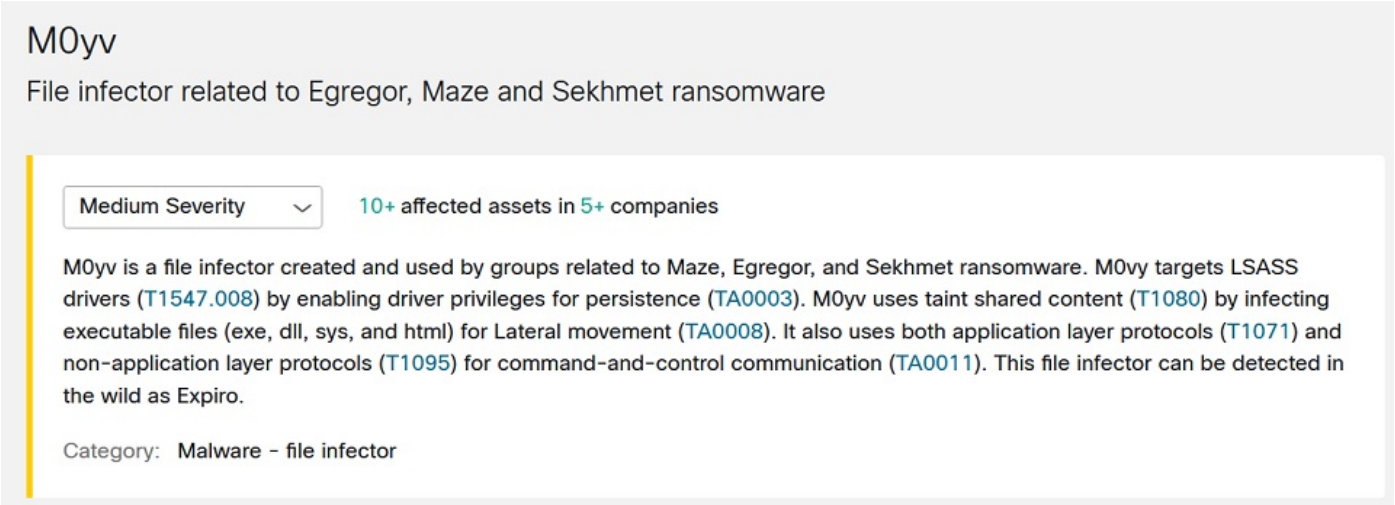
また、既存の脅威検出のインジケーターも更新しました。

M0yv

M0yv は、Maze、Egregor、および Sekhmet ランサムウェアに関連するグループによって作成および使用されるファイルインフェクタです。これは、永続化（TA0003）のドライバ権限を有効にすることにより、LSASS ドライバ（T1547.008）を標的にします。M0yv は、ラテラルムーブメント（TA0008）のために実行ファイル（.exe、.dll、.sys、および.html）を感染させることにより、汚染された共有コンテンツ（T1080）を使用します。また、コマンド アンド コントロール通信（TA0011）にアプリケーション層プロトコル（T1071）と非アプリケーション層プロトコル（T1095）の両方を使用します。このファイルインフェクタは、実際には Expiro として検出される可能性があります。

お使いの環境で M0yv が検出されたかどうかを確認するには、[M0yv 脅威の詳細（M0yv 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。

図 5 :

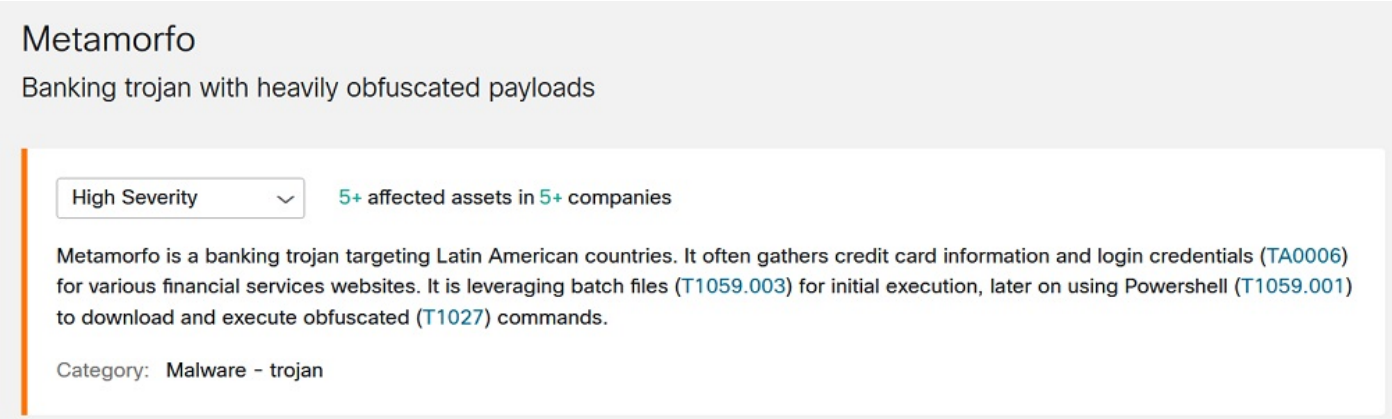


Metamorfo

Metamorfo は、中南米諸国を標的とするバンキング型トロイの木馬です。多くの場合、さまざまな金融サービス Web サイトのクレジットカード情報とログイン情報（TA0006）を収集します。初期実行にはバッチファイル（T1059.003）を利用し、難読化（T1027） コマンドをダウンロードして実行するには Powershell（T1059.001）を利用します。

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

図 *6*：



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。