2021 年 12 月

2021 年 12 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。

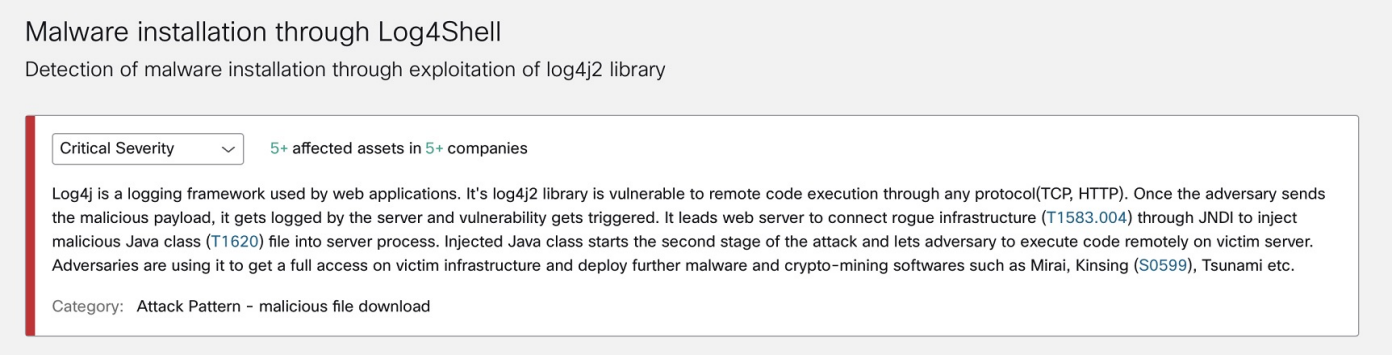
新しい Log4Shell 検出

最近発見された Log4j の脆弱性に関連する次の 2 種類の検出を含む、新しい脅威検出をポートフォリオに追加しました。

Log4Shell を介したマルウェアのインストール

これは、すでに成功している Log4j のエクスプロイトの検出です。Log4j は、Web アプリケーションで使用されるロギングフレームワークです。その log4j2 ライブラリは、任意のプロトコル（TCP、HTTP）を介したリモートコード実行（RCE）に対して脆弱です。攻撃者が悪意のあるペイロードを送信すると、サーバーによってログに記録され、脆弱性がトリガーされます。これにより、Web サーバーは JNDI を介して不正なインフラストラクチャ（T1583.004）に接続し、悪意のある Java クラス（T1620）ファイルをサーバープロセスに挿入します。挿入された Java クラスは、攻撃の第 2 段階を開始し、攻撃者が攻撃対象のサーバーでコードをリモートで実行できるようにします。攻撃者はこれを使用して、攻撃対象のインフラストラクチャへのフルアクセスを取得し、Mirai、Kinsing（S0599）、Tsunami などの追加のマルウェアや暗号通貨マイニングソフトウェアを導入します。

図 *1*:

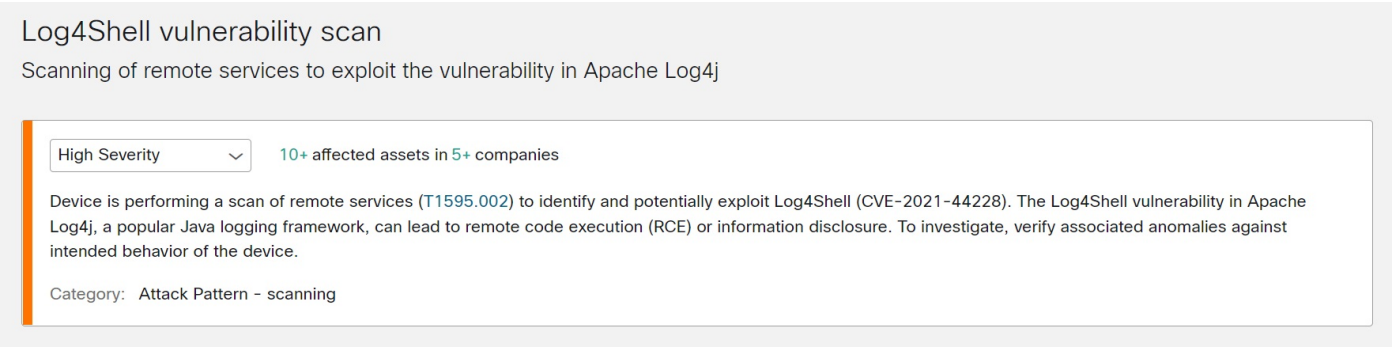


お使いの環境で [Log4Shell を介したマルウェアのインストール（Malware installation through Log4Shell）] が検出されたかどうかを確認するには、[Log4Shell を介したマルウェアのインストール（Malware installation through Log4Shell）] をクリックして、グローバル脅威アラートで詳細を表示します。

Log4Shell 脆弱性スキャン

これは、リモートサービス（T1595.002）のスキャンを実行して、Log4Shell（CVE-2021-44228）を特定して悪用する可能性があるデバイスの検出です。人気のある Java ロギングフレームワークである Apache Log4j の Log4Shell の脆弱性により、リモートコード実行（RCE）または情報の漏えいにつながる可能性があります。トリガーされたアラートは、スキャンを実行している望ましくないアプリケーションやマルウェアの存在、および侵入を意図したテストアクティビティを示している可能性があります。調査するには、デバイスの意図された動作に対して関連する異常を確認します。

図 *2*:



お使いの環境で [Log4Shell 脆弱性スキャン（Log4Shell vulnerability scan）] が検出されたかどうかを確認するには、[Log4Shell 脆弱性スキャン（Log4Shell vulnerability scan）] 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。

新しい SNI スプーフィングディテクタ

攻撃者はさまざまな手法を使用してネットワーク保護メカニズムを回避します。サーバー名識別（SNI）スプーフィングは、ドメインベースのネットワーク保護メカニズムを回避するために使用される一般的な手法です。この手法では、SNI フィールドで既知のドメイン名を使用し、その既知のドメインがホストされている IP アドレスとは異なるサーバー IP アドレスを使用します。既知の SNI と異なるサーバー IP アドレスの組み合わせにより、ドメインベースのセキュリティチェックに合格して、許可されていないサーバーに到達することができます。

図 *3 :*

新しい SNI スプーフィングディテクタは、SNI と IP アドレスの不一致がある場合に不整合を特定します。ディテクタは、暗号化トラフィック分析（ETA）を使用して SNI フィールドからドメインを抽出し、観測されたサーバーの IP アドレスを、ドメインが通常ホストされている IP アドレスのグローバル統計モデルと比較します。観測されたサーバーの IP アドレスがモデルと一致しない場合、SNI フィールドのドメインがスプーフィングされている可能性があり、ネットワークトラフィックが望ましくないサーバーにルーティングされています。不一致は、SNI 拡張子の一般的なホスト名が、実際に接続されている IP アドレスでホストされている可能性が低いことを示しています。

これは、[アラート（Alert）]>[アラート詳細（Alert detail）]>[セキュリティイベント（Security events）] で確認できます。

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。

- FluBot
- LokiBot
- Phorpiex
- Raccoon
- TrickBot

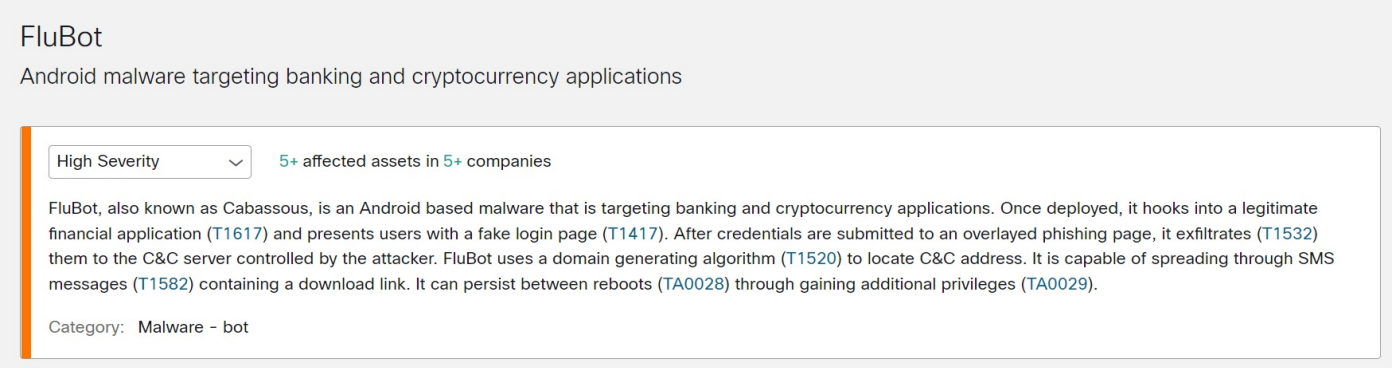
広告インジェクタ、暗号通貨マイナー、悪意のある広告、マルウェアの配布、スパムトラッキングなど、リスクの低い数多くの脅威検出も強化されています。

FluBot

FluBot（Cabassous とも呼ばれる）は、スペイン市場内でバンキングアプリケーションや暗号通貨アプリケーションを標的とする Android ベースのマルウェアです。正規の金融アプリケーション（T1617）にフックし、ユーザーに偽のログインページ（T1417）を提示します。ログイン情報がオーバーレイされたフィッシングページに送信されると、攻撃者が制御するコマンドアンドコントロール サーバーに流出（T1532）します。FluBot は、ドメイン生成アルゴリズム（T1520）を使用してコマンドアンドコントロール アドレスを見つけます。ダウンロードリンクを含む SMS メッセージ（T1582）を介して拡散することができ、追加の権限（TA0029）を取得することにより、再起動（TA0028）後も持続できます。

お使いの環境で FluBot が検出されたかどうかを確認するには、[FluBot脅威の詳細（FluBot 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 *4*:

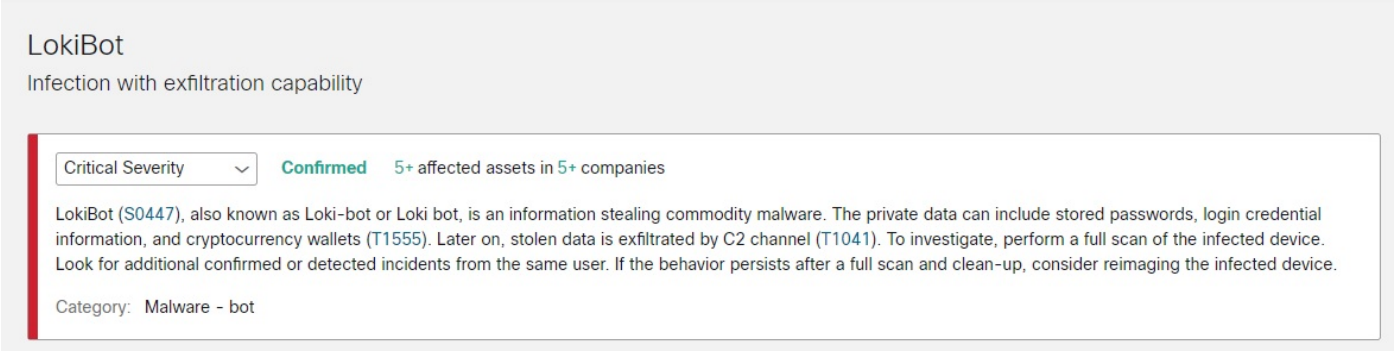


LokiBot

LokiBot（S0447）は、Loki-bot または Loki bot とも呼ばれ、情報を盗むコモディティマルウェアです。盗む個人データには、保存されているパスワード、ログイン情報、暗号通貨ウォレット（T1555）が含まれます。その後、盗まれたデータは C2 チャネル（T1041）によって流出します。調査するには、感染したデバイスのフルスキャンを実行します。同じユーザーからの追加の確認済みまたは検出されたインシデントを探します。フルスキャンとクリーンアップ後も動作が続く場合は、感染したデバイスのイメージを再作成することを検討してください。

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

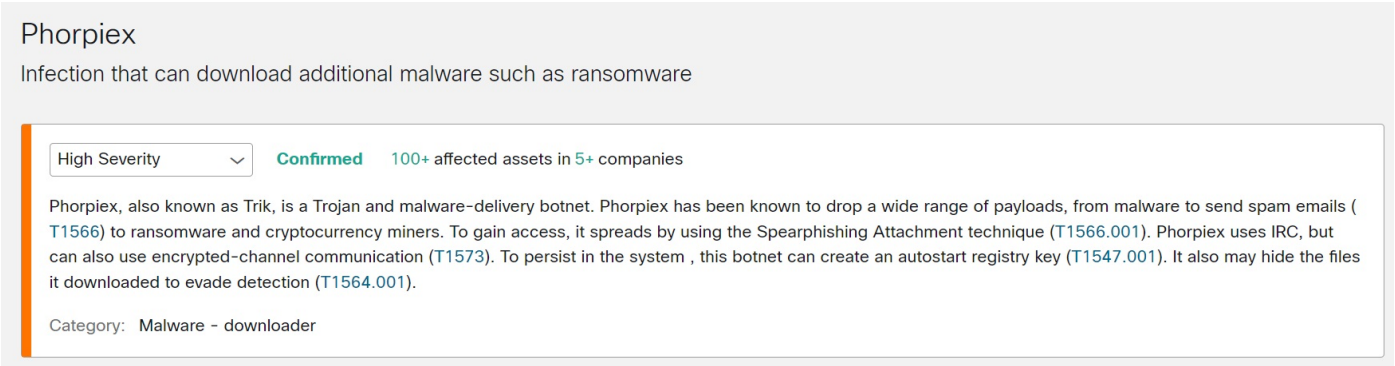


Phorpiex

Phorpiex は、オペレーティングシステムに感染して追加のマルウェアを配布するトロイの木馬とワームです。Phorpiex は、ランサムウェア、暗号通貨マイナー、スパムメール（T1566）を送信するマルウェアなど、さまざまなペイロードをドロップすることが知られています。アクセスするため、添付ファイルによるスピアフィッシング攻撃（T1566.001）を使用して拡散します。Phorpiex は IRC を使用しますが、暗号化チャネル通信（T1573）も使用できます。このボットネットはシステム内で存続するために、自動起動用レジストリキー（T1547.001）を作成します。また、検出（T1564.001）を回避するためにダウンロードしたファイルを非表示にすることもあります。

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



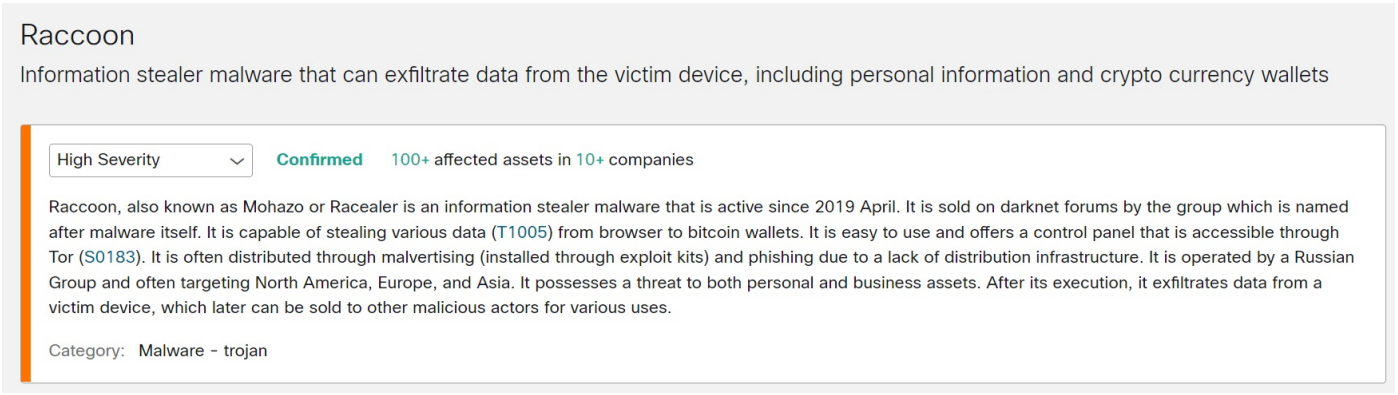
Raccoon

Raccoon（Mohazo または Racealer とも呼ばれる）は、2019 年 4 月から出回っている情報窃取マルウェアです。ブラウザからビットコインウォレットにデータ（T1005）を盗むことができ、個人資産とビジネス資産の両方に対する脅威です。Raccoon は、攻撃対象のデバイスからデータを盗み出します。このデータは、後でさまざまな用途のために他の悪意のある攻撃者に販売される可能性があります。

Raccoon は、このマルウェア自体から名を取っているグループによってダークネットフォーラムで販売され、北米、ヨーロッパ、およびアジアをターゲットとするロシアのグループによって運営されています。Tor（S0183）を介してアクセス可能なコントロールパネルで簡単に使用できます。Raccoon は、配布インフラストラクチャが不足していることから、マルバタイジング（エクスプロイトキットを介してインストールされる）やフィッシングによって配布されることがよくあります。

お使いの環境で Raccoon が検出されたかどうかを確認するには、[Raccoon脅威の詳細（Raccoon 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 7：

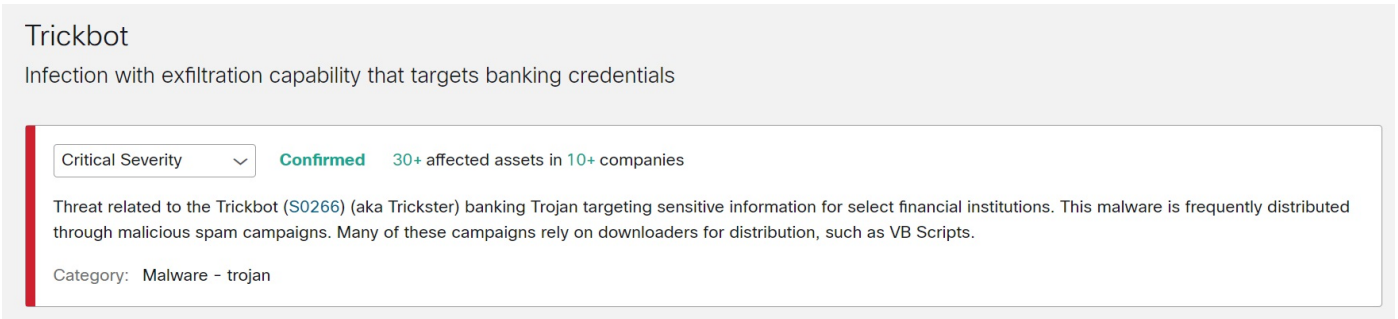


TrickBot

TrickBot（S0266）は Trickster とも呼ばれ、特定の金融機関の機密情報を標的とするバンキング型トロイの木馬です。このマルウェアは、悪意のあるスパムキャンペーンを通じて頻繁に配布されます。これらのキャンペーンの多くは、VB スクリプトなど、配布のためにダウンローダーを利用しています。

お使いの環境で TrickBot が検出されたかどうかを確認するには、[TrickBot脅威の詳細（TrickBot 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 8：



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。