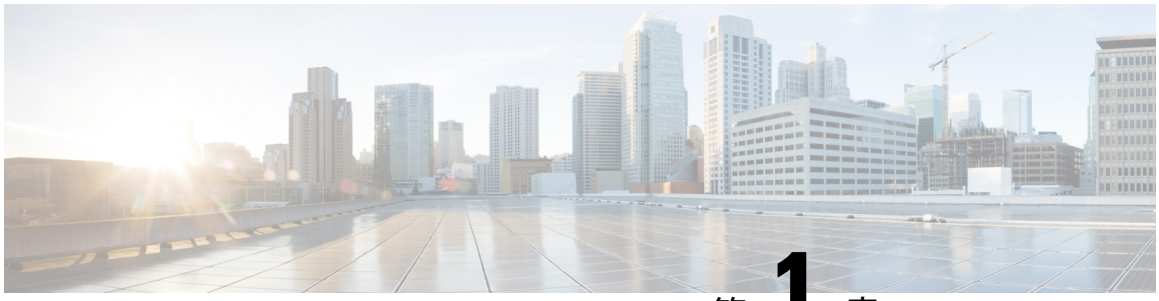
Secure Endpoint のグローバル脅威アラート

初版：2021 年 7 月 1 日

最終更新：2024 年 2 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

ダッシュボード

グローバル脅威アラート（以前はCognitive Intelligence）機能は、すでに進行中しているか、お客様のネットワーク内でプレゼンスを確立しようとしている高度で密かな攻撃を迅速に検出して対応するのに役立ちます。この機能は、不審なWebベースのトラフィックや悪意のあるトラフィックを自動的に調査します。確認済みの脅威と潜在的な脅威の両方を特定することで、感染を迅速に修復し、攻撃の範囲と損害を軽減できます。これは、既知の脅威キャンペーンが複数の組織に拡散している場合でも、これまでに見たことのない固有の脅威である場合でも同様です。

クラウドベースのサービスであるグローバル脅威アラートは、ハードウェアやソフトウェアを追加せずに、既存のWebセキュリティソリューションによって生成された情報を分析します。セキュリティ制御をバイパスした悪意のあるアクティビティに焦点を定めます。

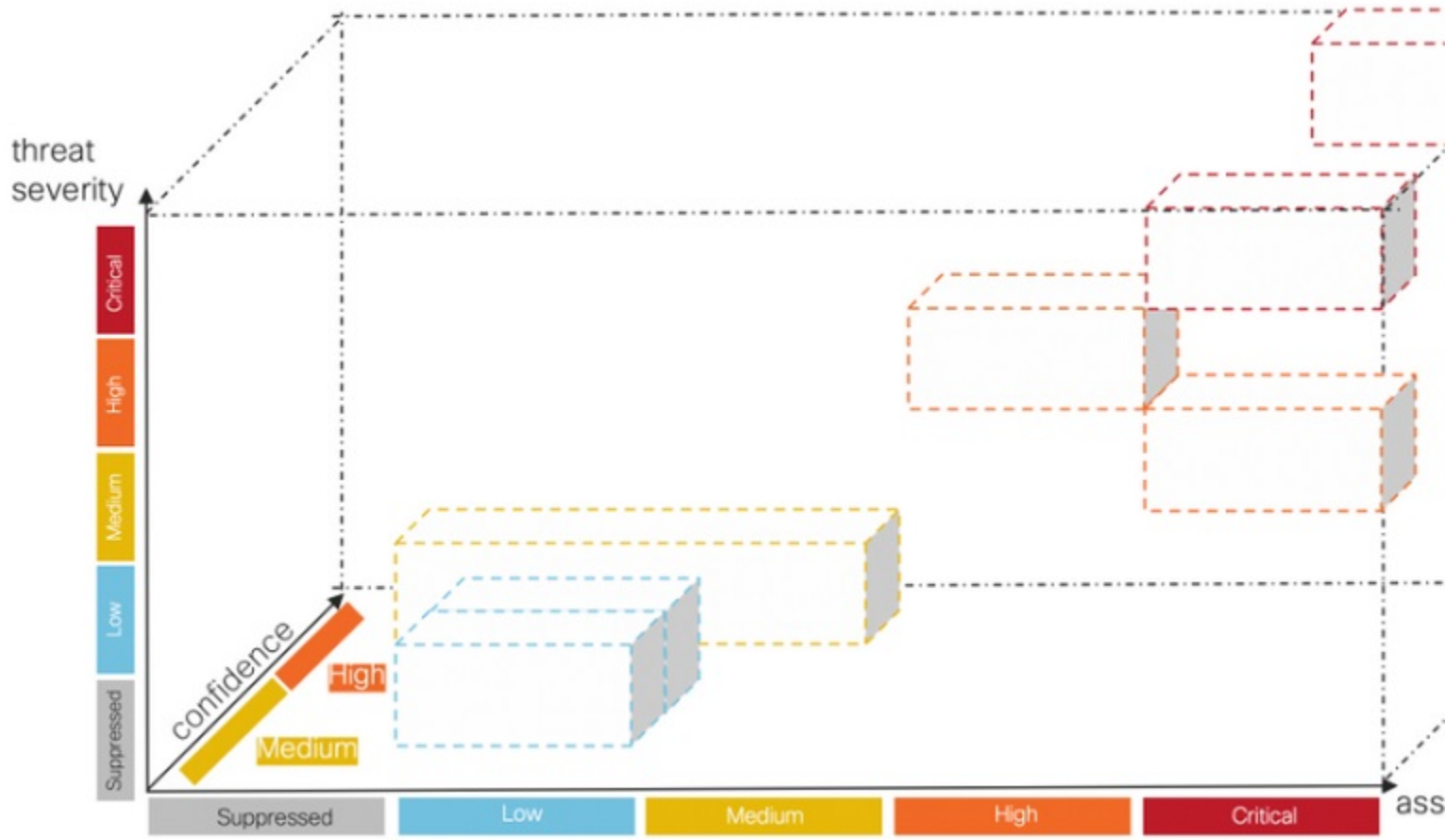
グローバル脅威アラートは、機械学習とネットワークの統計モデリングを使用して、通常のアクティビティのベースラインを作成し、ネットワーク内で発生する異常なトラフィックを特定します。デバイスのふるまいとWebトラフィックを分析して、コマンドアンドコントロール通信とデータ漏洩を特定します。

グローバル脅威アラートは、認識している情報から学習することで、継続的な侵害の特定を可能にし、繰り返し攻撃や継続的な感染のリスクを軽減します。複数のシスコセキュリティ製品と統合された直感的なWebベースのポータルを通じて情報を表示します。これにより、侵入の重大度と範囲を評価し、脅威のミッションとその仕組みを理解し、即座にアクションを実行できます。

概要

シスコの分析エンジンは、入力データストリームに機械学習を適用し、検出結果を3次元空間に投影します。

図 *1*:



- **脅威の重大度の次元。**脅威がどのぐらい深刻であるか。確認された脅威とその重大度。個々の脅威タイプに対する組織のリスクプロファイルとの整合性を高めるために、個々の脅威の事前定義された重大度を調整するオプションがあります。
- **アセット価値の次元。**アセットがどのぐらい貴重であるか。ネットワークに接続されているすべてのデバイスの重要度が等しくない場合は、個々のアセットグループのビジネス上の価値を調整して、より重要なデバイスの検出を優先させるオプションがあります。
- **信頼度の次元。**判定はどのぐらい信頼できるか。お客様の環境で観察された個々の脅威について、シスコのアルゴリズムが下している判定の信頼度。判定がほぼ確実となる十分な侵入兆候を観察できる場合もあります。その他の場合には、同様の症状にもかかわらず、実際の証拠が不完全なこともあります。そのため、許容誤差が大きくなります。

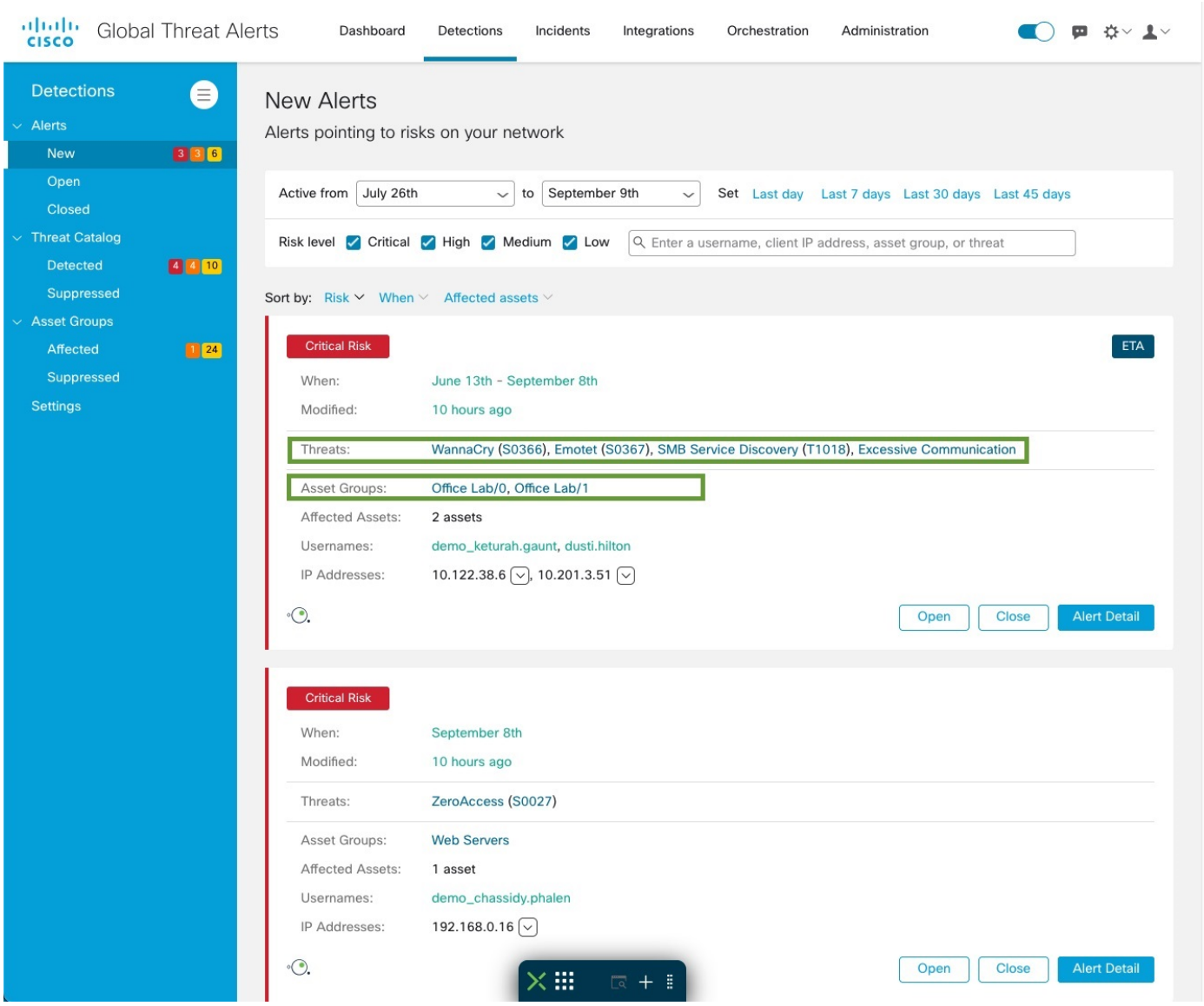
シスコのフュージョンアルゴリズムは、これらの検出結果を使用して同様の脅威とプロジェクションのクラスタを特定し、リスクレベルを計算します。シスコの Web ポータルでは、リスクレベルによって優先順位付けされたリストで、これらをセキュリティアラートとして表示します。各アラートは、ネットワーク上の脅威を指し、調査とその後の修復のための通常の作業単位を表します。

アラートの調査

ステップ 1 左側のナビゲーションメニューで [アラート（Alerts）] と [新規（New）] をクリックして、ネットワーク上のすべての新しいアラートを表示します。各アラートは、専用のカードに表示されます。

a) 各アラートカードには、同様のビジネス上の価値を持つネットワーク上の一連のアセットに同時に影響を与える 1 つ以上の脅威が集約されています。

図 *2*:



- **脅威**。同時に発生するさまざまな脅威。

- **アセットグループ**。これらの脅威は、同様のビジネス上の価値を持つアセットグループに属するエンドポイントで発生しています。

b) リスクレベルは、脅威の重大度レベルとアセットグループのビジネス上の価値に基づいています。リスクレベルが高いほど、脅威がネットワーク上の貴重なアセットに深刻な影響を与えるリスクがより高いことを示しています。

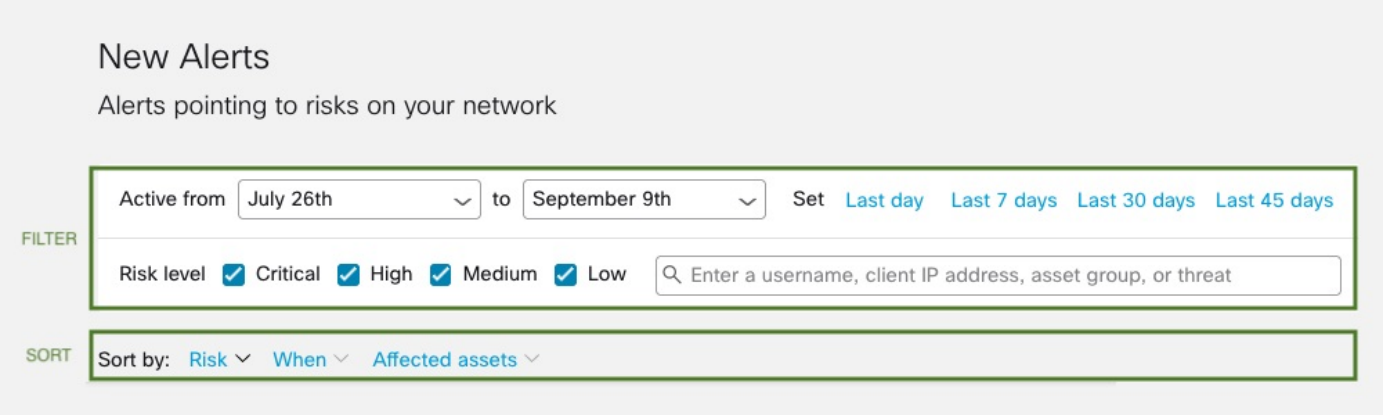
ステップ 2 アラートは、リスクの高い順に、リストの先頭から並べられます。リスクレベルに基づいてアラートに応答し、リスクの高いアラートを最初に調査することで、分析を優先順位付けします。

- 重大
- 高い
- 中規模
- 低い

（注） アラートカードは、新しい脅威がグループに追加されたときや、アセットグループのビジネス上の価値や脅威の重大度が変化したときなどに、動的に変更されます。

ステップ 3 経過時間、リスクレベル、ユーザー名、IPアドレス、アセットグループ、および/または脅威を選択して、表示するアラートをフィルタ処理するオプションがあります。また、リスクレベル、経過時間、または影響を受けるアセットの数でソートするオプションもあります。

図 *3:*

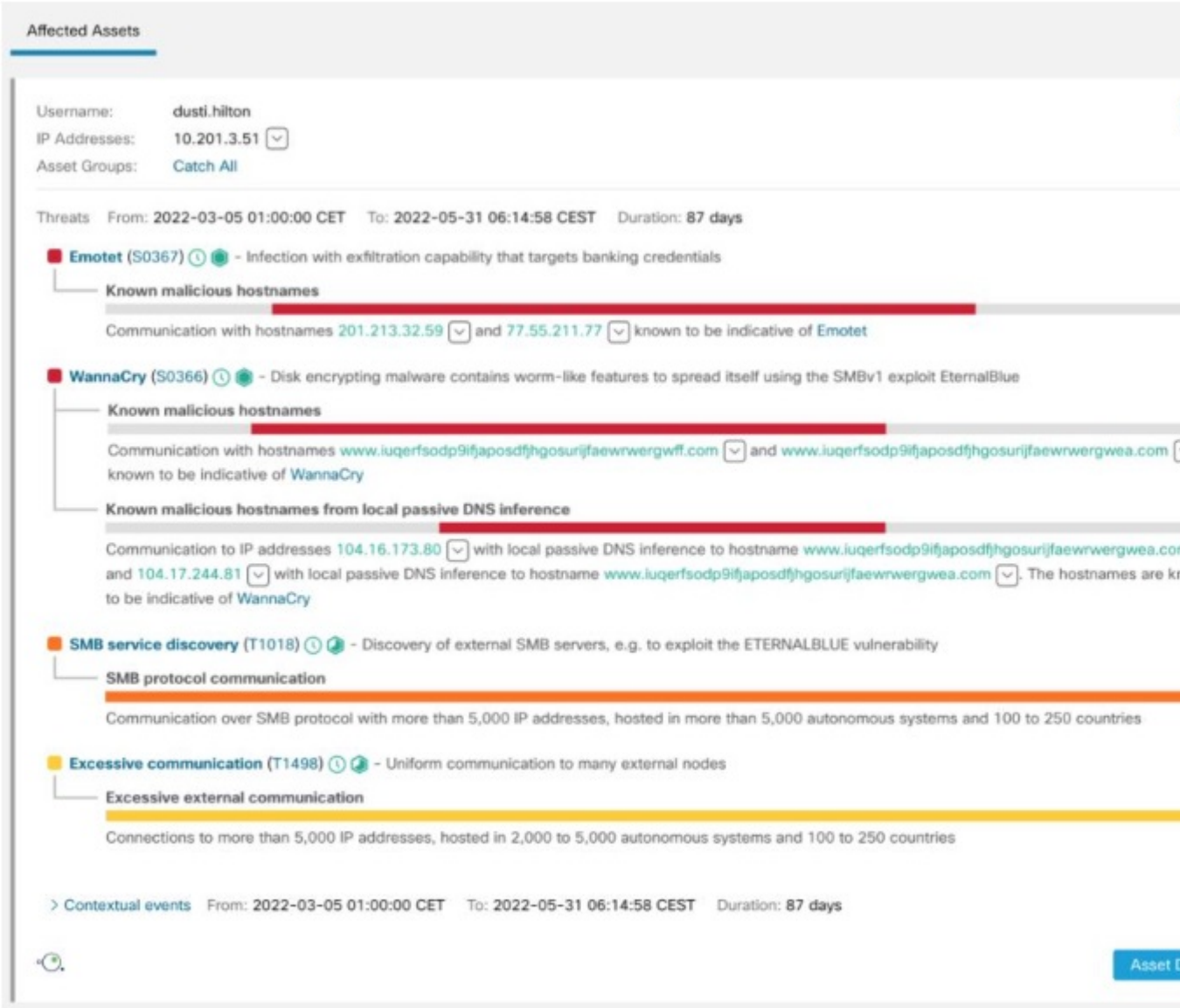


ステップ 4 アラートの状態を [オープン（Open）] に変更して、アラートの調査を開始します。

（注） 状態が [新規（New）] でなくなると、アラートカードは変更されず安定するため、調査が容易になります。

ステップ 5 [アラートの詳細（Alert Detail）] をクリックすると、検出された各脅威と影響を受けるアセットに関する追加のコンテンツが表示されます。影響を受けるアセットにはそれぞれそのアセットで行われたすべての脅威検出をリストする [脅威（Threats）] セクションがあり、すべての有害となるセキュリティイベントが含まれています。

図 *4 :*



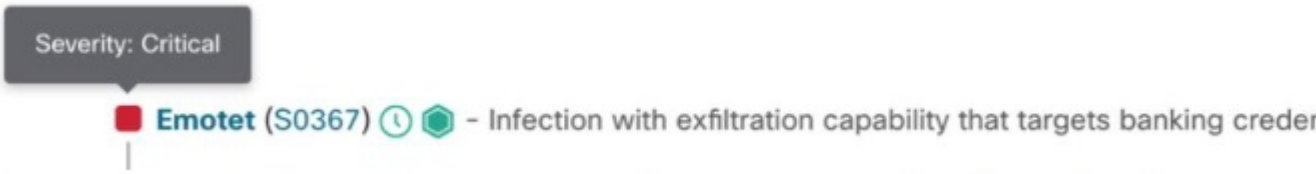
[脅威（Threats）] セクションの上部には、検出されたすべての脅威の合計観測期間と、特定のアセットでのそれらの有害となるセキュリティイベントが表示されます。

図 *5 :*

それぞれの脅威検出には、その名前、MITRE リンク、説明、および以下のものが表示されます。

- 重大度

図 *6 :*



- 観測期間

図 *7 :*

- 信頼度

図 *8 :*

それぞれの脅威検出は、下にあるセキュリティイベントによって裏付けられています。イベントの多くには、イベントの作成につながった証拠を提供する豊富なセキュリティアノテーションが含まれています。

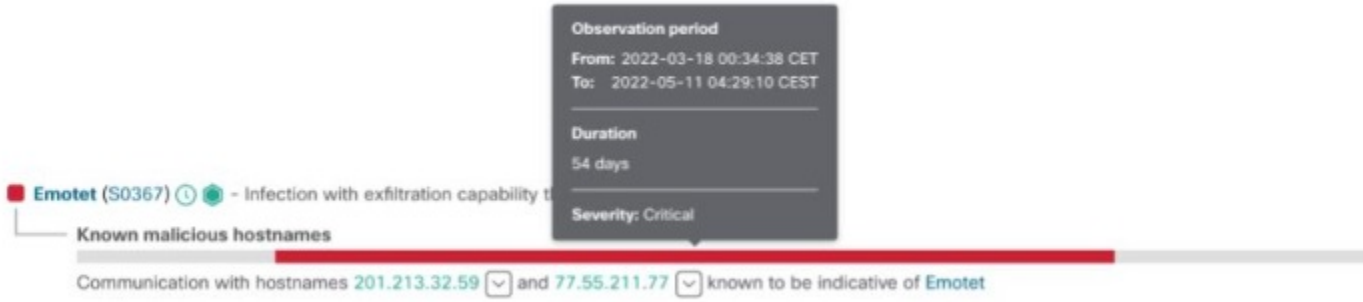
図 *9* :

イベントアノテーションには、他のシスコのセキュリティ製品にピボットして、監視対象に関する追加情報とインテリジェンスを取り込めるドロップダウンメニューが含まれている場合もあります。

図 *10* :

それぞれのセキュリティイベントには、[脅威（Threats）] の合計観測期間のコンテキスト内での動作のタイミングと発生を示すタイムラインが含まれています。

図 *11* :

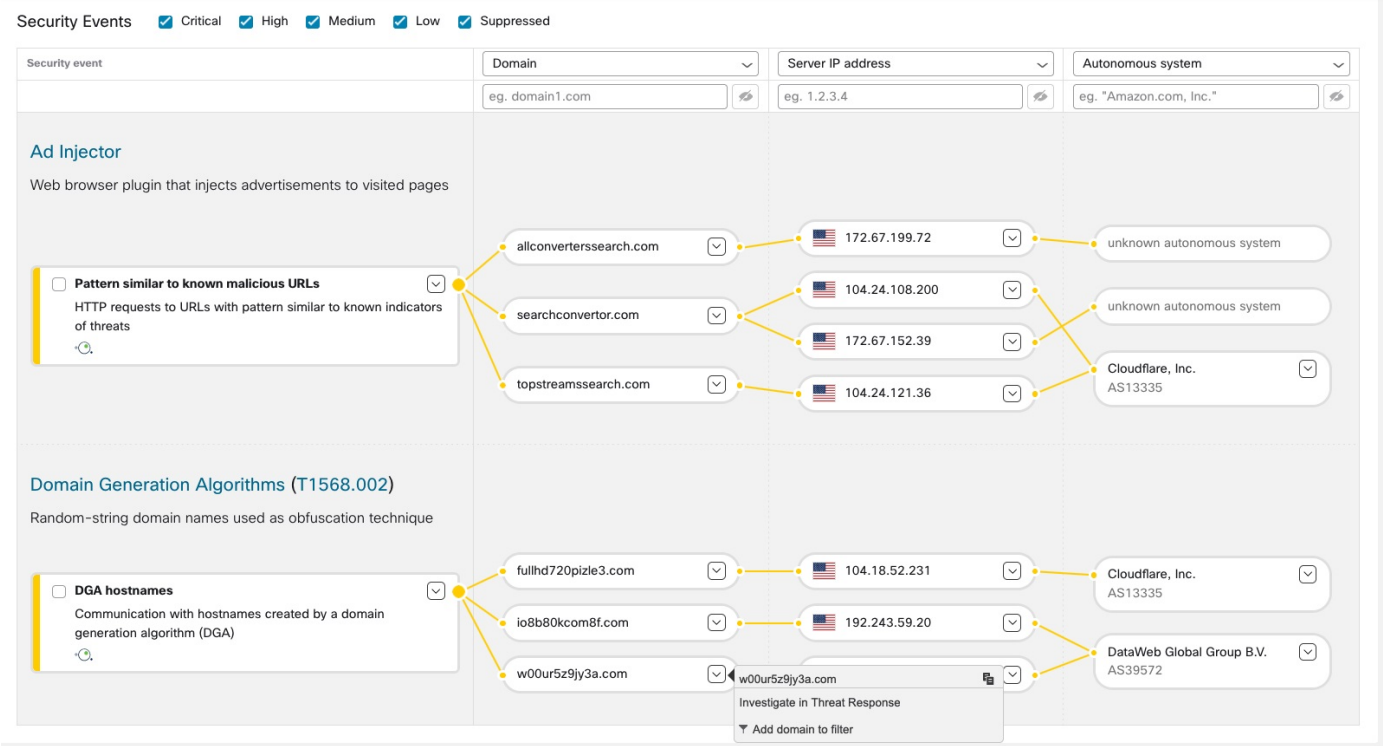


[コンテキストイベント（Contextual events）] セクションを展開して、アセット上で起こったことに関する追加のコンテキストを提供できる、より多くのイベントを表示することができます。

図 *12* :

ステップ 6 1 人のユーザーの特定のイベントの 1 つを選択すると、[セキュリティイベント（Security Events）] ビューに移動し、悪意のある検出をトリガーした特定のイベントの詳細なコンテキストを確認できます。

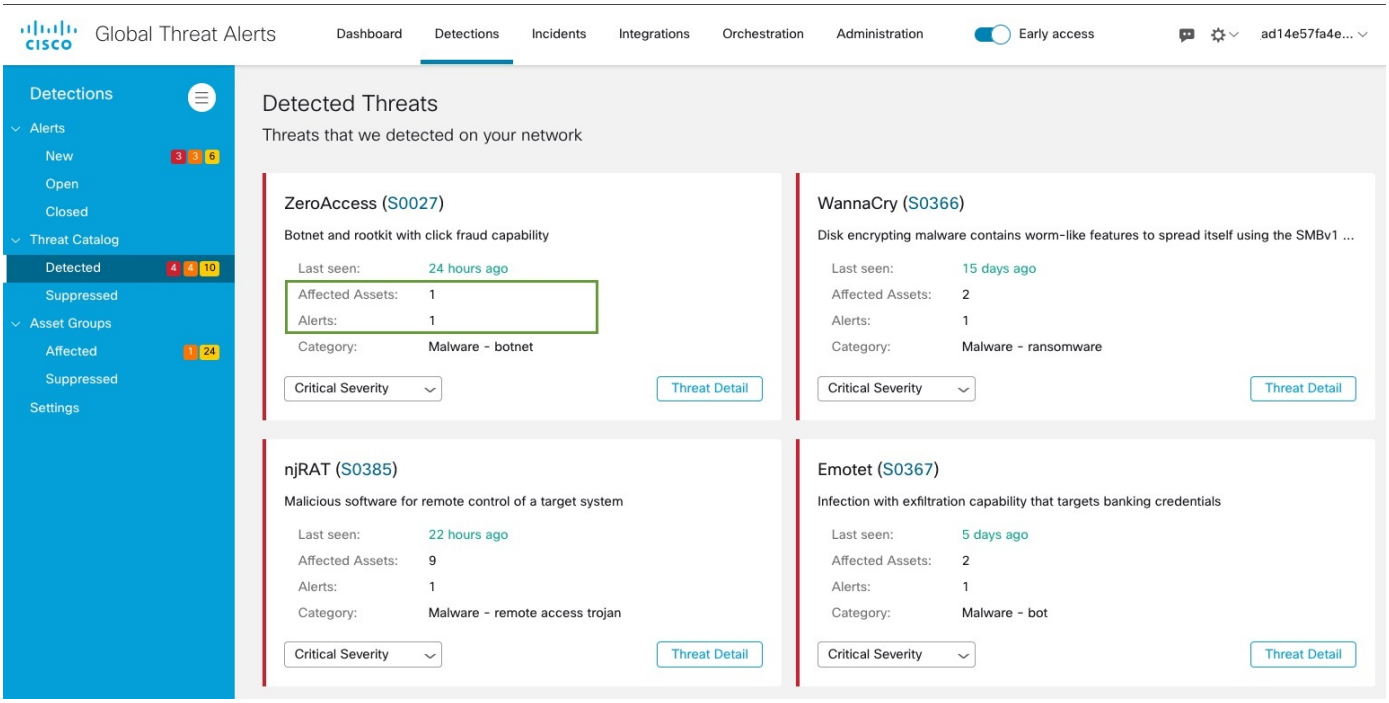
図 *13 :*



脅威の調査

ステップ 1 ネットワークで報告され、重大度で優先順位付けされた脅威のリストを表示するには、左側のナビゲーションメニューで[脅威カタログ（Threat Catalog）]および[検出（Detected）]をクリックします。各カードは、アラートにグループ化されるさまざまな脅威を表します。

図 *14 :*



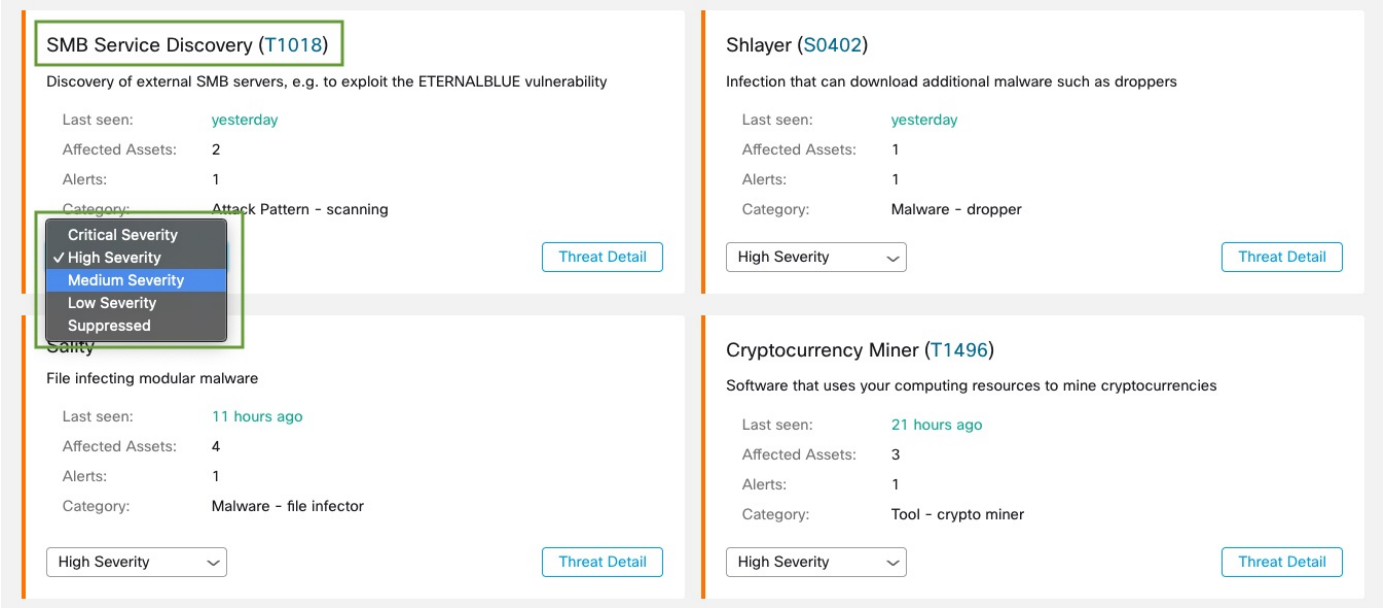
ステップ 2 特定のタイプの脅威が複数のアラートに関係している場合があります。この特定のタイプの脅威が関係するアラートの数と、この脅威の影響を受けるアセットの数を示すカウンタがカードにあります。

ステップ 3 グローバル脅威アラートの脅威インテリジェンスは、関連する ATT&CK の戦術、テクニック、およびソフトウェアエントリへの参照を提供します。

ステップ 4 ネットワーク固有の条件やビジネスニーズに応じて、脅威の重大度を調整するオプションがあります。

- その結果、このタイプの脅威を含むすべての [新規（New）] アラートのリスクレベルが再計算され、新しい重大度にアセットの価値と信頼度レベルが重み付けされます。
- その後、リスクレベルの変更は、 [新規（New）] アラートの相対的な順序に影響します。
- たとえば、脅威の重大度を下げると、関連付けられたアラートのリスクレベルが低下し、関連付けられたアラート カードが [アラート（Alerts）] タブのリストの下位に表示されます。
- ドロップダウンリストをクリックして、脅威の重大度を調整できます。

図 *15 :*



（注） [新規（New）] 状態ではなくなった他のすべてのアラートは、脅威の重大度の変更による影響を受けません。調査を容易にするために変更されず安定したままになります。

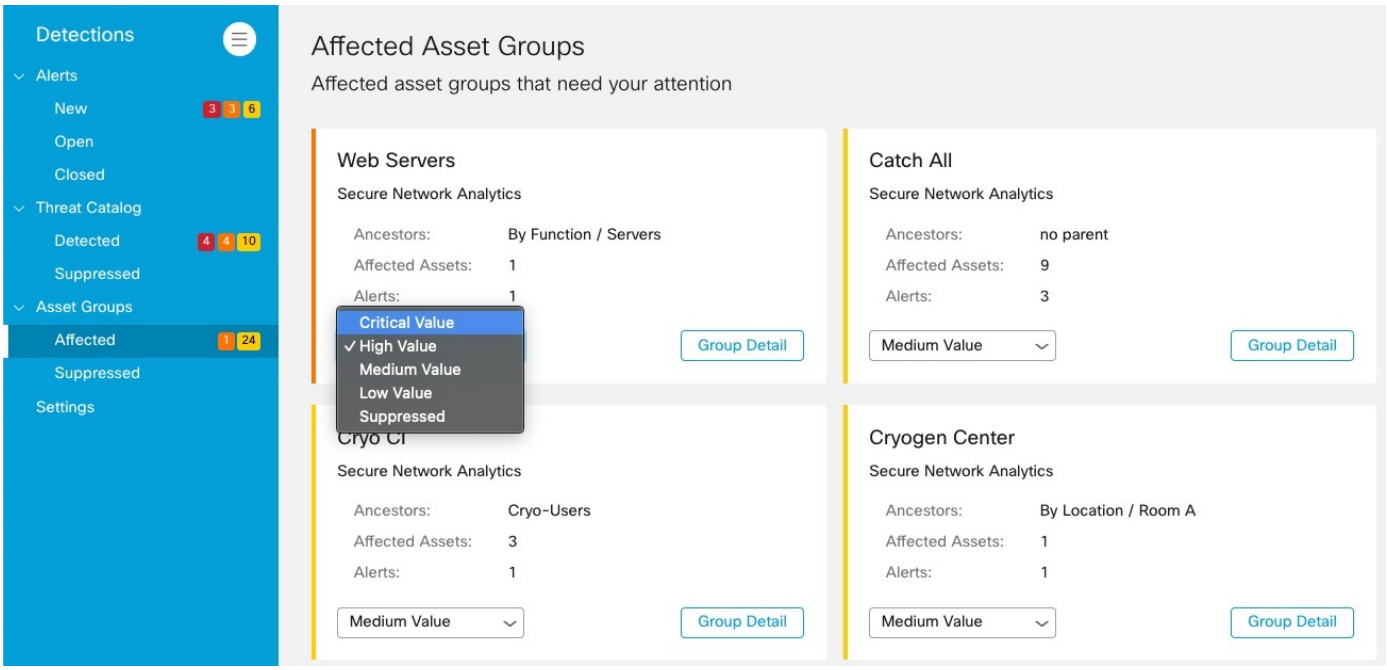
アセットグループ

ステップ 1 グローバル脅威アラートにトラフィックが送信されたすべてのアセットグループを表示するには、左側のナビゲーションメニューで [アセットグループ（Asset Groups）] および [アセット（Assets）] をクリックします。各カードは、グローバル脅威アラートが少なくとも 1 つのアラートを報告しているアセットグループを表します。

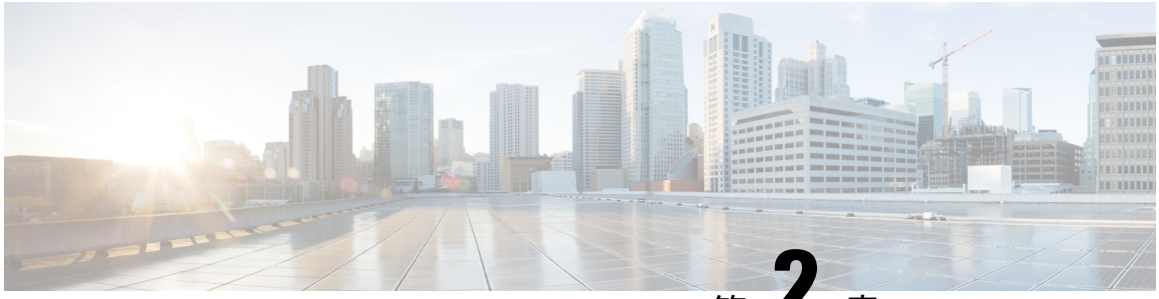
ステップ 2 アセットグループが組織にとってどのぐらい重要または価値があるかを判断します。アセットグループのビジネス上の価値を調整するオプションがあります。

- その結果、このアセットグループに影響するすべての [新規（New）] アラートのリスクレベルが再計算され、新しいアセットの価値に重大度と信頼度レベルが重み付けされます。
- その後、リスクレベルの変更は、 [新規（New）] アラートの相対的な順序に影響します。
- たとえば、アセットグループのビジネス上の価値を高めると、関連付けられたアラートのリスクレベルが高くなり、関連付けられたアラートカードが [アラート（Alerts）] タブのリストの上位に表示されます。
- ドロップダウンリストをクリックして、アセットグループのビジネス上の価値を調整します。

図 *16 :*



（注） [新規（New）] 状態ではなくなった他のすべてのアラートは、脅威の重大度の変更による影響を受けません。調査を容易にするために変更されず安定したままになります。



第 2 章

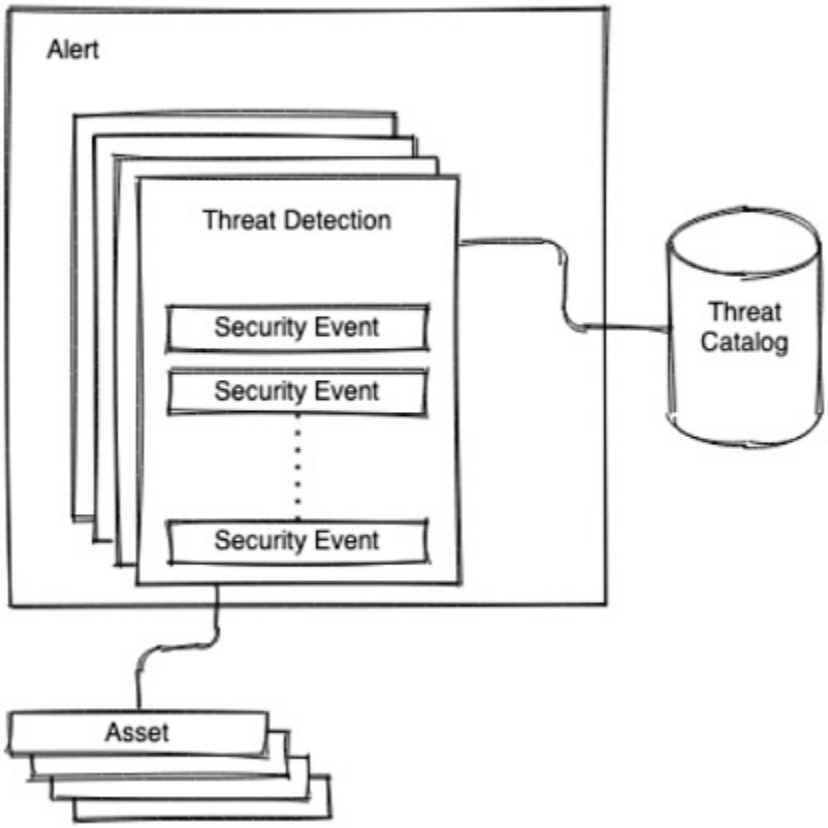
用語集

アラート

アラートとは、脅威の検出を調査するようにユーザに促す通知です。

グローバル脅威アラートでは、アラートは1つ以上の脅威の検出に焦点を当てます。これらの脅威の検出は、1 つ以上のアセットで発生します。シスコのフュージョンアルゴリズムは、これらの検出結果を使用して同様の脅威とプロジェクションのクラスタを特定し、リスクレベルを計算します。シスコの Web ポータルでは、リスクレベルによって優先順位付けされたリストで、これらをセキュリティアラートとして表示します。各アラートは、ネットワーク上の脅威を指し、調査とその後の修復のための通常の作業単位を表します。

図 *17*:



セキュリティ イベント

セキュリティイベントとは、悪意のある動作または疑わしい動作を示す可能性がある重要なセキュリティイベントです。脅威検出エンジンがセキュリティイベントを処理します。疑わしい動作や悪意のある動作の検出に大きな影響を与えるセキュリティイベントは、有害と呼ばれます。脅威の検出時に影響を受けるアセットで観察されるセキュリティイベントは、コンテキストと呼ばれます。各セキュリティイベントには、その重要性を示す説明が含まれています。この説明はセキュリティアノテーションと呼ばれます。

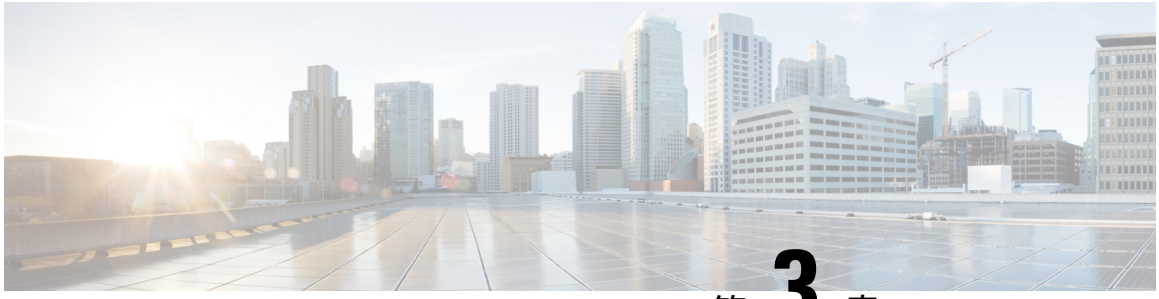
脅威カタログ

脅威カタログは、検出された脅威の可能性を整理し、マルウェア、ツール、攻撃パターンの 3 つの基本カテゴリに分類します。これには MITRE へのマッピング（存在する場合）も含まれます。

脅威の検出

脅威の検出とは、アセットに影響を与える疑わしい動作や悪意のある動作を検出することです。グローバル脅威アラートの脅威カタログでは、複数のタイプの脅威の検出を認識します。

脅威検出エンジンは、セキュリティイベントなどのさまざまなソースと連携します。これらを関連付けて、特定の信頼レベルで脅威の存在を明らかにする、または分析によって脅威の存在が確認される、異常なパターンや傾向を明らかにします。



第 3 章

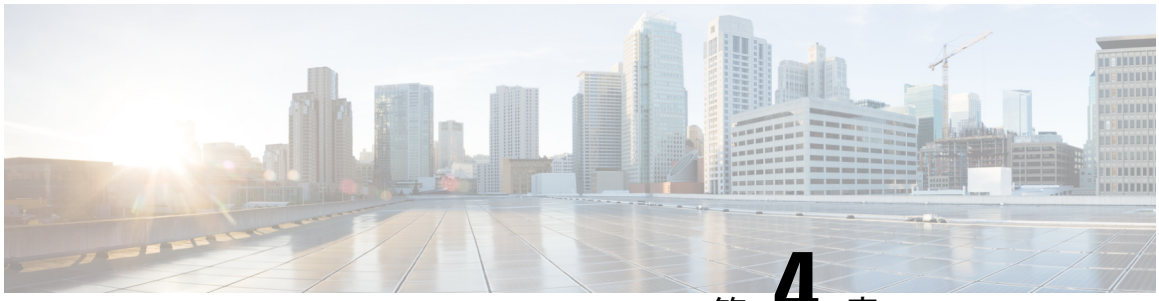
設定

設定

アプリケーションを設定するには、ナビゲーションメニューの [設定（Settings）] をクリックします。

- [Cisco SecureXの統合（Cisco SecureX Integration）]：SecureX アカウントのリージョンを選択し、[承認（Authorize）] をクリックして、SecureXアカウントにサインインすることで、SecureX との統合を有効にします。
- [デバイスアカウント（Device Accounts）] - 1 つ以上のソースプロキシデバイスから分析用グローバル脅威アラートシステムにログファイルのテレメトリデータをアップロードします。このサービスにアクセスするには、外部テレメトリ機能を有効にして、企業用にプロビジョニングする必要があります。外部テレメトリ機能がない場合は、Cisco Security アカウントチームにお問い合わせください。「プロキシデバイスのアップロード」を参照してください。
- [抑制されたネットワーク（Ignored Networks）]：無視する IPv4 アドレスとネットワーク範囲をリストしてアラートを非表示にします。これは、ゲストネットワークやその他の重要度の低いネットワークからのアラートなど、不要なアラートをフィルタ処理し抑制する場合に役立ちます。インシデントのリストから非表示にするホストの IPv4 アドレス、サブネット、または IPv4 アドレス範囲（例：10.100.10.1、10.100.10.0/24、10.100.10.1-10.100.10.254）を入力します。
- [Global Threat Alerts API] - REST API を使用して、さらなる分析、インシデント対応、およびデータアーカイブのために、グローバル脅威アラートで検出されたインシデントに関する情報を SIEM クライアントまでプルします。
- [電子メール通知（Email Notifications）] - 新規および更新された脅威のサマリーを送信する電子メール アドレスを 24 時間ごとに入力します。
- [リリースノート（Release Notes）]：機能の更新、変更、および修正の概要を示します（このガイドで後述）。

設定



第 4 章

プロキシデバイスのアップロード

プロキシデバイスのアップロード

Cisco Secure Web Appliance（旧 Cisco Web セキュリティアプライアンスまたは WSA）や Blue Coat ProxySG などのプロキシデバイスから分析用のグローバル脅威アラートシステムに、ログファイルのテレメトリデータをアップロードします。

ステップ 1 ページ右上隅の歯車アイコンをクリックし、[デバイスアカウント（Device Accounts）] を選択して設定ウィザードを開きます。

（注） すでに既存のデバイスアカウントが 1 つ以上ある場合は、設定を省略して [デバイスアカウント（Device Accounts）] ページが表示されます。

ステップ 2 セットアップウィザードを開始してデバイスアカウントを追加する準備ができたら、[では始めましょう（Let's Get Started）] をクリックします。

ステップ 3 ドロップダウンから自動アップロードまたは手動アップロードのいずれかを選択して、テレメトリデータをデバイスからアップロードする方法を選択します。グローバル脅威アラートシステムは、一度に 1 つのアップロード方法のみをサポートします。組み合わせることはできません。

（注） 自動から手動にアップロード方法を切り替えるには、まず、すべてのプロキシデバイスを自動アップロード設定から削除する必要があります。

ステップ 4 自動アップロード方式を選択した場合は、[SCP] または [HTTPS] のいずれかを選択して、ログファイルの転送に使用するプロトコルを選択します。

a) このデバイスの名前を入力し、[アカウントの追加（Add Account）] をクリックします。

b) SCP を選択した場合：

- Cisco WSA の設定に情報（ホスト、ポート、ディレクトリ、ユーザ名）をコピーします。セキュリティ上の理由により、情報は 1 度しか表示されません。

プロキシデバイスのアップロード

- Cisco WSA の設定方法の詳細については、「Configure Cisco Secure Web Appliance to Upload Log Files to Cisco Global Threat Alerts」を参照してください。
- Cisco WSA 管理コンソールが SSH 公開キーを返したら、この SSH 公開キーをデバイスアカウントにコピーして貼り付けます。
- [終了（Finish）] をクリックします。
- また、[デバイスアカウント（Device Accounts）] ページに移動してデバイスをクリックすると、SSH 公開キーを後で入力できます。

c) HTTPS を選択した場合：

- 情報（ホスト、ポート、パス、ユーザ名、パスワード）をコピーして Blue Coat ProxySG 設定に貼り付けます。
- Blue Coat ProxySG の設定方法の詳細については、「Configure Blue Coat ProxySG to Upload Log Files to Cisco Global Threat Alerts」を参照してください。
- [終了（Finish）] をクリックします。

ステップ 5 手動アップロード方式を選択した場合：

a) ログファイルの形式を検証します。次の準備ガイドラインに従ってください。

- Cisco WSA および Blue Coat プロキシで作成された W3C ログファイルはサポートされています。
- すべてのログファイルは GZip（*.gz）形式で圧縮する必要があります。
- 各ログファイルは 1 GB 未満にする必要があります。1 GB を超えるログファイルは、複数の小さいファイルに分割する必要があります。それぞれの間隔が重複していないこと、すべてのファイルに同一の適切なヘッダーが含まれていることを確認します。
- ログファイルに必要な間隔の合計は 2 日以上です。
- 各ログファイルの間隔は、固有で重複しないようにする必要があります。
- 各ログファイルには、時間の昇順（古いエントリが前、新しいエントリが後）にログエントリを含める必要があります。
- ログファイルはアルファベット順/数字順にソートし、時間に応じた順序でアップロードする必要があります。古いファイルを新しいファイルの前にアップロードする必要があります。1回のアップロードの中では、アップロードコンポーネントが自動的にファイルをソートします。複数回アップロードする場合は、常に以前よりも新しいデータをアップロードしてください。プロキシログファイルでデフォルトで使用される命名規則が保持されている場合、ファイル名はすでに正しくソートされています。
- 前にアップロードしたデータよりも古いデータは処理されません。
- ログファイルの内容は、アップロードに有効な特定の基準に一致する必要があります。
  - シスコは、アップロード前にログファイルを確認するためのログ検証ツールを提供しています。

- ログファイルの先頭の 20 行をコピーしてログ検証ツールに貼り付け、エラーをチェックします。
- エラーが表示されたら、ユーザがそのエラーを修正すると同時に、ツールはエラーのチェックを自動的に継続します。

b) [ファイルの追加（Add files）] をクリックしてアップロードするログファイルを選択するか、ログファイルをアップロードボックスにドラッグアンドドロップします。

（注） [ファイルの削除（Clear files）] をクリックして、アップロードボックスに追加されたすべてのファイルをクリアします。

c) [アップロードを開始（Start upload）] をクリックすると、選択したログファイルが 解析用グローバル脅威アラートシステムにアップロードされます。グローバル脅威アラートシステムに結果が表示されるまでしばらく待ちます。

（注） データをドロップするリスクを最小限に抑えるため、グローバル脅威アラートシステムは 5 時間後にアップロードされたデータの処理を開始します。これにより、処理が開始される前にすべてのアップロードを完了して、すべてが適切な順序で配置されるようにできます。

注意 手動から自動に切り替えると、すべてのアップロードが中止し、アップロードデータの処理が停止されます。アップロードしたデータはすべて廃棄されます。

（注） ページを閉じたり、ページから移動したりすると、現在のファイルアップロードが停止されます。

（注） 最初にすべての手動アップロードを停止するまで、自動アップロードを使用することはできません。すべてのデータが処理される前に切り替えると、移行の際に一部の分析データが消失する場合があります。システムがデータをドロップしないようにするには、最後の手動アップロードから 24 時間後に切り替えを実行します。

次のタスク

[デバイスアカウント（Device Accounts）] ページには、プロキシデバイスとその情報が一覧で表示されます。[ステータス（Status）] 列には、各デバイスのステータスが表示されます。

- New - SCP の設定が未完了で、SSH 公開キーが消失している場合があります
- Provisioning - プロビジョニング中のアカウントの準備がまだできていません
- Ready - アカウントが正常に作成されました
- Error - ステータスにカーソルを合わせると、エラーを説明するポップアップメッセージが表示されます

この概要ページから、別のデバイスアカウントの追加、削除するデバイスの選択、SSH 公開キーの入力、トラブルシューティングを行うことができます。

プロキシデバイスのアップロード

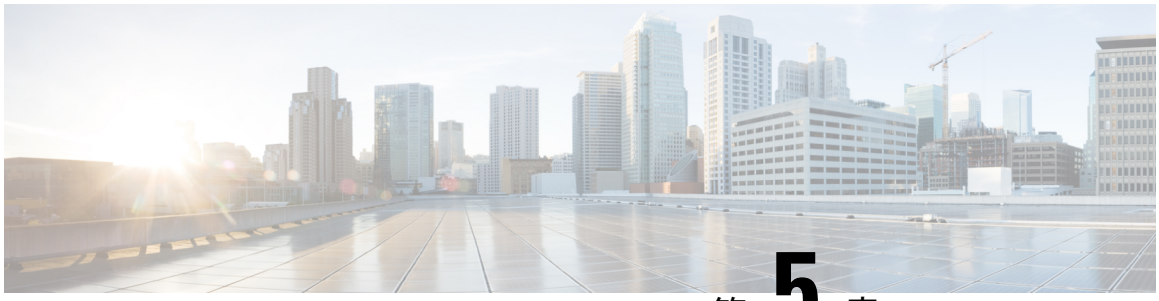
複数のデバイス間またはアップロードプロセス間でアカウントを共有できますが、各デバイスに個別のアカウントを使用し、ファイル名の競合の可能性を最小限に抑え、アップロード問題のトラブルシューティングを簡単にすることを推奨します。

デバイスアカウントの準備が完了したら、クリックして [確認済み（Confirmed）] ページまたは [検出済み（Detected）] ページを表示し、ネットワーク内の疑わしいアクティビティを確認します。

（注） 通常、データは、プロビジョニングの完了後 2 ～ 3 日以内に利用可能になります。

第 I 部

リリースノート



第 5 章

2024 年 2 月

2024 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

新しい脅威検出をポートフォリオに追加しました。

- Coyote
- Donut Loader
- RisePro

また、既存の脅威検出のインジケーターも更新しました。

Coyote

Coyuteは、主にラテンアメリカのユーザーを標的とするバンキング型トロイの木馬で、支払請求書を装った電子メールによるフィッシング手法（T1566.001）を利用します。このマルウェアは、配布に Squirrel インストーラを使用します。Coyute は NodeJS や Nim などのプログラミング言語を使用して作成されていて、このマルウェアの適応性と回避能力を示しています。このトロイの木馬は、検出を回避するために、文字列難読化技術（T1027）と AES暗号化を組み合わせて使用しています。被害者のシステムにインストールされた Coyute は、コマンドアンドコントロール（C2）サーバー（TA0011）との通信を確立して、スクリーンショットを要求したり、キーロギングを実行したりします。

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

Donut Loader

Donut Loader は、スクリプトやアセンブリをメモリ内で実行するための高度なツールキットであり、悪意のある目的にも使用されます（T1055.009）。ステルス Windows プロセスインジェクション（T1055）用に暗号化されたシェルコード（T1027）を生成します。このマルウェア

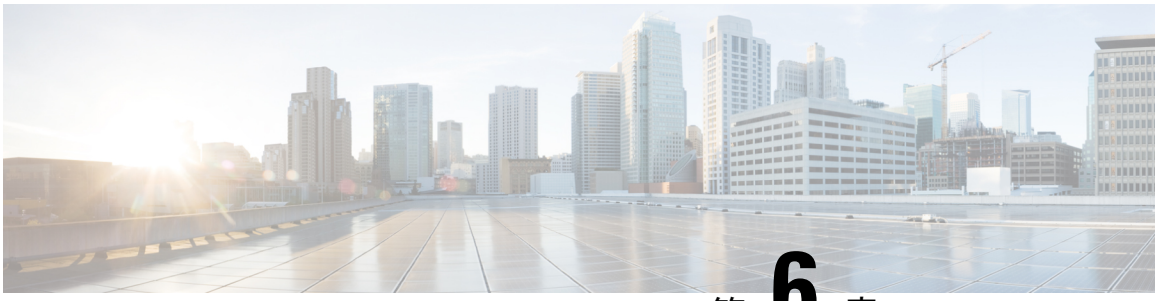
は、Chaskey暗号を使用して暗号化されたペイロードをシェルコード内に埋め込むか、URLからダウンロードすることによって（T1105）ステージレスに動作します。実行されると、メモリトレースを消去し（T1070）、新しいアプリケーションドメインでペイロードを分離することで検出を回避します。

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

RisePro

RiseProは、Telegramで販売されている情報窃盗マルウェアであり、Private Loaderマルウェアによって配布されます。RiseProは、感染したデバイスからデータを収集したり（TA0009）、スクリーンショットをキャプチャしたりできます（T1113）。RiseProは、ブラウザのログイン情報、暗号資産ウォレット（アドレスと秘密キー）、およびクレジットカード情報を読み取って盗むことができます。RiseProによって収集されたデータは、zipファイルに圧縮され、HTTPメッセージで盗み出されます（T1071.001）。この窃盗マルウェアは、コマンドアンドコントロール（C2）（T1041）を使用して構成を取得し、他のマルウェアをロードすることもできます。

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



第 6 章

2024 年 1 月

2024 年 1 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 （27 ページ）

追加の脅威検出

新しい脅威検出をポートフォリオに追加しました。

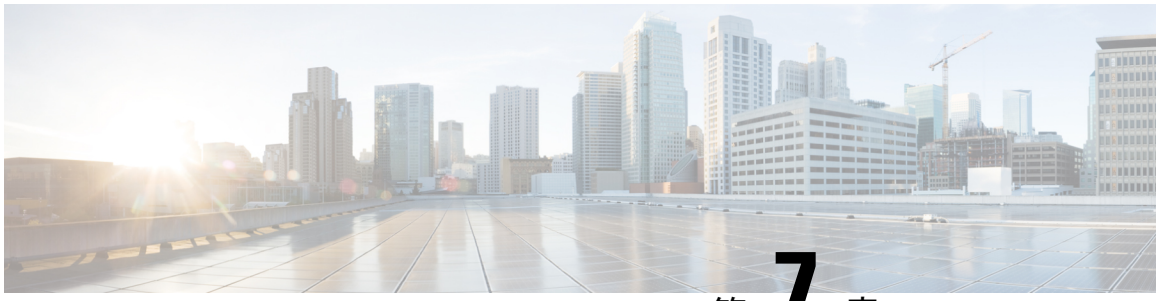
- Balada Injector

また、既存の脅威検出のインジケーターも更新しました。

Balada Injector

Balada Injector は、WordPress ベースの Web サイトに感染するマルウェアです。バックドアを仕込んで、偽のサポートページ、宝くじ当選サイト、プッシュ通知詐欺など、安全性に問題のあるサイトに訪問者をリダイレクトします。最新の Balada Injector キャンペーンは、Popup Builder バージョン 4.2.3 以前のクロスサイト スクリプティング（XSS）脆弱性（T1189）である CVE-2023-6000 について WPScan が報告した後に開始されました。これらの侵害された Web サイトは、マルウェアを配布するためのフィッシングメール（T1566.001）で使用され、さまざまなマルウェアファミリを展開できます。

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



第 7 章

2023 年 12 月

2023 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。

- 追加の脅威検出 （29 ページ）

追加の脅威検出

新しい脅威検出をポートフォリオに追加しました。

- Agniane Stealer
- Pikabot
- SectopRAT

また、既存の脅威検出のインジケーターも更新しました。

Agniane Stealer

Agniane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）を標的とする窃取マルウェアです。2023 年以降、Malware-as-a-Service モデルを通じて人気を得ています。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。WMI（T1047）、PowerShell（T1059.001）、および ConfuserEx 難読化ツール（T1027）を使用して保護されている .NET 実行可能ファイルを使用します。

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

Pikabot

Pkabotは、ローダーとコアペイロードで構成されるモジュール型マルウェアです。C/C++で記述されていて、被害者のシステムに他のマルウェアを展開するためによく使用されます（T1105）。CIS 諸国のメンバーはターゲットリストから除外され、多くの場合、悪意のある添付ファイルを含むフィッシングメール（T1566.001）で配信されます。そのコアモジュール

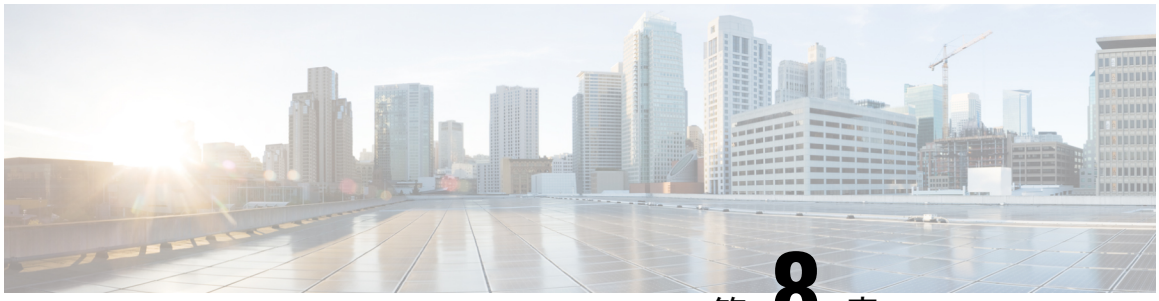
は、多くの場合、ファイルのダウンロードやさまざまなペイロードの実行（TA0002）など、複数の段階を介して展開されます。Pkabotは回避能力が非常に高く、VM対策/デバッグ（T1622）技術と難読化された文字列（T1027）を活用して検出を回避します。これはQakbot（S0650）やDarkGateなどのマルウェアと同様の動作を示します。

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

SectopRAT

SectopRAT（別名ArechClient2）は、正規のソフトウェアを装った悪意のあるリンク（T1204.001）によって配布される、.NETリモートアクセス型トロイの木馬です。SectopRATには複数の機能があります。感染したデバイスからオペレーティングシステムやハードウェア情報などの詳細情報を抽出したり（T1082）、保存されているログイン情報を窃取したり（T1552.001）、非表示のブラウザセッションを起動したりできます。アプリケーション層プロトコルを使用してコマンドアンドコントロールサーバーと通信し（T1071）、非標準ポート（T1571）を使用して他のペイロードをダウンロードし、情報を盗み出します。SectopRATには、マルウェア対策ソリューションを無効にし、サンドボックスの実行を回避するためのさまざまな機能があります。

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



第 8 章

2023 年 11 月

2023 年 11 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 （31 ページ）

追加の脅威検出

新しい脅威検出をポートフォリオに追加しました。

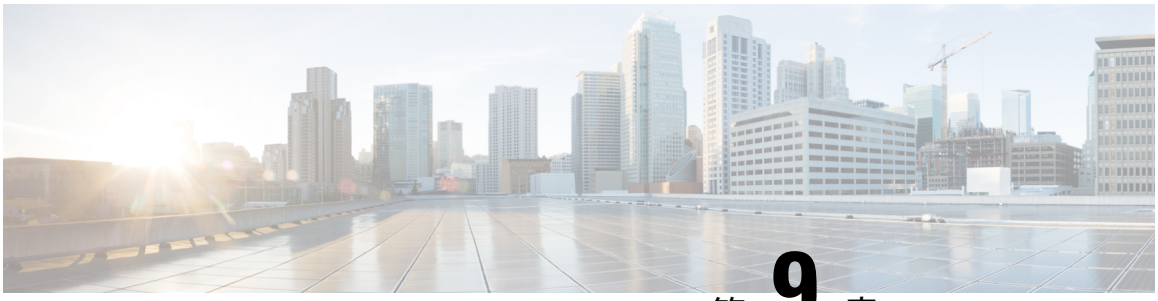
- 危機的状況主導型のサイバー脅威

また、既存の脅威検出のインジケーターも更新しました。

危機的状況主導型のサイバー脅威

危機的状況に連動するサイバー活動は、パンデミック、戦争、自然災害などの世界的な危機によって引き起こされ、さまざまな攻撃者によって実行されます。1 つのイベントに複数の攻撃者が関与している場合、その帰属が不明であったり混在していることはよくあります。これらのアクティビティには、通常、フィッシングキャンペーン（T1566）、正当な組織へのなりすまし（T1656）、信頼関係の悪用（T1199）、および詐欺が含まれます。潜在的な成果には、情報戦に対する優位性の獲得、初期アクセスの獲得、サイバー攻撃の実施（T1583）、および金銭的利益が含まれます。

お使いの環境で危機的状況主導型のサイバー脅威が検出されたかどうかを確認するには、[危機的状況主導型のサイバー脅威の詳細（Crisis-Driven Cyber 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。



第 9 章

2023 年 10 月

2023 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。

- 追加の脅威検出 （33 ページ）

追加の脅威検出

新しい脅威検出をポートフォリオに追加しました。

- DarkGate Loader

また、既存の脅威検出のインジケーターも更新しました。

DarkGate Loader

DarkGate Loader（MehCrypter とも呼ばれます）は、QakBot の亜種です。このローダーは、Microsoft Teams メッセージを悪用して、DarkGate Loader をインストールする悪意のある添付ファイルを送信するフィッシングキャンペーン（T1566）によって配布されます。マルウェアがエンドポイントで実行されると（T1204.002）、リモートアクセス（T1219）、暗号通貨マイニング（T1496）、キーロギング（T1056.001）、クリップボード窃盗、情報窃盗など、さまざまな悪意のあるアクティビティが発生する可能性があります。

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

第 10 章

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 （35 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ーも更新しました。

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）。スピアフィッシング（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ッパーマルウェアです。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。

第 11 章

2023 年 8 月

2023 年 8 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 （37 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。

- Spyder Backdoor
- AsyncRAT

また、既存の脅威検出のインジケーターも更新しました。

Spyder Backdoor

Spyder は、WarHawk と同様のバックドアであり、主に攻撃者である SideWinder によって使用されます。このマルウェアは、Word、Excel、PDF、またはその他のドキュメントファイルを装った実行ファイルです。バックドアがインストールされると、マシン GUID、ユーザー名、CPU、ウイルス対策情報などのシステム情報を収集し（T1082）、HTTP/HTTPS（T1071.001）を使用したコマンドアンドコントロールによって漏洩します。Spyderは、翌日に実行されるようにスケジュールされたタスクを作成できます（T1053.005）。また、追加のペイロードをダウンロードすることもできます（T1105）。

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

AsyncRAT

AsyncRAT は当初、NYAN-x-CAT によってオープンソースのリモート管理ツールとして開発されました。当初は C# で記述されていましたが、他の開発者が Python と Java に適応させました。DcRAT（別名 DarkCrystal RAT）などのマルウェアは、AsyncRAT のクローンです。その汎用性の高い機能から、攻撃者の間で人気があります。AsyncRAT は、画面の録画と表示

（T1113）、コマンドの実行（T1059）、ファイルのアップロードとダウンロード（T1105）、および被害デバイスでのパスワードの回復（T1003）を実行できます。.NET フレームワークバイナリに挿入され（T1055.002）、ダイナミック DNS ベースのコマンドアンドコントロールサーバーに接続される（T1583.001）ことが確認されています。

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

第 12 章

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 （39 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。

- 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。

第 13 章

2023 年 6 月

2023 年 6 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 （43 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。

- AMOS
- JackalControl
- RMS
- Satacom
- UNC4841

また、既存の脅威検出のインジケーターも更新しました。

AMOS

AMOS は Atomic macOS Stealer とも呼ばれ、Apple MacOS を標的とする情報窃取プログラムです。キーチェーンパスワード（T1555.001）、暗号ウォレット、システムデータ、ローカルファイル、さらには OS ログイン情報のダンプ（T1003）など、さまざまなタイプの情報のキャプチャに焦点を当てています。データを収集すると（T1560）、コマンドアンドコントロールチャネル（T1041）を介してデータを盗み出します。

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

JackalControl

JackalControl は、攻撃者が攻撃対象デバイスを制御できるようにする、GoldenJackal APT によって使用されるトロイの木馬です。JackalControl は、偽の Skype インストーラまたは添付ファイルとして配布される MS Word ドキュメントを介して配布されます。スケジュールされたタス

ク（T1053.005）、レジストリキー（T1547.001）、または Windows サービス（T1543.003）を作成することで、JackalControl は永続性を得ることができます。JackalControl は、感染したデバイス（T1082）に関する情報を収集し、HTTP POST 要求（T1071.001）を使用してコマンドアンドコントロールサーバーと通信するために使用されるボット ID を生成します。

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

RMS

RMS（Remote Manipulator System）は、RuRat および Gussdoor とも呼ばれ、Microsoft Windows および Android デバイスのリモート管理のために TektonIT によって開発された正規のツールです。このツールは、ペイロード配布の手段としてフィッシングメールを使用した TA505 やその他の攻撃者によって実行されたキャンペーンで確認されています（T1566.001）。RMS がインストールされると、攻撃者は、コマンドアンドコントロール（T1071.001）を介した機密データの漏洩や追加のマルウェアの展開などの悪意のあるアクティビティのために、侵害されたデバイスに対する不正なリモートアクセスと制御を取得します。

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

Satacom

LegionLoader とも呼ばれる Satacom は、主に暗号通貨を盗むように設計されたブラウザ拡張機能（T1176）を配布するマルウェアです。このマルウェアは、違法コピーされたソフトウェアを配布するサードパーティの Web サイトを介して拡散し、その後、Satacom インストーラを含む zip ファイルをホストしている Web サイトに攻撃対象をリダイレクトします。攻撃対象がリダイレクションリンク（T1204.001）にアクセスすると、悪意のあるファイル（T1204.002）がダウンロードされ、実行されます。このファイルによって、ビットコインウォレットに関連するデータが収集され、コマンドアンドコントロールチャネル（T1041）経由でデータが流出します。Satacom によって配信される悪意のあるブラウザ拡張機能は、Coinbase、Bybit、KuCoin、Huobi、および Binance のユーザーをターゲットにしていることが確認されています。2FA をバイパスして、攻撃対象のビットコインアドレスと通貨を盗むことができます。

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

UNC4841

UNC4841 は、スパイ活動を目的としたキャンペーンを実行している疑いがある攻撃者です。このグループは、南北アメリカ、ヨーロッパ、およびアジア太平洋地域の公共部門と民間部門のさまざまな組織を対象としています。UNC4841 は、ゼロデイ脆弱性をエクスプロイトすることが確認されています。UNC4841 によってエクスプロイトされる脆弱性の 1 つは、Barracudo Email Security Gateway（ESG）の CVE-2023-2868 です。このグループは、フィッシング電子メールの添付ファイルを使用してマルウェア（T1566.001）を配布し、Saltwater、Seaside、SeaSpy、SkipJack などのバックドアを含めて、さまざまなマルウェアファミリを展開できます。一部のマルウェアは、Barracuna ESG をエクスプロイトするように特別に設計されています。

お使いの環境でUNC4841アクティビティが検出されたかどうかを確認するには、[UNC4841アクティビティ脅威の詳細（UNC4841 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。

第 14 章

2023 年 5 月

2023 年 5 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 （47 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。

- DarkCrystal RAT
- Fabookie
- Nemesis Project
- TrueBot

また、既存の脅威検出のインジケーターも更新しました。

DarkCrystal RAT

DarkCrystal RAT（別名 DCRAT）は、攻撃対象のデバイスを制御して情報を盗むことができるリモートアクセス型のトロイの木馬です。フィッシング（T1566）、その他のローダー（PrivateLoader など）、または偽のソフトウェアのクラックやアップデート（T1036）を介して配布されます。モジュール型マルウェアであるため、キーロギング（T1056.001）を実行し、感染したデバイスから Cookie、ログイン情報、およびその他の情報を盗むことができます。情報が収集されると、コマンドアンドコントロール通信（T1041）を介して漏洩します。

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

Fabookie

Fabookie は、感染したデバイスからログイン情報（特に Facebook ログイン情報）を盗むことを目的とした情報窃取プログラムです。Fabookie は通常、SmokeLoader、PrivateLoader、Nullmixer などの他のマルウェアによって配布されます。Fabookie がデバイスにインストールされると、

保存されているログイン情報（T1552）を検索し、システムにインストールされているソフトウェアに関する情報を収集します（T1518）。ログイン情報を取得すると、Facebook API とやり取りし、コマンドアンドコントロールサーバー（T1071）と通信します。

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

Nemesis Project

Nemesis Project は、ダークネットフォーラムで販売されている情報窃取プログラムです。フィッシングメール（T1566.001）、悪意のあるオンライン広告、および偽のソフトウェアのダウンロード（T1036）を介して配布されます。また、Dave や Minodo Loader などの他のマルウェアとともに配布される可能性もあります。コマンドアンドコントロールサーバーと通信するために、Nemesis Project は HTTP や HTTPS（T1071.001）などのアプリケーション層プロトコルを使用し、DNS 要求（T1071.004）を活用できます。情報窃取プログラムは、VPN とブラウザを標的とし、攻撃対象システムから入力アクション（T1056）とスクリーンショット（T1113）をキャプチャできます。Nemesis Project マルウェアは、Web サービス（T1567）または FTP や SMTP などの代替プロトコル（T1048）を使用して、盗んだデータをコマンドアンドコントロールサーバーに送信します。

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

TrueBot

TrueBot（サイレンスとも呼ばれる）は、攻撃対象デバイスで追加のペイロードを取得して実行できるダウンローダーマルウェアです。これは、以前の感染（T1105）を介して、または一般向けアプリケーション（T1190）をエクスプロイトすることによって展開できます。TrueBot は、Grace（S0383）、Clop（S0611）、CobaltStrike（S0154）などのマルウェアやツールを展開することが知られています。TrueBot 感染は、ローダーとダウンローダーの 2 つのモジュールで構成されます。ローダーが復号化すると（T1140）、追加のペイロードを取得するためにダウンローダーをドロップします。TrueBot は、スケジュールされたタスク（T1053.005）とレジストリ実行キー（T1547.001）によって永続性を維持します。感染チェーンの後半で関連するマルウェアが使用されているため、TA505（G0092）の一部であると想定されています。

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

第 15 章

2023 年 4 月

2023 年 4 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。

- Lumma
- PYbot

また、既存の脅威検出のインジケーターも更新しました。

Lumma

悪意のある情報窃盗マルウェアである Lumma には、攻撃対象のコンピュータに関する情報の取得（T1005）、メッセンジャーアプリケーションからのメッセージの取得、ブラウザ履歴、Cookie、保存されたログイン情報の収集（T1185）など、多くの機能があります。Lumma はフィッシング（T1566）によって配布され、コマンドアンドコントロール（T1071）を介してデータを盗み出し、自動漏洩手法（T1020）を使用します。

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

PYbot

PYbot は、Python（T1059.006）で記述され、PyInstaller を使用してコンパイルされた DDoS ボット（T1498）です。これにより、Python がインストールされていないホストでマルウェアを実行できるようになります（T1204.002）。これは、.NET ベースのダウンローダーを含む偽のクラッキングされたソフトウェア（T1189）を介して配布されます。その後に、ダウンローダーは、インターネットから PYbot ペイロードを取得します（T1105）。PYbot は、レイヤ 4 およびレイヤ 7 のフラッディング攻撃（T1498.001）を介して攻撃対象を標的にすることができます。

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

第 16 章

2023 年 3 月

2023 年 3 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 （51 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。

- Amadey
- BatLoader
- Retadup
- Stealc
- ViperSoftX

また、既存の脅威検出のインジケーターも更新しました。

Amadey

Amedy は、データを盗み、他のマルウェアを展開することで知られるトロイの木馬ボットです。フィッシング（T1566）電子メールを介して配信されるか、他のマルウェアファミリによって展開されます。レジストリエントリ（T1547.001）とスケジュールされたタスク（T1053.005）を介して、攻撃対象のデバイスでの永続性を維持します。コマンドアンドコントロールサーバーと通信する前に、攻撃対象のデバイス（T1005）からドメイン名、ユーザー名、コンピュータ名、OSバージョンなどのさまざまなデータを収集します。収集されたデータの漏洩（T1041）後、エクスプロイトキット、情報窃盗、ランサムウェアなどのマルウェアをダウンロード（T1105）およびインストールできます。

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

BatLoader

BatLoader は、情報窃盗マルウェア、バンキング型トロイの木馬、ランサムウェア、およびその他のローダーなど、さまざまなマルウェアを攻撃対象のデバイスにインストールするモジュラーダウンローダーです。BatLoader は、クラックされたソフトウェア（T1204.001）を使用して配布されます。特に、Adobe、AnyDesk、CCleaner、TeamViewer、Zoom になりすますことが確認されています。攻撃対象が MSI ファイル（T1204.002）をダウンロードして実行すると、さらなる感染のためにカスタムアクションを介して Powershell（T1059.001）ペイロードを実行します。その後、攻撃対象のデバイスは、コマンドアンドコントロールサーバー（T1071.001）に接続し、他のペイロード（T1105）をダウンロードします。

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

Retadup

Retadup は、自己複製機能を備えた Monero マイナーです。攻撃対象のデバイス（T1091）の使用可能なすべての外部ドライブに LNK ファイルをコピーします。その後、悪意のある AutoIt でコンパイルされたスクリプト（T1204.002）を実行し、ホスト名や OS バージョンなどのエンコードされたホスト情報（T1132.001）をコマンドアンドコントロール サーバーにエクスポートします。スティーラーやランサムウェアなどの追加のマルウェア（T1105）を展開できます。2019年にテイクダウンされたにもかかわらず、特に中南米のデバイスをターゲットにしたネットワークで引き続き確認されています。多くの場合、ペイロード名は、正規のソフトウェアや、Google や Microsoft などの企業を模倣します（T1036.005）。

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

Stealc

Stealc は、ダークネットフォーラムで販売されている情報窃取型マルウェアです。フィッシングメール（T1566.001）、悪意のあるオンライン広告、および偽のソフトウェアのダウンロード（T1036）を介して配布されます。コマンドアンドコントロール サーバーと通信するために、Stealc は HTTP や HTTPS（T1071.001）などのアプリケーション層プロトコルを使用できます。また、DNS 要求（T1071.004）を活用し、攻撃対象のデバイスから入力アクション（T1056）またはスクリーンショット（T1113）をキャプチャすることもできます。Stealc は、Web サービス（ T1567 ）または FTP や SMTP などの代替プロトコル（ T1048 ）を使用して、盗んだデータをコマンドアンドコントロール サーバーに送信します。https://attack.mitre.org/versions/v12/techniques/T1567https://attack.mitre.org/versions/v12/techniques/T1048

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

ViperSoftX

ViperSoftX は、VenomSoftX と呼ばれる Chrome ブラウザ拡張機能を展開するマルウェアです。マルウェアは、クラッキングされたソフトウェアまたはトレントダウンロード（T1036）を使用して配布されます。暗号化されたバイナリ（T1027）、Powershell ペイロード（T1059.001）、およびブラウザ拡張機能（T1176）を活用してタスクを実行できます。HTTP または HTTPS

（T1071）を使用してコマンドアンドコントロール サーバーと通信します。このマルウェアは、暗号通貨ウォレット（T1496）の窃取、クリップボードデータの収集（T1115）、コマンドの実行（TA0002）、およびその他のタスクを実行できます。

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

第 17 章

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

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

自動化サポート用の新しい REST API 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。

第 18 章

2023 年 1 月

2023 年 1 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 （57 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。

- GootLoader
- Laplas Clipper
- Neoreklami
- Rhadamanthys

また、既存の脅威検出のインジケーターも更新しました。

GootLoader

GootLoader は、ドロッパーマルウェアであり、SEO ポイズニングを介して拡散します（T1608.006）。ユーザーをだまして、悪意のある JS ファイルを含む無害に見える ZIP ファイルをダウンロードさせます。wscript と cscript（T1059.005）を使用して、この初期ペイロードを実行します。スケジュールされたタスク（T1053.005）を通じて永続性を獲得し、C2 トラフィックに Powershell（T1059.001）を活用します。攻撃対象デバイスで CobaltStrike（S0154）をドロップすることが確認されています。そのコマンドアンドコントロールインフラストラクチャは、侵害された WordPress Web サイト（T1584.004）で構成されています。

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

Laplas Clipper

Laplas Clipper は、暗号通貨を盗むマルウェアです。SmokeLoader（S0226）またはフィッシング（T1566）によって配信されます。永続化のために、schtasks（T1053.005）を使用してスケジュールタスクを作成します。 Laplas Clipper は、攻撃対象を模倣したウォレットアドレスを

生成して、通貨トランザクションをハイジャックします。このマルウェアは、ビットコイン、イーサリアム、ビットコインキャッシュ、ライトコイン、ドージコインなど、さまざまなウォレットから盗み出します。

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

Neoreklami

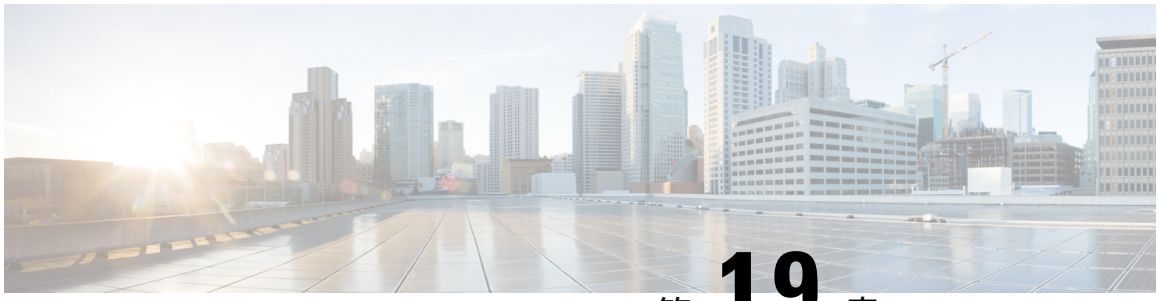
Neoreklami は、ユーザーのブラウザセッションを制御するために AdBlocker を模倣することが知られています（T1185）。永続化のために WSF（T1059.005）および DLL（T1218.011）ファイルを実行するタスク（T1053.005）をスケジュールします。これらのファイルを保存するために、ProgramData および Program Files（x86）内にランダムな英数字で名前が付けられたフォルダが作成されます。ユーザーのブラウザセッションに感染すると、難読化されたペイロード（T1027）をダウンロードして次のアクションを決定します。感染したデバイスは、ハイパーリンクに変換されたランダムな Web ページテキスト、正当な Web ページが挿入された広告バナー、偽の更新を推奨するポップアップなどを表示する可能性があります。

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

Rhadamanthys

Rhadamanthys は、感染したデバイスから情報を抽出して抜き取る情報窃取プログラムです。最初のアクセスは、AnyDesk、Zoom、Notepad++ などのアプリケーションの偽のソフトウェア配布（T1036）によって行われます。このマルウェアを配布するドメインは、Google 広告を悪用し、それらのアプリケーションを偽装することが確認されています。Rhadamanthys マルウェアは、オペレーティングシステムのバージョン、デバイス名、インストールされているソフトウェアなどのデバイス情報とともに、暗号通貨ウォレットに関連する情報を盗みます。このマルウェアは、コマンドアンドコントロール（T1041）を介してデータを盗み出します。

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



第 19 章

2022 年 12 月

2022 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。

- 追加の脅威検出 （59 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。

- Private Loader
- PlugX

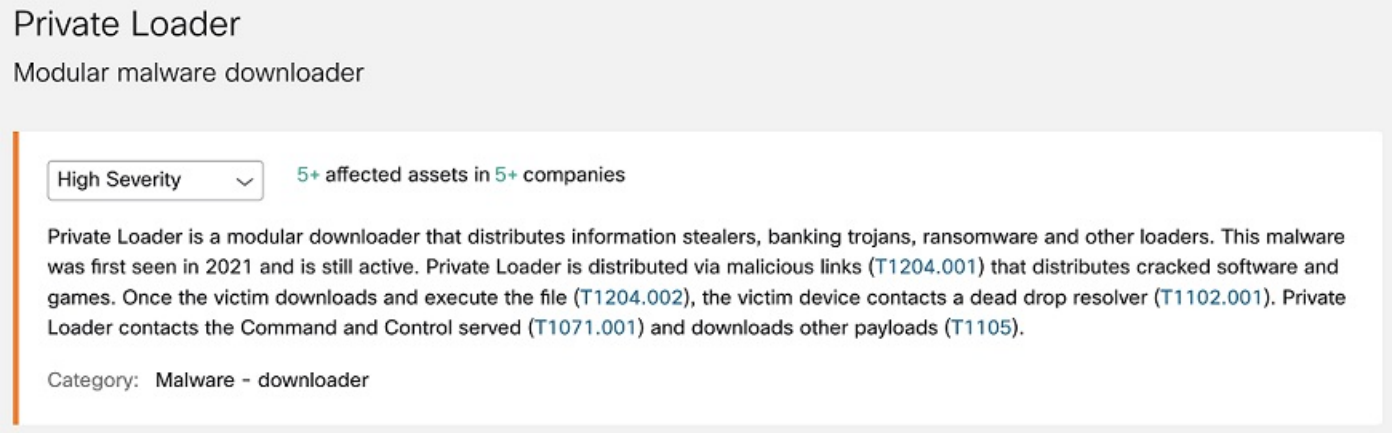
また、既存の脅威検出のインジケーターも更新しました。

Private Loader

Private Loaderは、情報窃盗マルウェア、バンキング型トロイの木馬、ランサムウェア、およびその他のローダーを配布するモジュラーダウンローダーです。このマルウェアは 2021 年に最初に確認され、現在も活動しています。Private Loaderは、クラックされたソフトウェアやゲームを配布する悪意のあるリンク（T1204.001）を使用して配布されます。攻撃対象がファイルをダウンロードして実行すると（T1204.002）、攻撃対象のデバイスはデッドドロップリゾルバ（T1102.001）に接続します。Private Loader は、コマンド アンド コントロール サーバー（T1071.001）に接続し、他のペイロード（T1105）をダウンロードします。

お使いの環境で Private Loader が検出されたかどうかを確認するには、[Private Loader 脅威の詳細（Private Loader 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 *18 :*

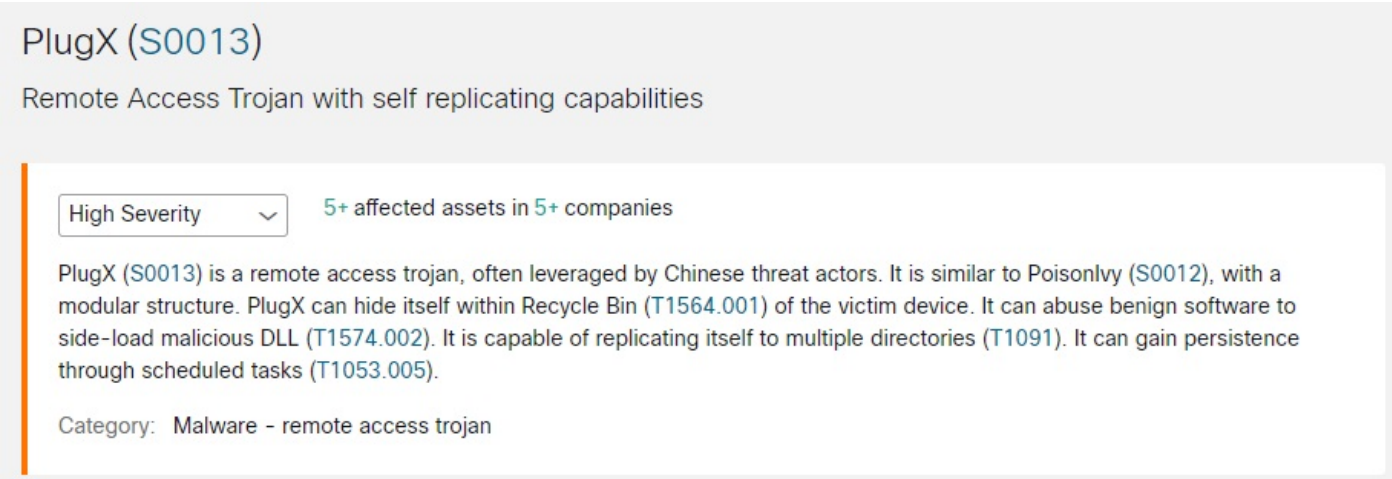


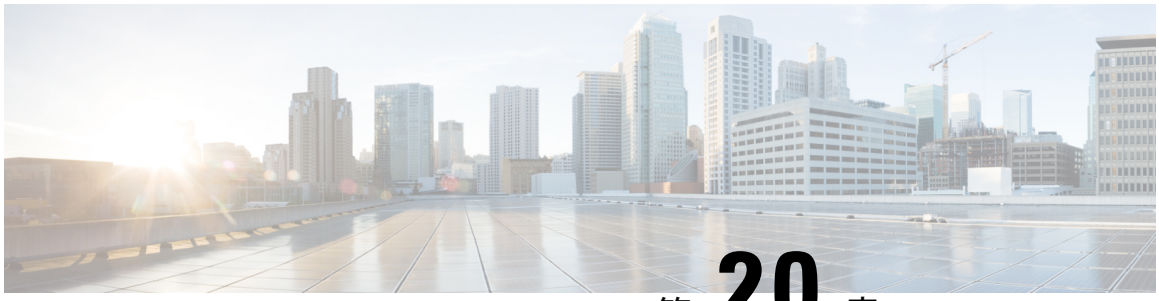
PlugX

PlugX（S0013）は、リモートアクセス型トロイの木馬であり、中国の攻撃者によってよく利用されます。これは PoisonIvy（S0012）に似ており、モジュラー構造です。PlugX は、攻撃対象のデバイスのごみ箱（T1564.001）内に隠れることができます。また、無害なソフトウェアを悪用して、悪意のある DLL（T1574.002）をサイドローディングすることもできます。複数のディレクトリへのそれ自体の複製が可能で（T1091）、スケジュールされたタスクを通じて永続性を得ることができます（T1053.005）。

お使いの環境で PlugX が検出されたかどうかを確認するには、[PlugX 脅威の詳細（PlugX 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 *19 :*





第 20 章

2022 年 11 月

2022 年 11 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 （61 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。

- ChromeLoader
- CryptBot
- Mispadu
- Pterodo

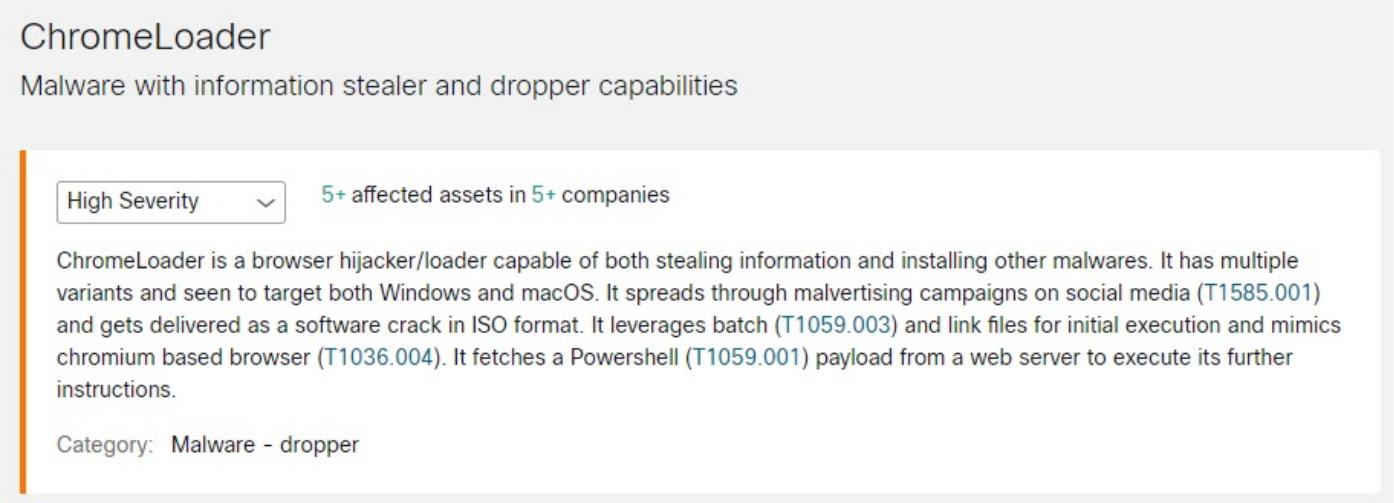
また、既存の脅威検出のインジケーターも更新しました。

ChromeLoader

ChromeLoader は、情報を盗み、他のマルウェアをインストールすることができるブラウザハイジャッカー/ローダーです。複数のバリアントがあり、Windows と macOS の両方を標的としています。ソーシャルメディア（T1585.001）上のマルバタイジング攻撃を通じて拡散し、ISO 形式のソフトウェアクラックとして配信されます。バッチ（T1059.003）とリンクファイルを初期実行に活用し、Chromium ベースのブラウザ（T1036.004）を模倣します。Web サーバーから Powershell（T1059.001）ペイロードを取得して、さらに命令を実行します。

お使いの環境で ChromeLoader が検出されたかどうかを確認するには、[ChromeLoader 脅威の詳細（ChromeLoader 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 *20 :*

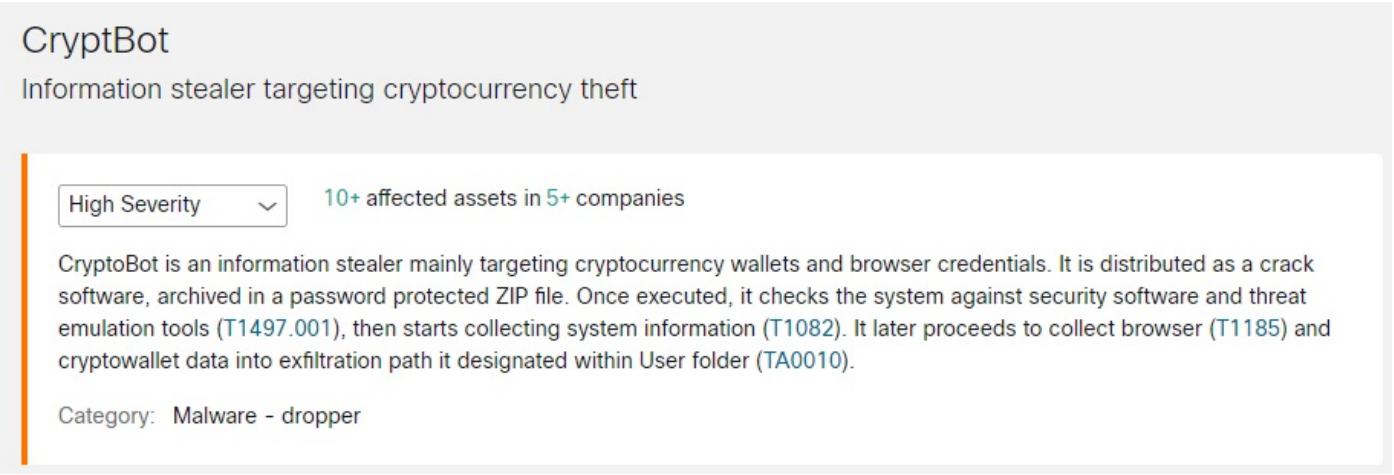


CryptBot

CryptBot は、主に暗号通貨ウォレットとブラウザのログイン情報を標的とする情報窃盗マルウェアです。これはクラックソフトウェアとして配布され、パスワードで保護されたZIPファイルにアーカイブされています。実行されると、セキュリティソフトウェアと脅威エミュレーションツール（T1497.001）に対してシステムをチェックし、システム情報（T1082）の収集を開始します。その後、ブラウザ（T1185）と暗号ウォレットのデータを収集し、ユーザーフォルダ（TA0010）内で指定した漏洩パスに移動します。

お使いの環境でCryptBotが検出されたかどうかを確認するには、[CryptBot 脅威の詳細（CryptBot 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 *21 :*

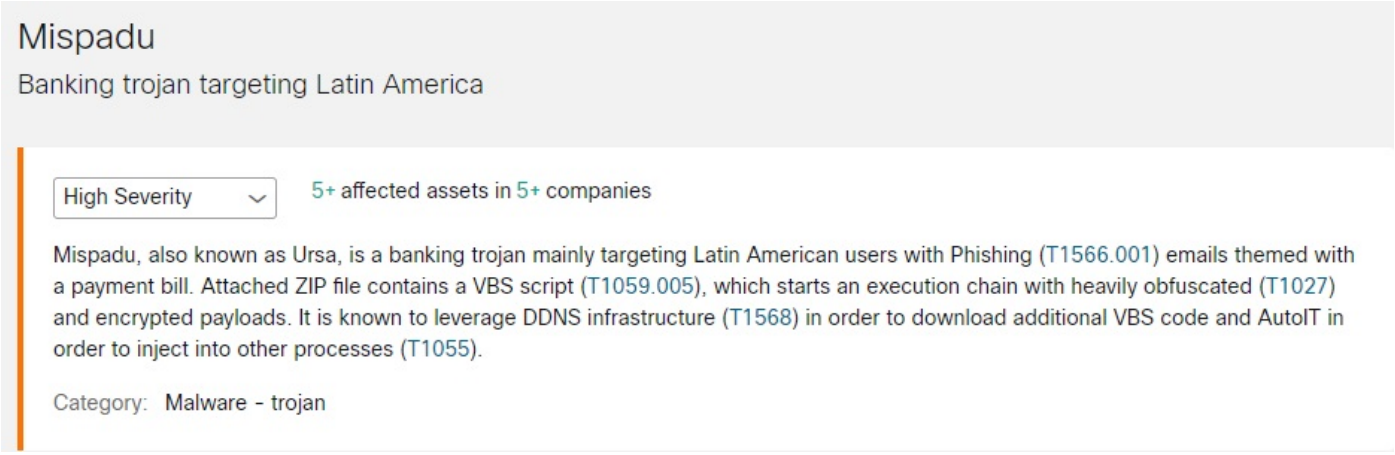


Mispadu

Ursa としても知られる Mispadu は、支払い請求書をテーマにしたフィッシング（T1566.001）メールで主に南米のユーザーを標的にしたバンキング型トロイの木馬です。添付の ZIP ファイルには、高度に難読化（T1027）され暗号化されたペイロードで実行チェーンを開始する VBS スクリプト（T1059.005）が含まれています。DNS インフラストラクチャ（T1568）を利用して、追加の VBS コードと AutoIT をダウンロードして、他のプロセス（T1055）に挿入することが知られています。

お使いの環境で Mispadu が検出されたかどうかを確認するには、[Mispadu 脅威の詳細（Mispadu 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 *22 :*

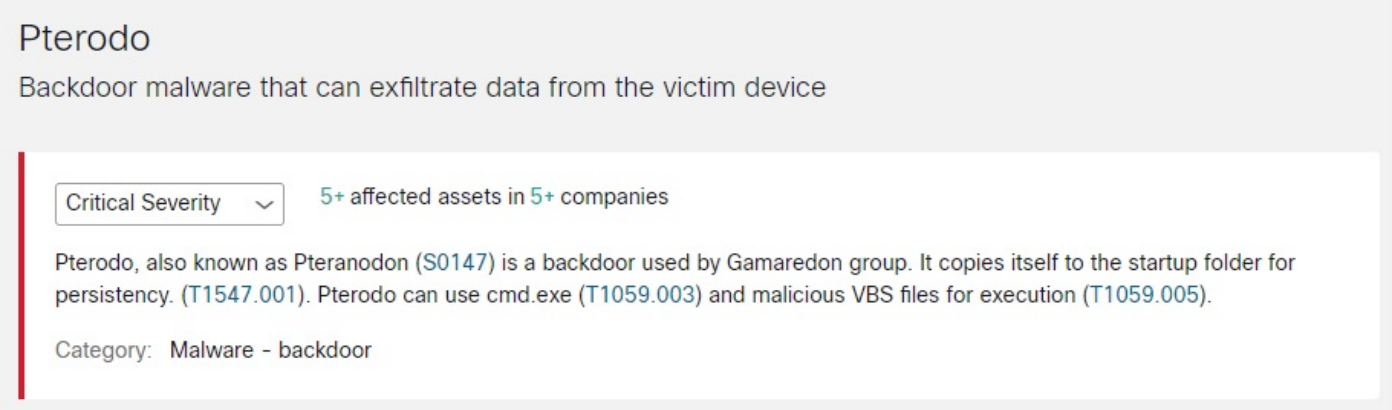


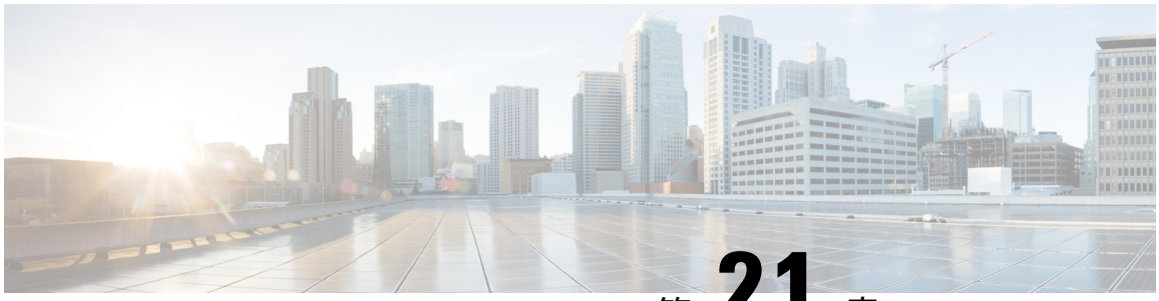
Pterodo

Pteranodon としても知られる Pterodo（S0147）は、Gamaredon グループが使用するバックドアです。永続化（T1547.001）のために自身をスタートアップフォルダにコピーし、cmd.exe（T1059.003）と悪意のある VBS ファイル（T1059.005）を実行に使用します。

お使いの環境で Pterodo が検出されたかどうかを確認するには、[Pterodo 脅威の詳細（Pterodo 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 *23 :*


Pterodo
Backdoor malware that can exfiltrate data from the victim device
Critical Severity
5+ affected assets in 5+ companies
Pterodo, also known as Pteranodon (S0147) is a backdoor used by Gamaredon group. It copies itself to the startup folder for persistency. (T1547.001). Pterodo can use cmd.exe (T1059.003) and malicious VBS files for execution (T1059.005).
Category: Malware - backdoor



第 21 章

2022 年 10 月

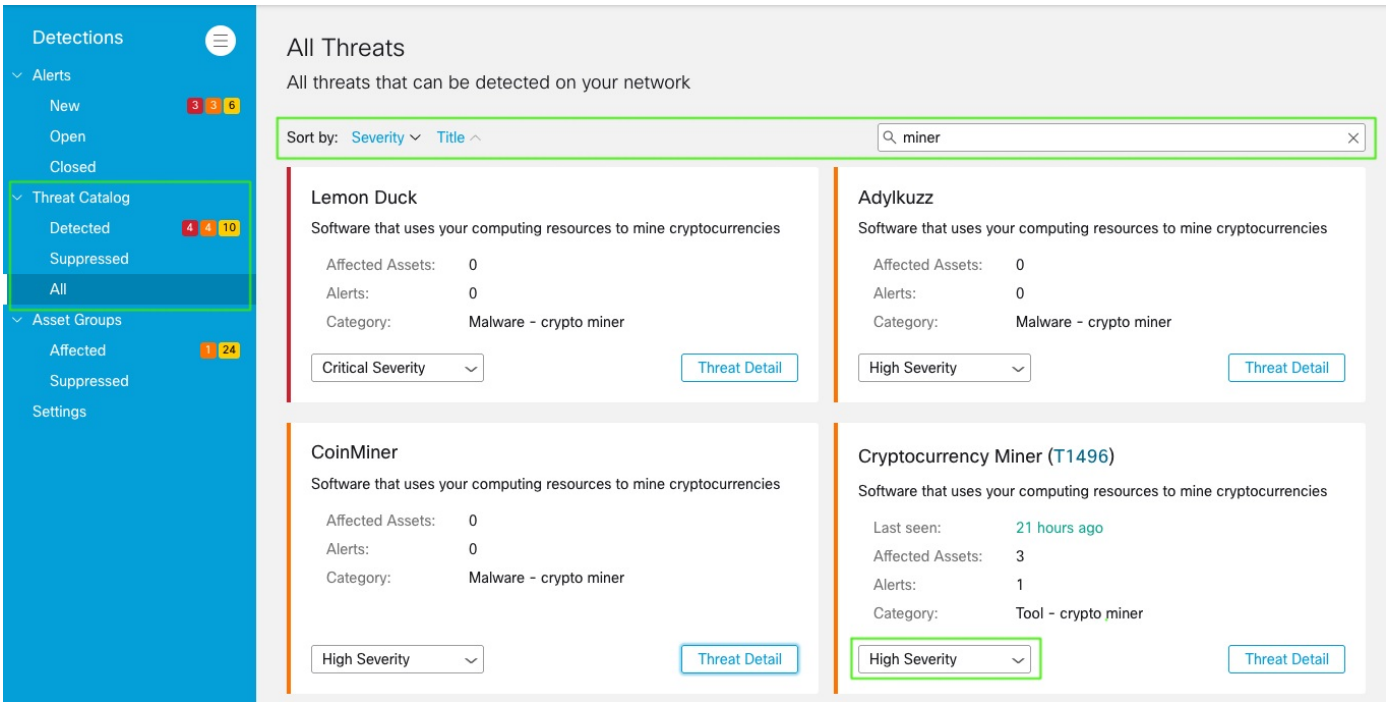
2022 年 10 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

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。

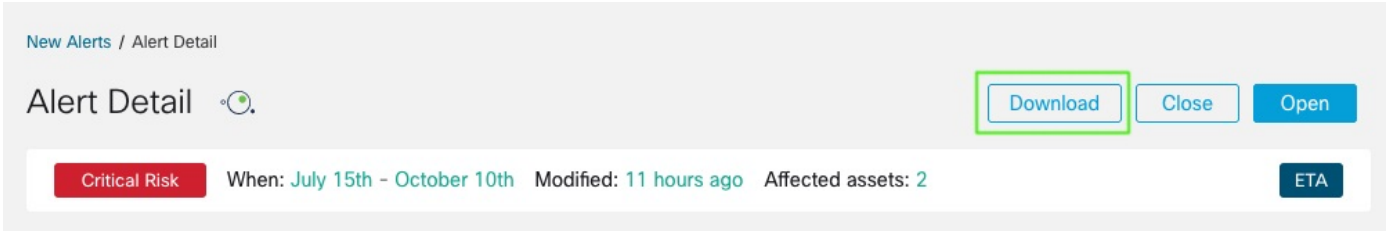
図 *24 :*



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。

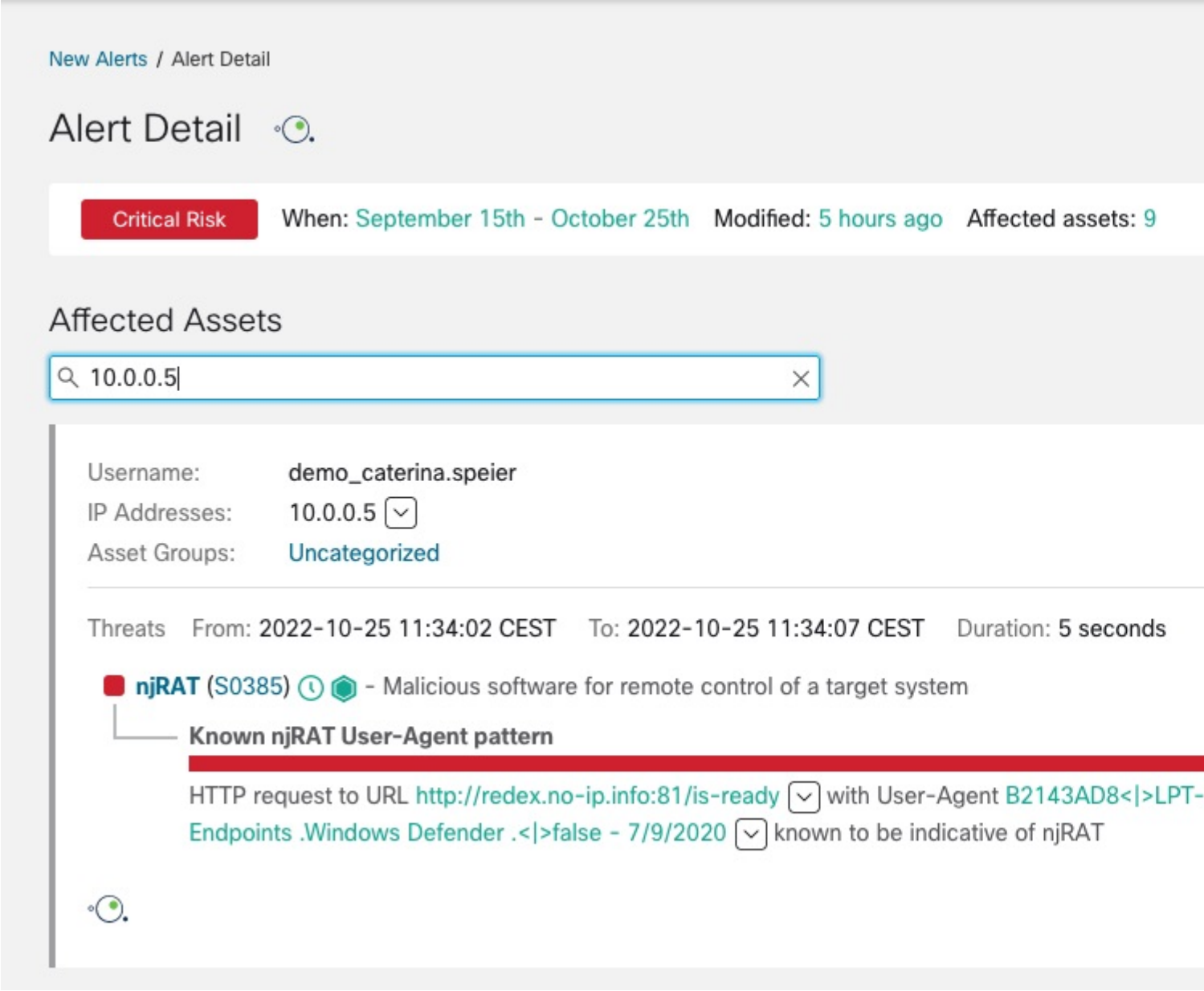
図 *25 :*



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 *26 :*

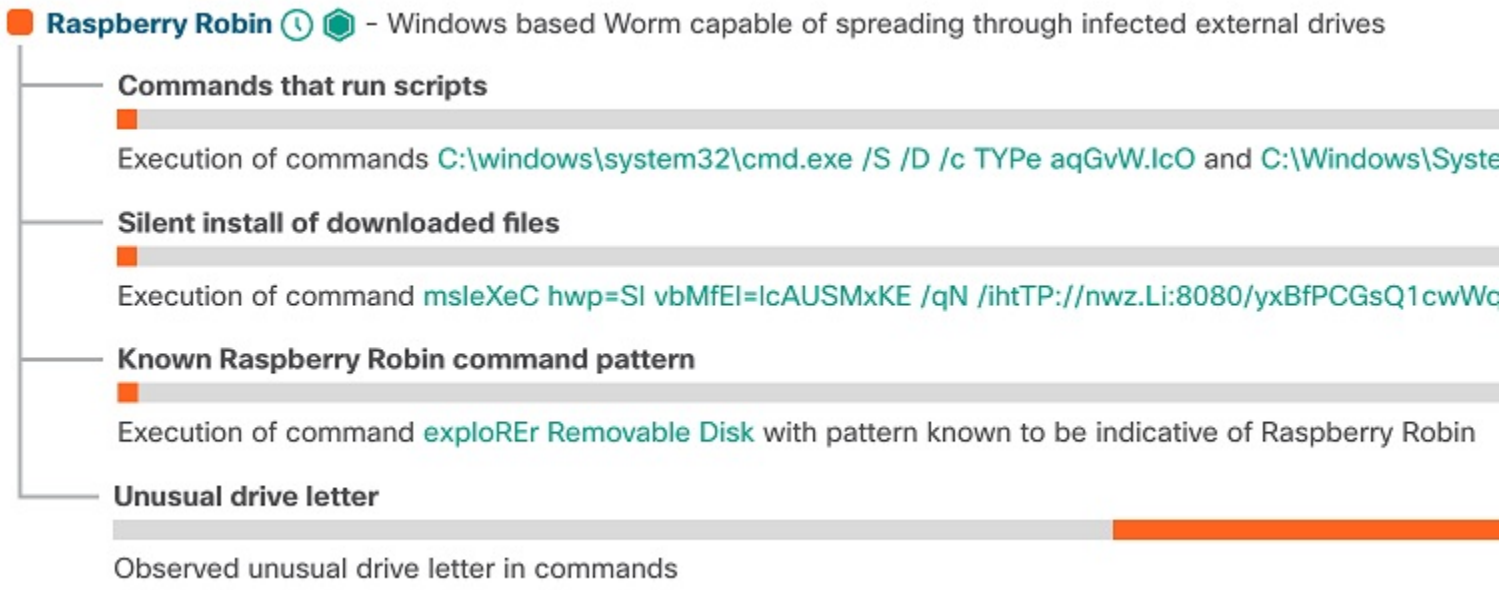


新たな検出

（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 *27 :*



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

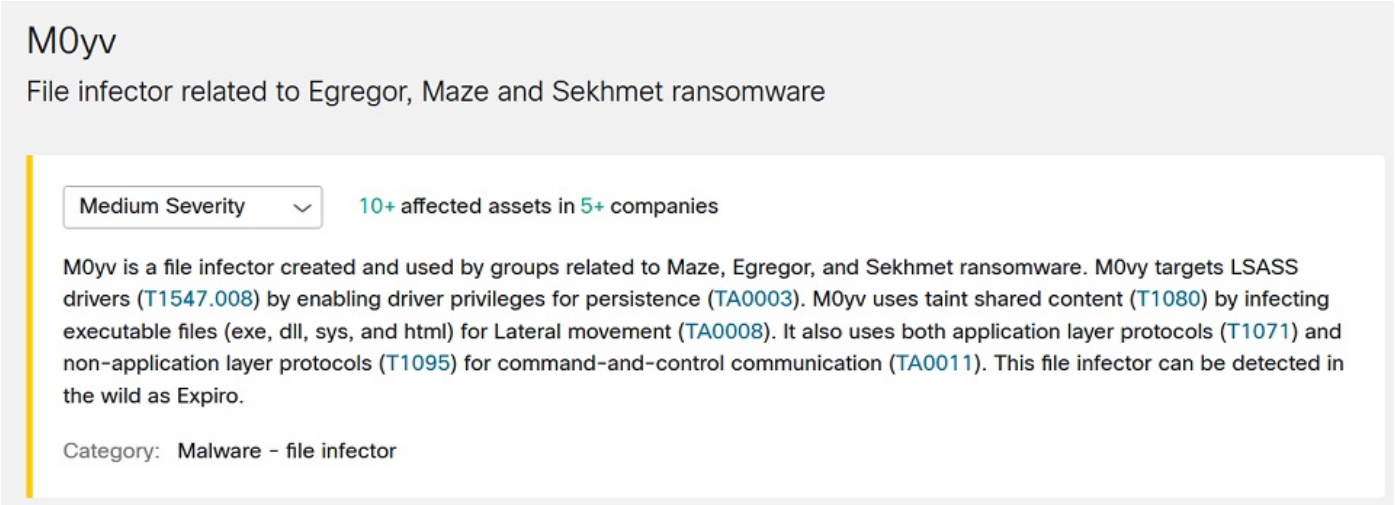
また、既存の脅威検出のインジケーターも更新しました。

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 *28 :*

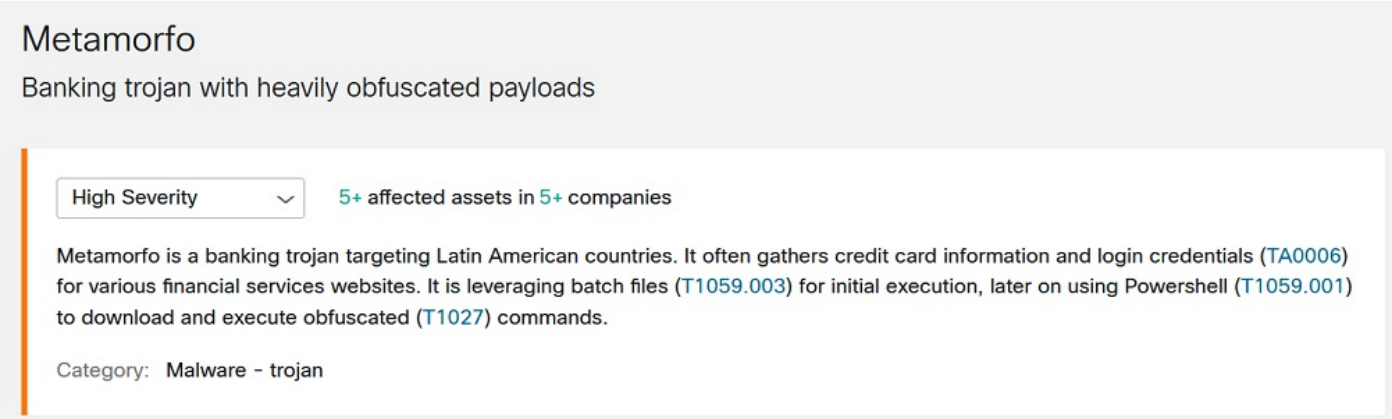


Metamorfo

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 *29 :*



第 22 章

2022 年 9 月

2022 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。

新しい Web インターフェイス

早期アクセスフェーズ中に、グローバル脅威アラートのメイン Web インターフェイスとして提供するために新しい Web インターフェイスを改良しました。

新しいインターフェースにより、次のことが可能になります。

- 改善されたアラートワークフロー
- MITRE ATT&CK® との調整
- アラート詳細の拡張表示

詳しくは、ダッシュボードのウォークスルーをご覧ください。

追加の脅威検出

新しい脅威検出、SolarMarker をポートフォリオに追加しました。また、既存の脅威検出のインジケーターを更新しました。

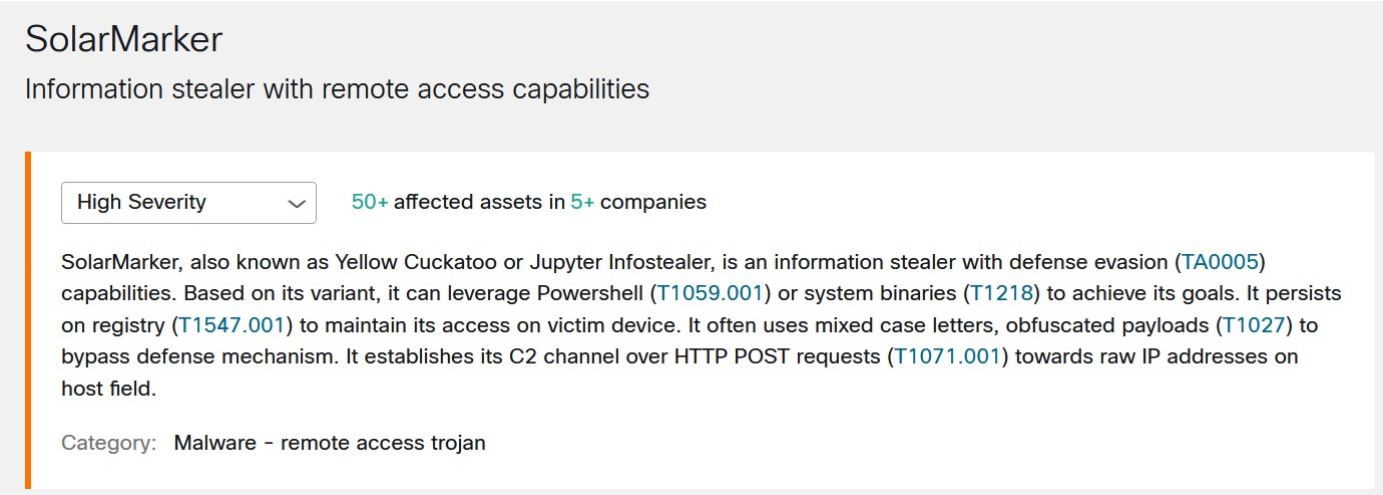
SolarMarker

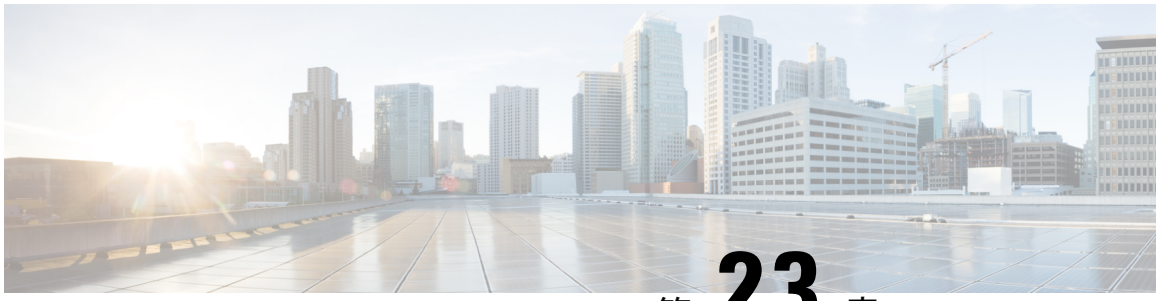
SolarMarker は、Yellow Cuckatoo または Jupyter Infostealer とも呼ばれ、防御を回避（TA0005）できる情報窃取マルウェアです。そのバリアントに基づいて、Powershell（T1059.001）またはシステムバイナリ（T1218）を利用して目標を達成できます。これはレジストリ（T1547.001）に保持され、攻撃対象のデバイスへのアクセスを維持します。多くの場合、大文字と小文字が混在する文字と難読化されたペイロード（T1027）を使用して、防御メカニズムをバイパスし

ます。ホストフィールドの未加工の IP アドレスに対して HTTP POST リクエスト（T1071.001）を介して C2 チャネルを確立します。

お使いの環境で SolarMarker が検出されたかどうかを確認するには、[SolarMarker 脅威の詳細（SolarMarker 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 *30 :*





第 23 章

2022 年 8 月

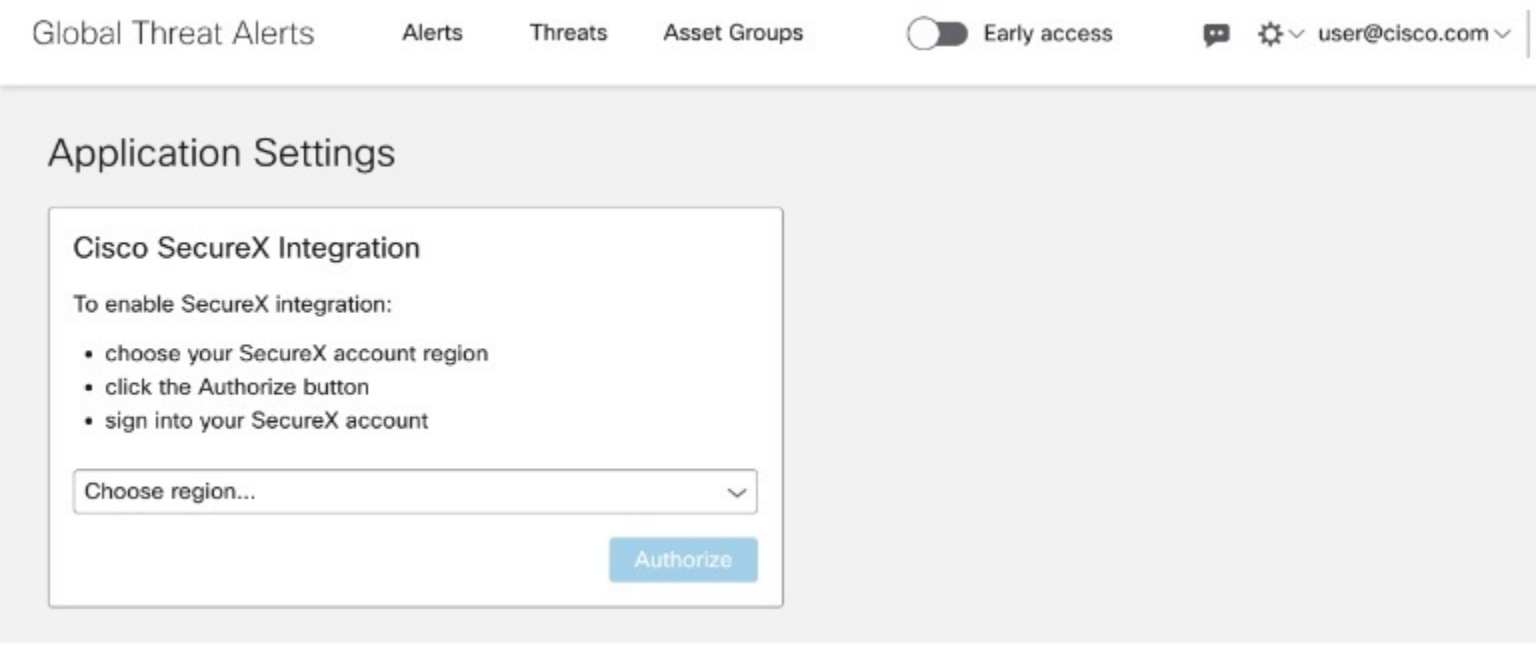
2022 年 8 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

改善されたアラートワークフロー

[早期アクセス（Early access）] でアラートを操作する方法を改善し、グローバル脅威アラートでアラートを SecureX incident manager にプロモートする方法を改善しました。

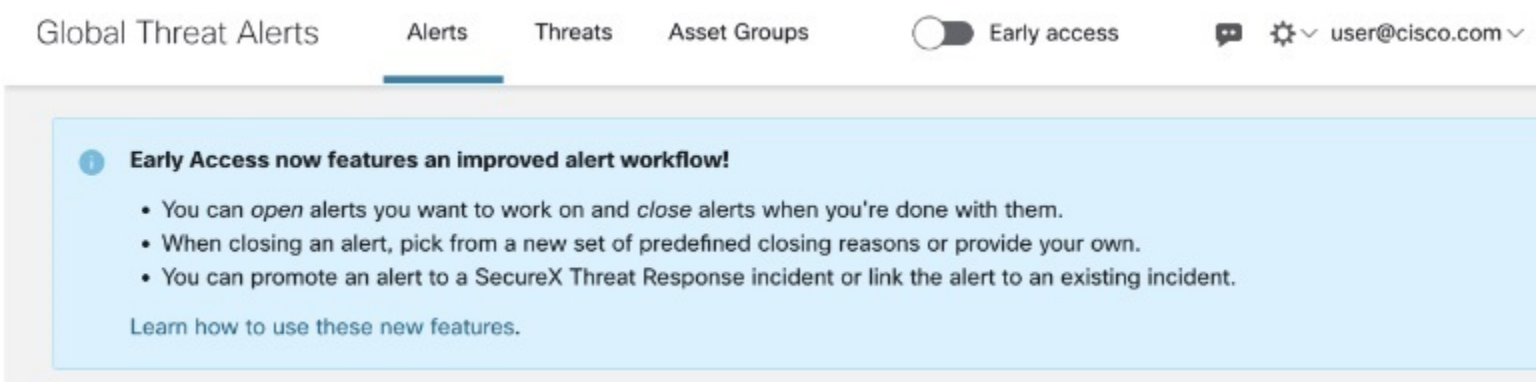
SecureX incident manager との統合のメリットを享受するには、グローバル脅威アラートコンソールの**アプリケーション設定**で SecureX の統合を有効にします。

図 *31* : アプリケーション設定で ***SecureX*** の統合を承認



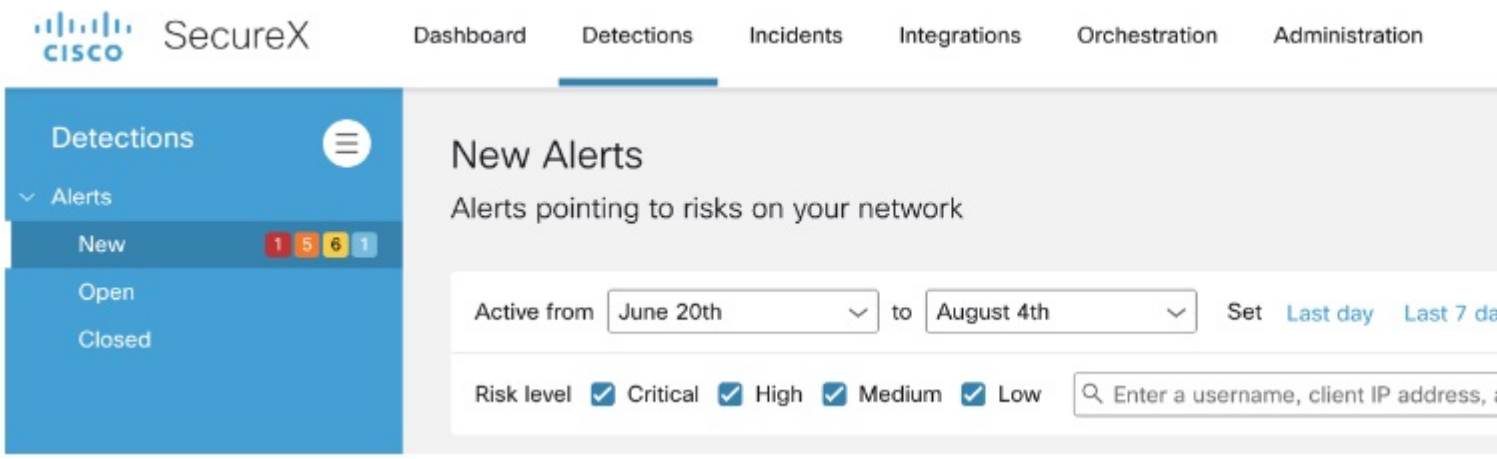
グローバル脅威アラートコンソールのヘッダーで、[早期アクセス（Early access）] をクリックして有効にします。

図 *32* : *[*早期アクセス（***Early access***）*]* をオンにして新機能を有効化



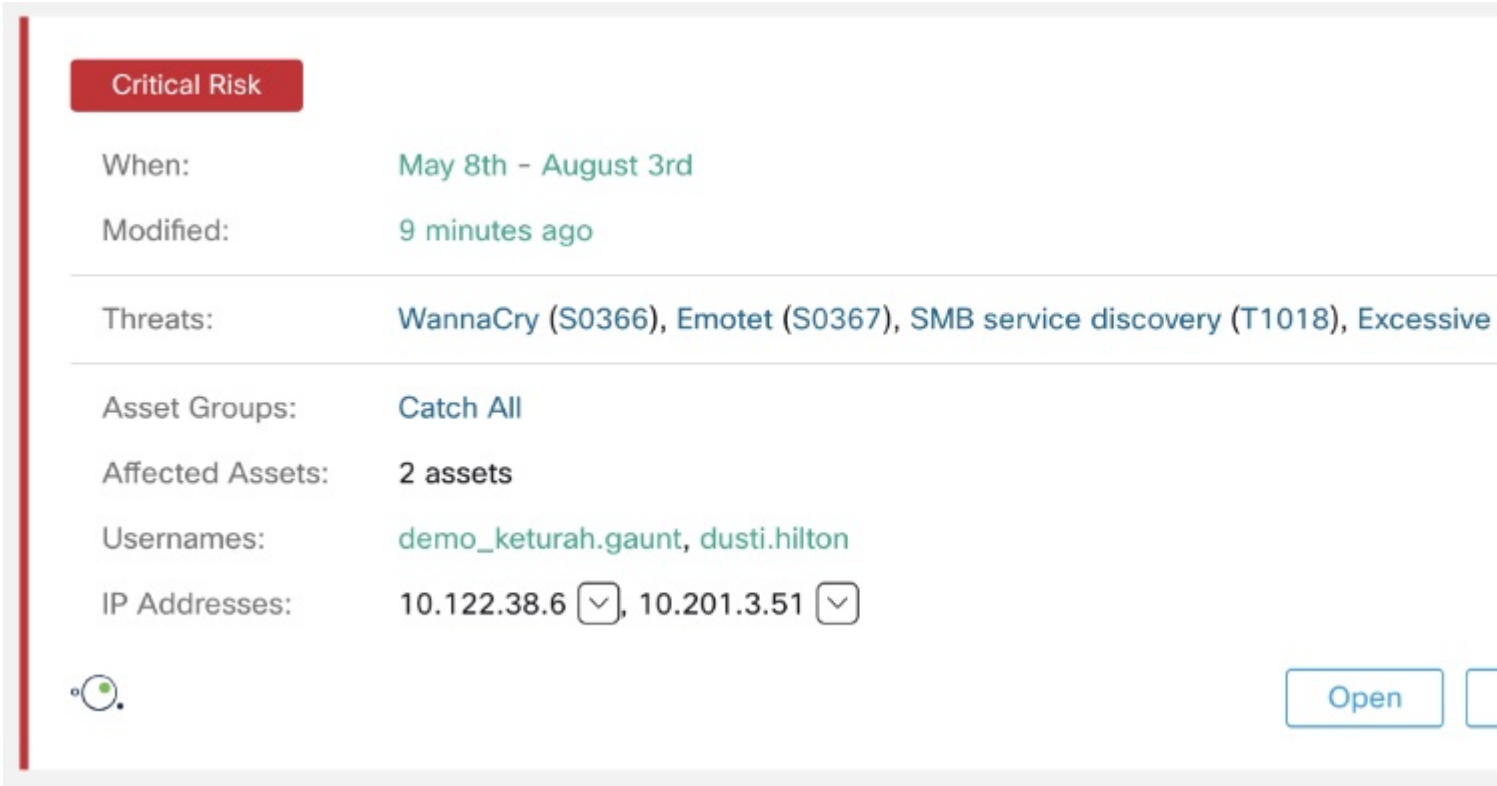
[早期アクセス（Early access）] を有効にすると、アラートは [新規（New）]、[オープン（Open）]、または [終了（Closed）] に分類されます。

図 *33* : *[*新規（*New*）*]*、*[*オープン（*Open*）*]*、*[*終了（*Closed*）*]* のステータスのカテゴリのアラート



[新規（New）] アラートのステータスは、[開く（Open）] または [閉じる（Close）] ボタンを使用して変更できます。

図 *34* : アラートの開閉

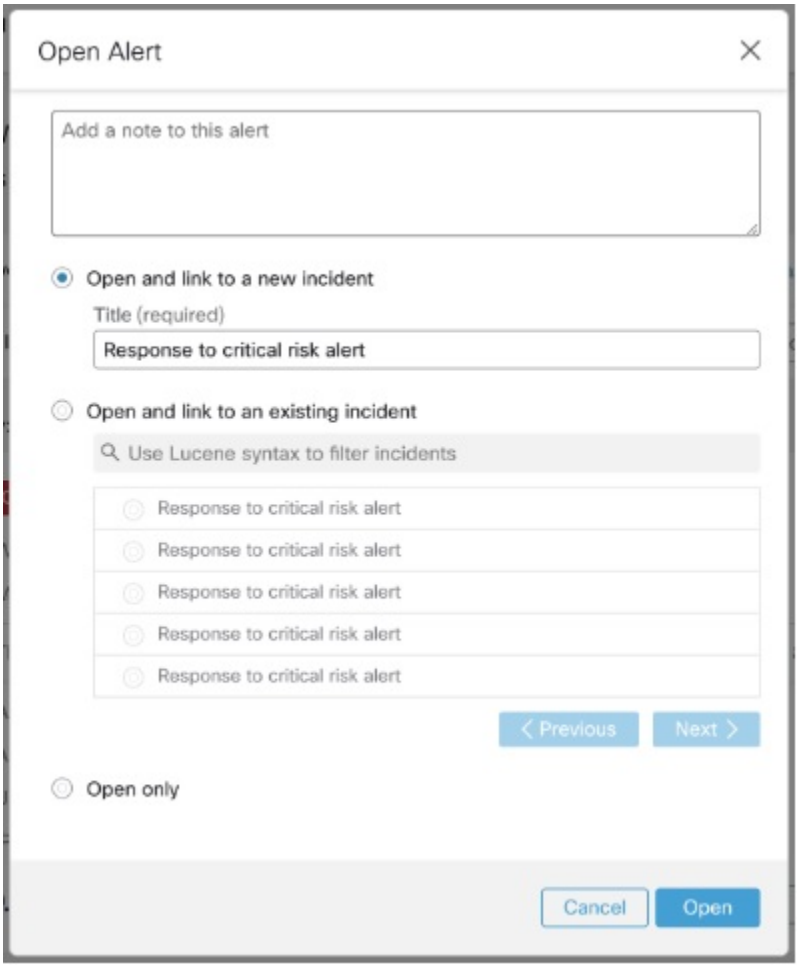


グローバル脅威アラートは、拡張された検出や効率的なアラートトリアージなどのコアコンピテンシーに引き続き重点を置いていますが、現在は SecureX エコシステムとより緊密に統合され、ワンクリックで SecureX のインシデント対応ワークフローへ検出をプロモートします。

アラートが開かれると、以下のオプションが用意されています。

- アラートを開いて新しいインシデントにリンク
- アラートを開いて既存のインシデントにリンク
- 開くのみ

図 *35*：インシデントにリンクするオプション付きのアラートを開く

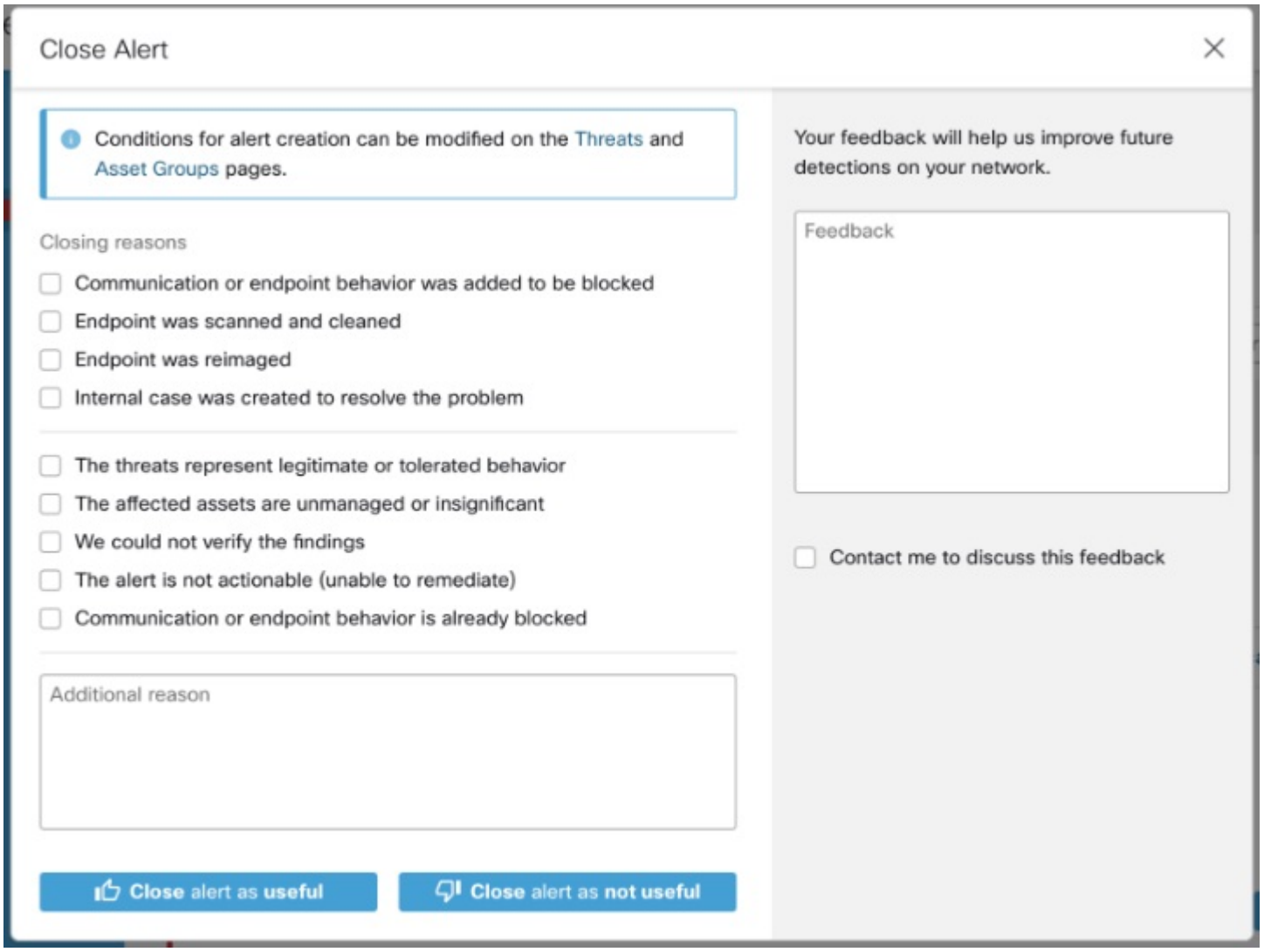


SecureX incident manager では、インシデントには、[概要（Summary）] や、元のアラートからのすべてのセキュリティ [イベント（Events）] と [監視対象（Observables）] などの詳細が含まれています。その後、調査、エンリッチメント、オーケストレーションといった SecureX の機能を使用して、より詳細に調査して対応することができます。

アラートをインシデントとしてプロモートすることが望ましくない場合でも、グローバル脅威アラートコンソールでのみ [開くのみ（Open only）] を実行でき、作業を追跡できます。

どちらの場合も、完了後はアラートを [閉じる（Close）] ことができます。アラートを閉じるときは、定義されている新しい一連の [閉じる理由（Closing reasons）] から選択するか、自身で理由を指定します。

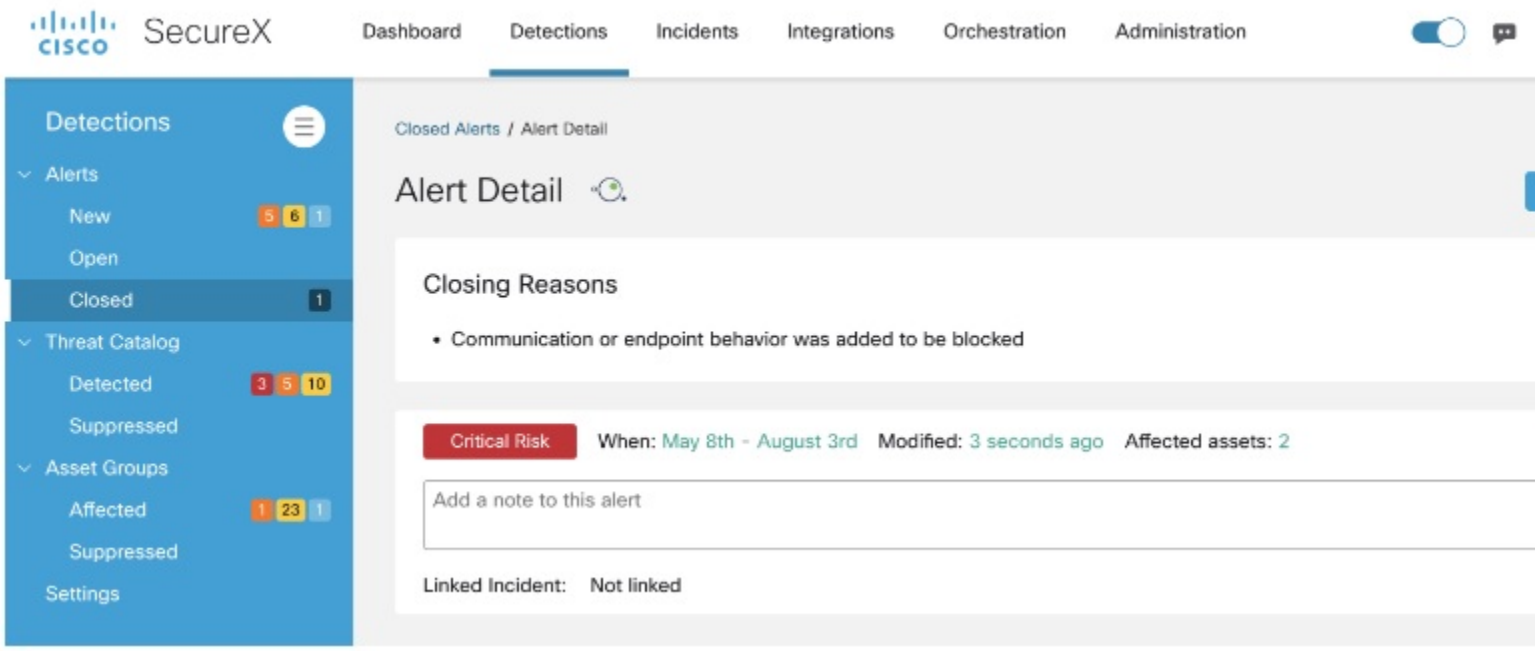
図 *36 :* 閉じる理由を使用してアラートを閉じる



アラートを閉じるときは、[有用（useful）] または [有用でない（not useful）] として閉じることができます。アラートに関する追加のフィードバックをシスコのチームに提供することもできます。貴重なフィードバックは、今後の検出の改善に活用されます。

閉じる理由は、後で参照できるようにアラートの一部として記録されます。

図 *37* : アラートの詳細ページに表示される閉じる理由



閉じたアラートを開くことができます。アラートを再び開くと、閉じる理由はすべて削除されます。また、以前にリンクされたSecureXインシデントへの参照も削除されます。ただし、以前と同じSecureXインシデントであっても、アラートを再度リンクすることを選択できます。

追加の脅威検出

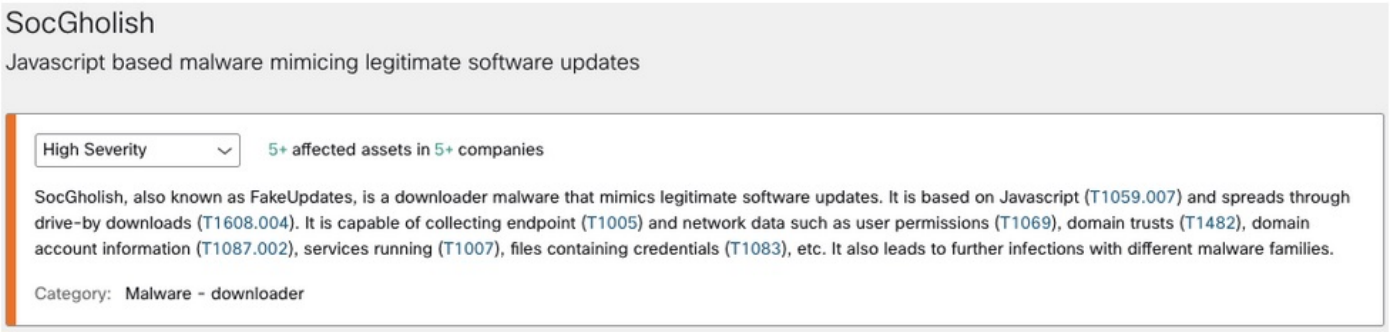
新しい脅威検出、SocGholishをポートフォリオに追加しました。また、既存の脅威検出のインジケーターを更新しました。

SocGholish

FakeUpdates とも呼ばれる SocGholish は、正規のソフトウェアアップデートを模倣するダウンローダーマルウェアです。これは Javascript（T1059.007）に基づいており、ドライブバイダウンロード（T1608.004）を介して展開します。エンドポイント（T1005）と、ユーザー許可（T1069）、ドメイン信頼（T1482）、ドメインアカウント情報（T1087.002）、実行中のサービス（T1007）、資格情報を含むファイル（T1083）などのネットワークデータを収集できます。また、異なるマルウェアファミリによるさらなる感染につながります。

お使いの環境で SocGholish が検出されたかどうかを確認するには、[SocGholish脅威の詳細（SocGholish Threat Detail）]https://cta.eu.amp.cisco.com/ui/threats/74536f03-a984-4a28-8dfa-a415f2d56cc5 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 *38 :*


SocGholish
Javascript based malware mimicing legitimate software updates
High Severity
5+ affected assets in 5+ companies
SocGholish, also known as FakeUpdates, is a downloader malware that mimics legitimate software updates. It is based on Javascript (T1059.007) and spreads through drive-by downloads (T1608.004). It is capable of collecting endpoint (T1005) and network data such as user permissions (T1069), domain trusts (T1482), domain account information (T1087.002), services running (T1007), files containing credentials (T1083), etc. It also leads to further infections with different malware families.
Category: Malware - downloader

第 24 章

2022 年 7 月

2022 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。

SSO を CCI に移行

カスタマーエクスペリエンスを向上させるために、シングルサインオンが Cisco Customer Identity（CCI）ポータルに移行されました。引き続き [Cisco SSO] をクリックし、[id.cisco.com] で電子メールとパスワードを入力してログインします。

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。

- Conti
- REvil

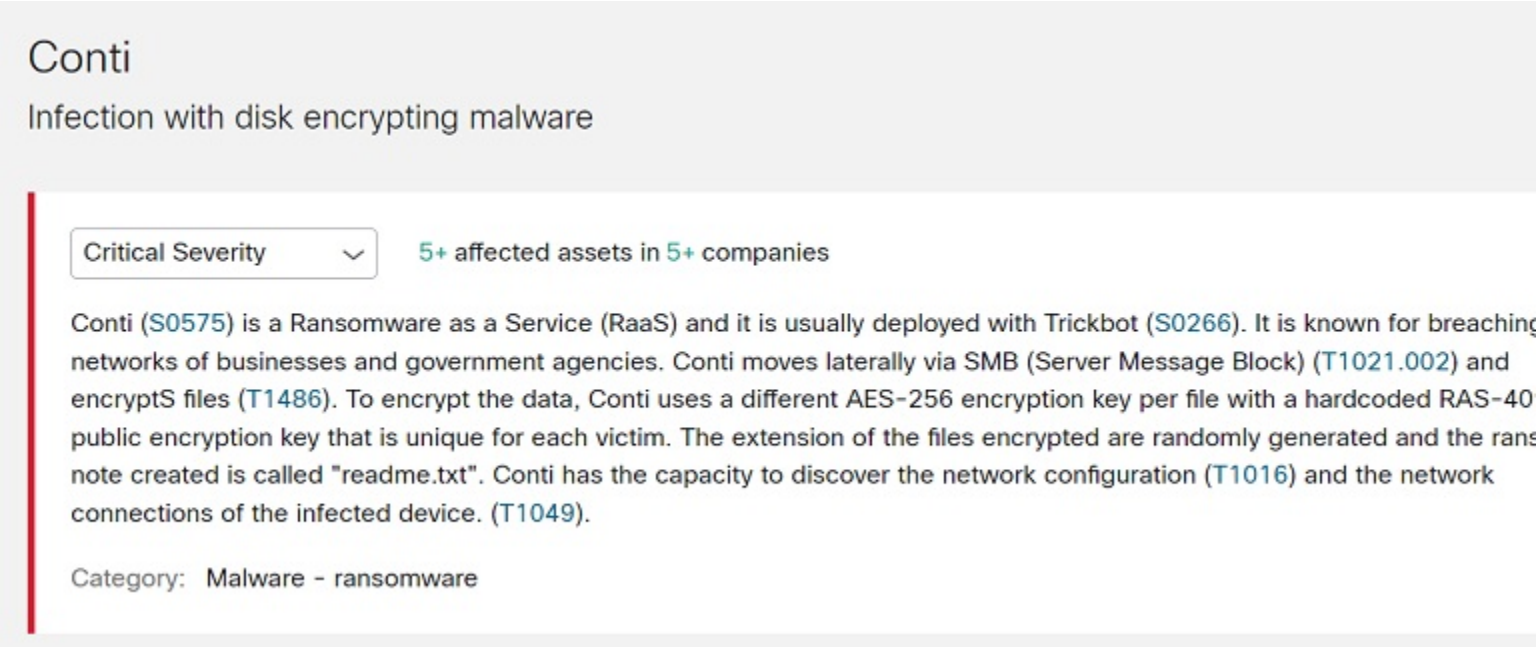
また、既存の脅威検出のインジケーターも更新しました。

Conti

Conti（S0575）は、通常 Trickbot（S0266）とともに導入されるサービスとしてのランサムウェア（RaaS）です。ビジネスや政府機関のネットワークに侵入することで知られています。Conti は、SMB（サーバーメッセージブロック）（T1021.002）およびファイルの暗号化（T1486）を使用して水平方向に移動します。データを暗号化するために、Conti はファイルごとに異なる AES-256 暗号化キーと攻撃対象ごとに固有のハードコーディングされた RAS-4096 公開暗号化キーを使用します。暗号化されたファイルの拡張子はランダムに生成され、作成される身代金要求メッセージは「readme.txt」と呼ばれます。Conti には、感染したデバイス（T1049）のネットワーク設定（T1016）とネットワーク接続を発見する能力があります。

お使いの環境で Conti が検出されたかどうかを確認するには、[Conti脅威の詳細（Conti 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 *39 :*

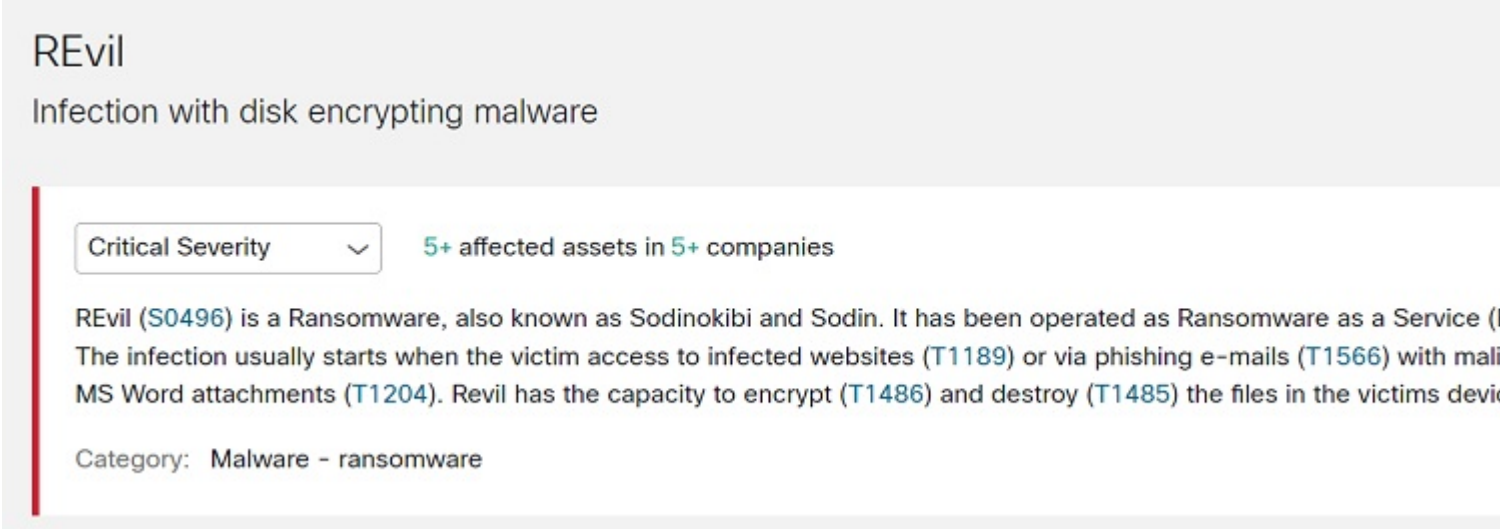


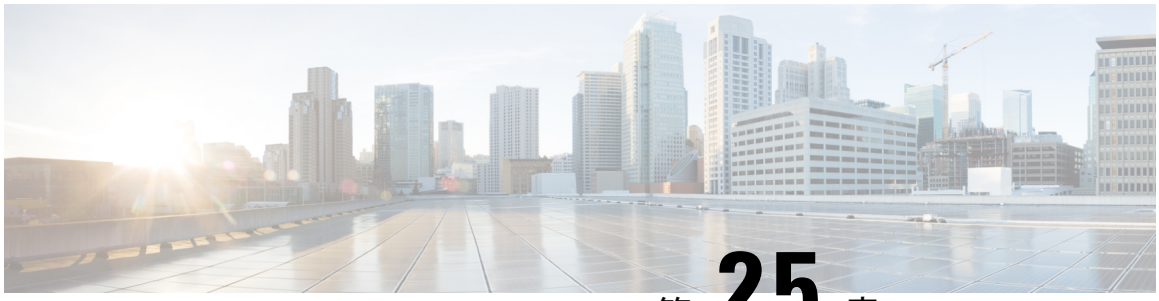
REvil

REvil（S0496）は、Sodinokibi および Sodin としても知られるサービスとしてのランサムウェア（RaaS）です。感染は通常、攻撃対象が感染した Web サイト（T1189）または悪意のある MS Word 添付ファイル（T1204）を含むフィッシングメール（T1566）にアクセスしたときに始まります。REvil には、攻撃対象のデバイス上のファイルを暗号化（T1486）および破壊（T1485）する能力があります。

お使いの環境で REvil が検出されたかどうかを確認するには、[REvil脅威の詳細（REvil 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 *40 :*


REvil
Infection with disk encrypting malware
Critical Severity
5+ affected assets in 5+ companies
REvil (S0496) is a Ransomware, also known as Sodinokibi and Sodin. It has been operated as Ransomware as a Service (
The infection usually starts when the victim access to infected websites (T1189) or via phishing e-mails (T1566) with mali
MS Word attachments (T1204). Revil has the capacity to encrypt (T1486) and destroy (T1485) the files in the victims devi
Category: Malware - ransomware



第 25 章

2022 年 6 月

2022 年 6 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 （85 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。

- AutoKMS ハックツール
- Raspberry Robin
- UNC2447 アクティビティ

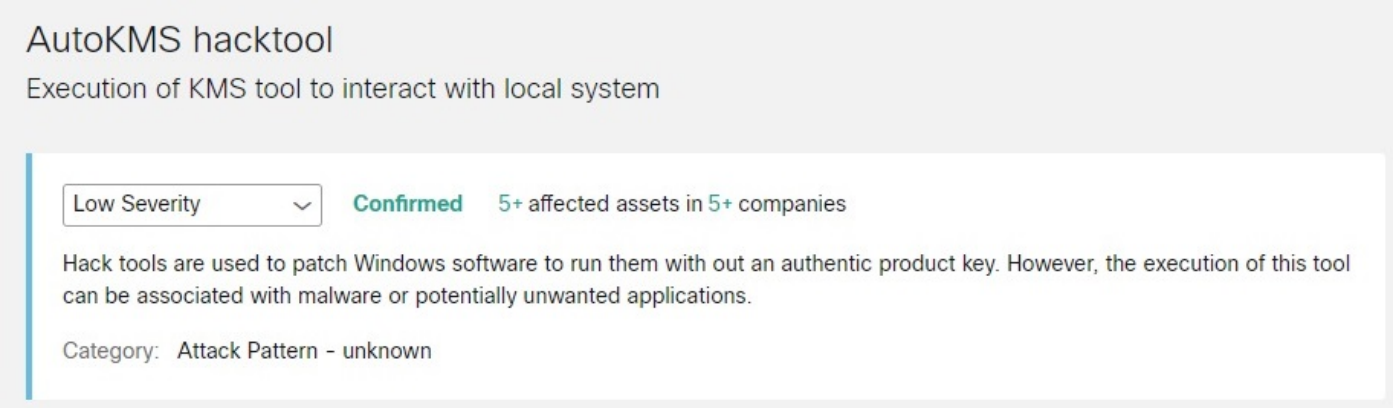
また、既存の脅威検出のインジケーターも更新しました。

AutoKMS ハックツール

ハックツールは、Windows ソフトウェアにパッチを適用して製品認証キーなしで実行するために使用されます。しかし、このツールの実行は、マルウェアや望ましくない可能性のあるアプリケーションに関連付けられている可能性があります。

お使いの環境で AutoKMS ハックツールが検出されたかどうかを確認するには、[AutoKMSハックツール脅威の詳細（AutoKMS HackTool 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 *41 :*



Raspberry Robin

Raspberry Robin は、外部ドライブから .lnk（T1204.002）ファイルを介してマシンに感染し、msiexec.exe（T1218.007）で実際のペイロードをダウンロードし、rundll32.exe（T1218.011）でコードを実行し、TOR 接続（S0183）を介して C2 を確立します。そのインフラストラクチャは、侵害された QNAP デバイスに基づくものです。

お使いの環境で Raspberry Robin が検出されたかどうかを確認するには、[Raspberry Robin脅威の詳細（Raspberry Robin 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 *42 :*

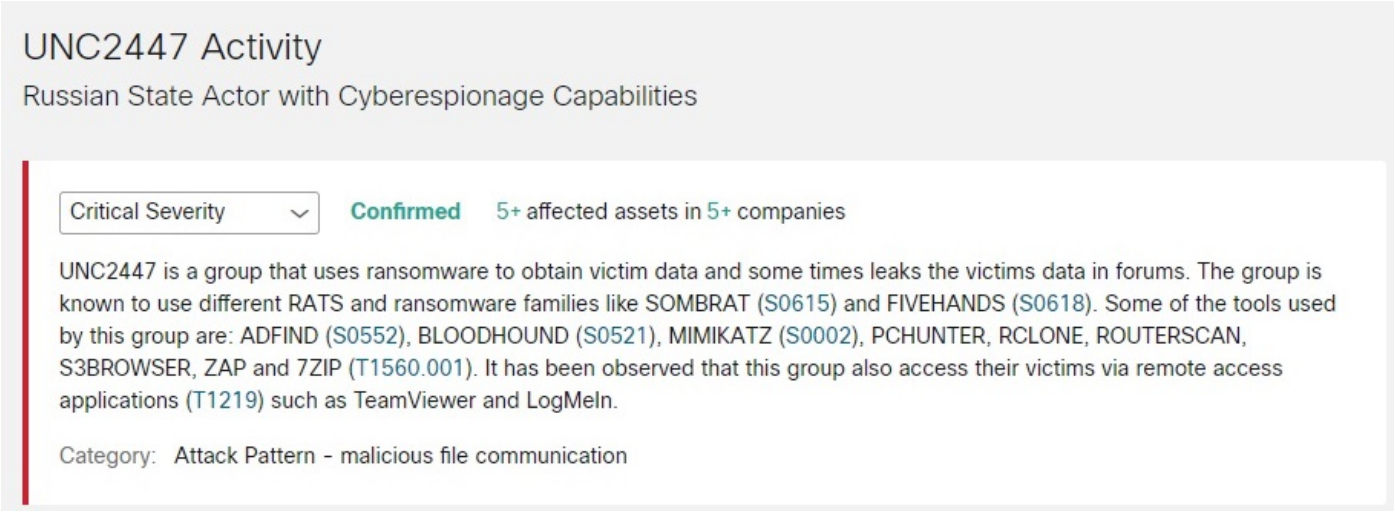
UNC2447 アクティビティ

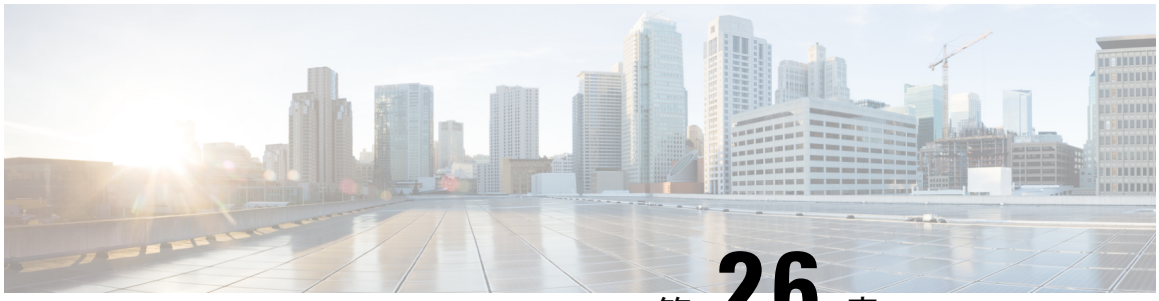
UNC2447 は、ランサムウェアを使用してデータを取得し、フォーラムで被害者のデータを漏洩する可能性があるグループです。このグループは、さまざまなRATSと、SOMBRAT（S0615）や FIVEHANDS（S0618）などのランサムウェアファミリを使用することが知られています。ADFIND（S0552）、BLOODHOUND（S0521）、MIMIKATZ（S0002）、PCHUNTER、RCLONE、ROUTERSCAN、S3BROWSER、ZAP、7ZIP（T1560.001）などのツールがこのグ

ループに使用されます。また、このグループは、TeamViewer や LogMeIn などのリモート アクセス アプリケーション（T1219）も使用します。

お使いの環境でUNC2447アクティビティが検出されたかどうかを確認するには、[UNC2447アクティビティ脅威の詳細（UNC2447 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。

図 *43 :*





第 26 章

2022 年 5 月

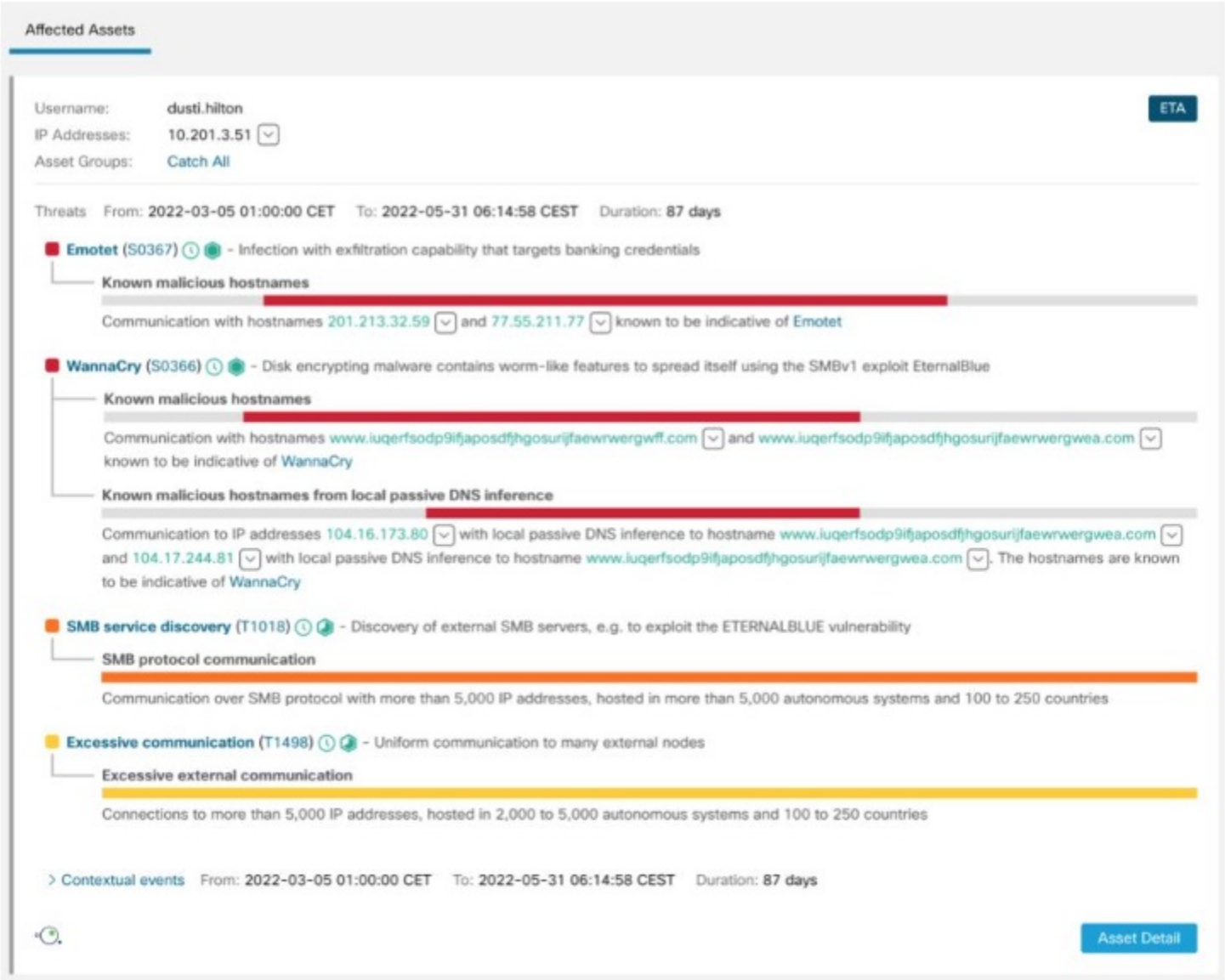
2022 年 5 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

- アラート詳細の拡張表示 （89 ページ）

アラート詳細の拡張表示

[アラート詳細（Alert detail）] ページを強化し、[影響を受けるアセット（Affected Assets）] に関する詳細情報を表示するようにしました。影響を受けるアセットにはそれぞれそのアセットで行われたすべての脅威検出をリストする新しい[脅威（Threats）]セクションがあり、すべての有害となるセキュリティイベントが含まれています。

図 *44 :*



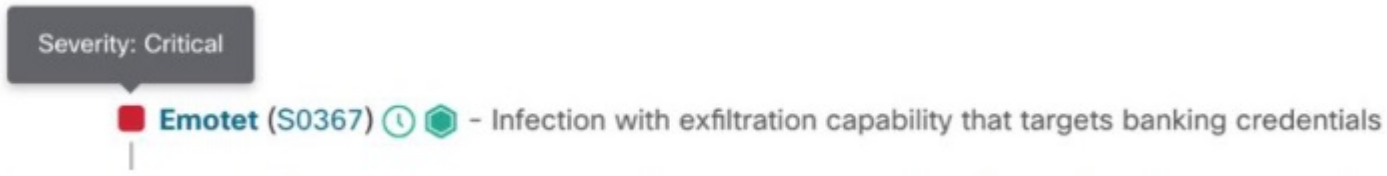
[脅威（Threats）]セクションの上部には、検出されたすべての脅威の合計観測期間と、特定のアセットでのそれらの有害となるセキュリティイベントが表示されます。

図 *45 :*

それぞれの脅威検出には、その名前、MITRE リンク、説明、および以下のものが表示されます。

- 重大度

図 *46 :*

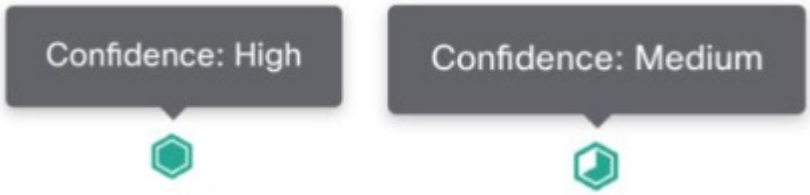


- 観測期間

図 *47 :*

- 信頼度

図 *48 :*



それぞれの脅威検出は、下にあるセキュリティイベントによって裏付けられています。イベントの多くには、イベントの作成につながった証拠を提供する豊富なセキュリティアノテーションが含まれています。

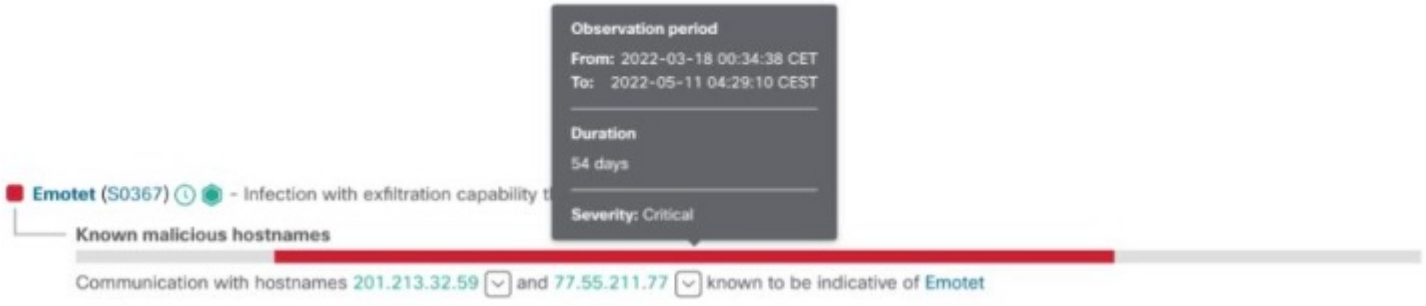
図 *49 :*

イベントアノテーションには、他のシスコのセキュリティ製品にピボットして、監視対象に関する追加情報とインテリジェンスを取り込めるドロップダウンメニューが含まれている場合もあります。

図 *50 :*

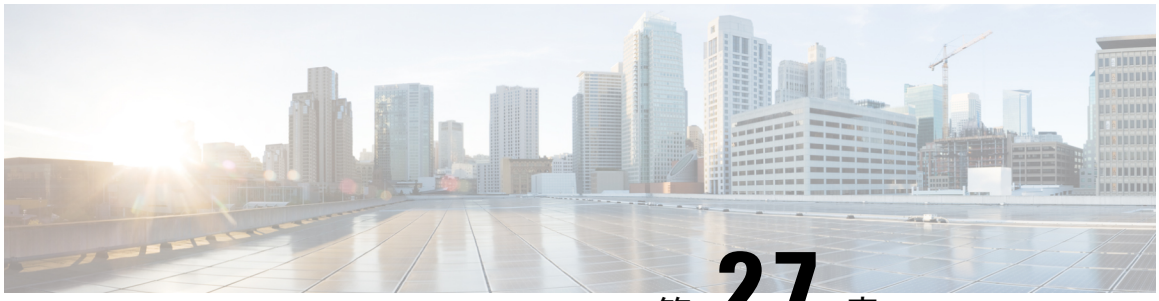
それぞれのセキュリティイベントには、[脅威（Threats）]の合計観測期間のコンテキスト内での動作のタイミングと発生を示すタイムラインが含まれています。

図 *51 :*



新しい [コンテキストイベント（Contextual events）] セクションを展開して、アセット上で起こったことに関する追加のコンテキストを提供できる、より多くのイベントを表示することができます。

図 *52 :*



第 27 章

2022 年 4 月

2022 年 4 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。

• MITRE ATT&CK® との調整 （95 ページ）

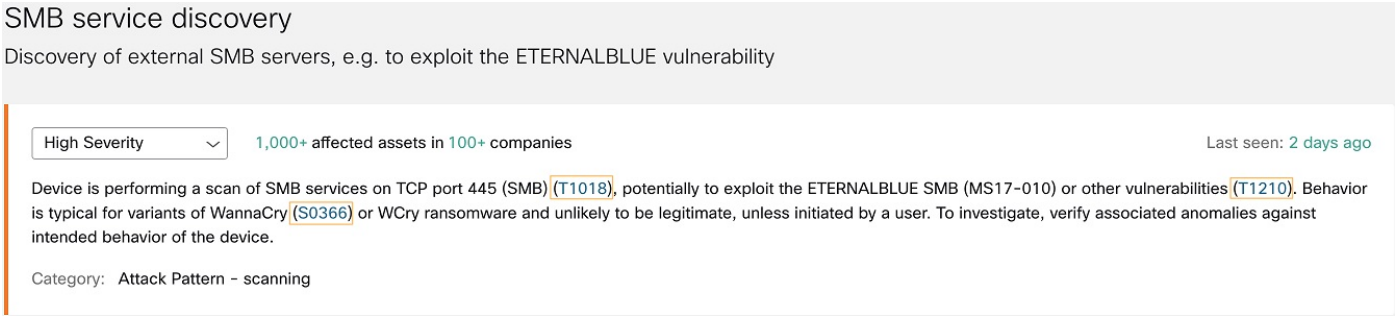
MITRE ATT&CK® との調整

グローバル脅威アラートの脅威インテリジェンスレコードは、MITRE ATT&CK® フレームワークに関して調整されています。

- 必要に応じて、ATT&CK フレームワークからの命名が直接使用されます。
- グローバル脅威アラートの脅威インテリジェンスは、関連する ATT&CK の戦術、テクニック、およびソフトウェアエントリへの参照を提供します。

図 *53 :*

図 *54 :*



これらの改善により、インシデント対応の既存の標準操作手順とのプロセス統合が容易になり、新しいアナリストの学習曲線が短縮されます。

第 28 章

2022 年 3 月

2022 年 3 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 （97 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。

- Cyclops Blink
- FormBook
- Gamaredon
- MuddyWater

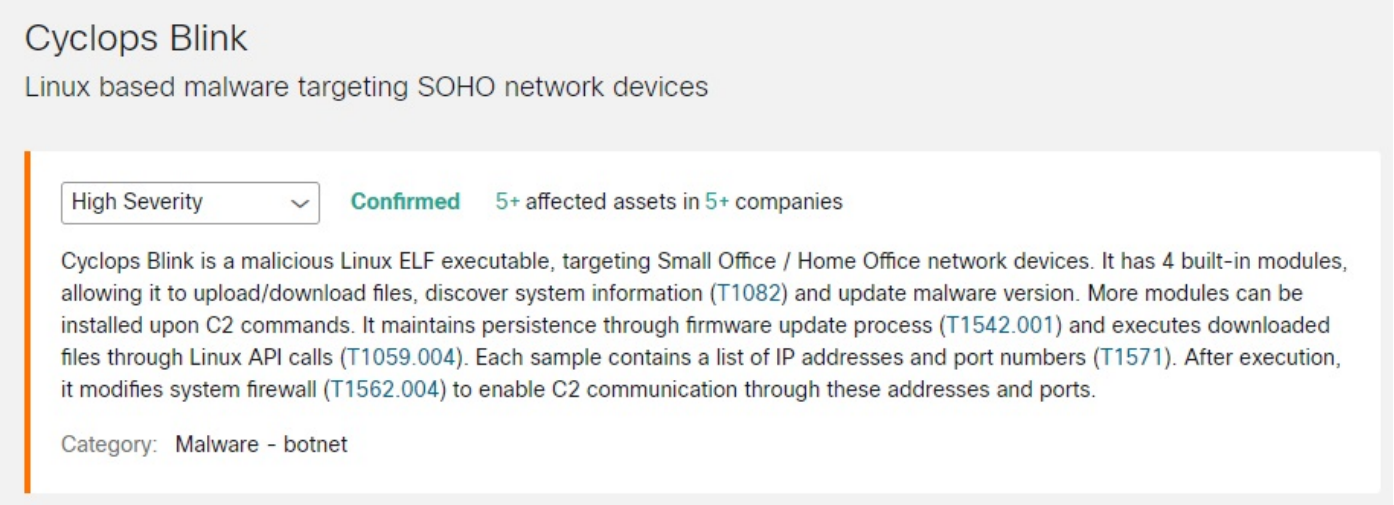
低リスクの脅威検出も多数強化されています。

Cyclops Blink

Cyclops Blink は、悪意のある Linux ELF 実行ファイルであり、スモールオフィス、ホームオフィスのネットワークデバイスをターゲットにしています。4つの組み込みモジュールがあり、ファイルのアップロードとダウンロード、システム情報（T1082）の発見、マルウェアのバージョンの更新を行うことができます。C2 コマンドを使用して、さらに多くのモジュールをインストールできます。ファームウェア更新プロセス（T1542.001）を通じて永続性を維持し、Linux API コール（T1059.004）を通じてダウンロードされたファイルを実行します。各サンプルには、IP アドレスとポート番号（T1571）のリストが含まれています。実行後、システムのファイアウォール（T1562.004）を変更して、これらの IP アドレスとポートを介した C2 通信を有効にします。

お使いの環境で Cyclops Blink が検出されたかどうかを確認するには、[Cyclops Blink 脅威の詳細（Cyclops Blink 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 *55 :*

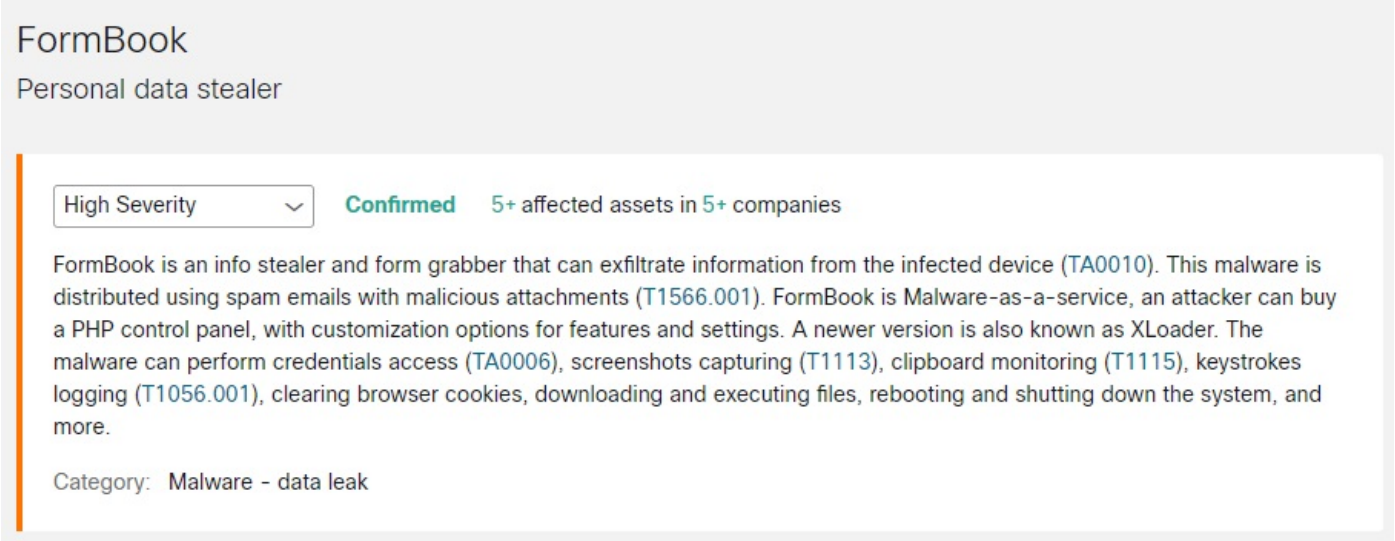


FormBook

FormBook は、感染したデバイス（TA0010）から情報を盗み出す情報窃取およびフォームグラバーです。このマルウェアは、悪意のある添付ファイル（T1566.001）を含むスパムメールを使用して配布されます。FormBook はサービスとしてのマルウェアであり、攻撃者は機能と設定のカスタマイズオプションを備えた PHP コントロールパネルを購入できます。新しいバージョンは XLoader とも呼ばれます。このマルウェアは、ログイン情報（TA0006）へのアクセス、スクリーンショット（T1113）のキャプチャ、クリップボード（T1115）の監視、キーストローク（T1056.001）のログ、ブラウザ Cookie のクリア、ファイルのダウンロードと実行、システムの再起動とシャットダウンなどを行うことができます。

お使いの環境で FormBook が検出されたかどうかを確認するには、[FormBook 脅威の詳細（FormBook 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 *56 :*



Gamaredon

Primitive Bear としても知られる Gamaredon は、サイバースパイ活動の目的で政府組織を標的にすることが多い、国家レベルの攻撃者です。ロシアとウクライナの間の緊張が高まった後、グループの活動が活発になりました。Gamaredon は、攻撃の第 1 段階として、スピアフィッシング（T1566.001）を介して配布された悪意のある Office ファイル（T1204.002）を利用することがよくあります。彼らは、次の段階で PowerPunch と呼ばれる Powershell（T1059.001）ビーコンを使用して、マルウェア（T1204.002）をダウンロードして実行することが知られています。Pterodo（S0147）と QuietSieve は、情報（TA0010）を盗んだりその他のさまざまなアクションを目的としてよく導入されるマルウェアファミリです。

お使いの環境で Gamaredon アクティビティが検出されたかどうかを確認するには、[Gamaredon アクティビティの脅威の詳細（Gamaredon 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。

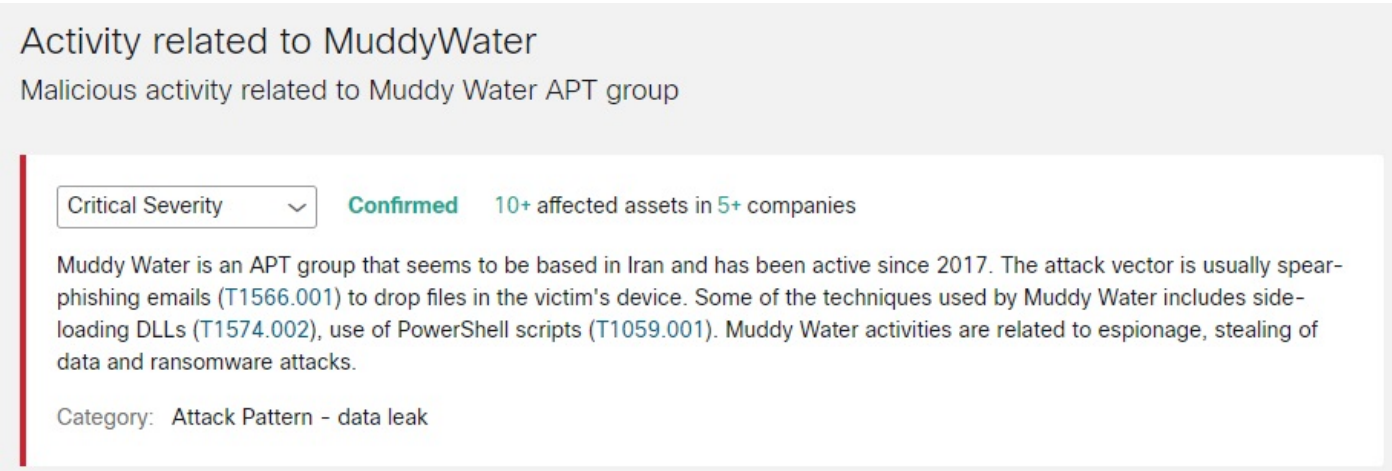
図 *57 :*

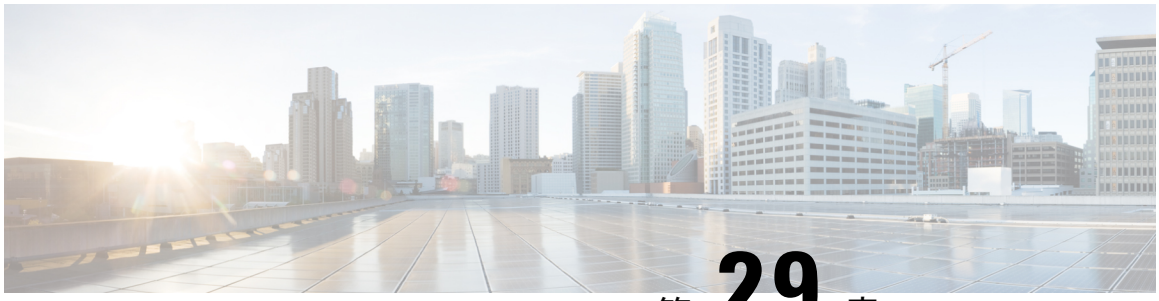
MuddyWater

MuddyWaterは、イランを拠点としていると思われる高度で連続的な脅威（APT）グループで、2017年から活動しています。攻撃ベクトルは通常、攻撃対象のデバイスにファイルをドロップするスピアフィッシングメール（T1566.001）です。MuddyWater で使用されるテクニックには、サイドローディング DLL（T1574.002）や PowerShell スクリプト（T1059.001）の使用などがあります。MuddyWater の活動は、スパイ活動、データの盗難、ランサムウェア攻撃に関連しています。

お使いの環境でMuddyWaterアクティビティが検出されたかどうかを確認するには、[MuddyWaterアクティビティの脅威の詳細（MuddyWater Activity Threat Detail）] をクリックして、グローバル脅威アラートでその詳細を表示します。

図 *58 :*





第 29 章

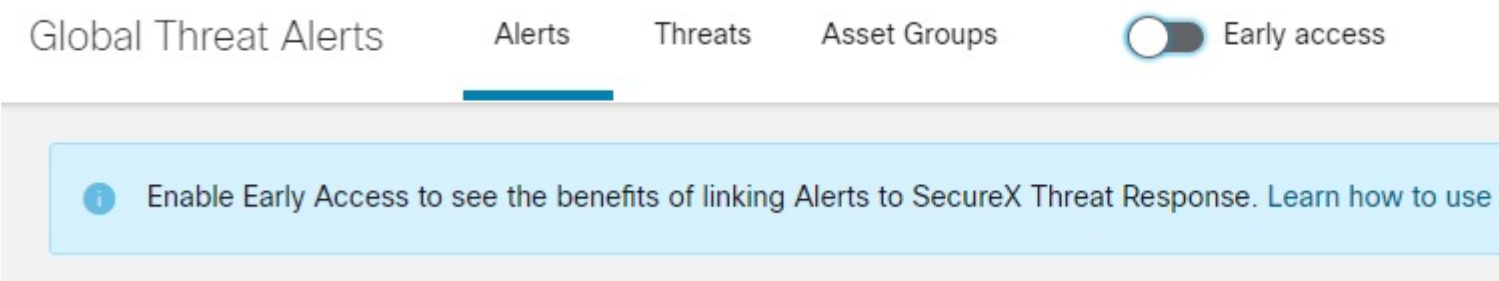
2022 年 1 月

2022 年 1 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。

SecureX Incident Manager へのアラートプロモーション

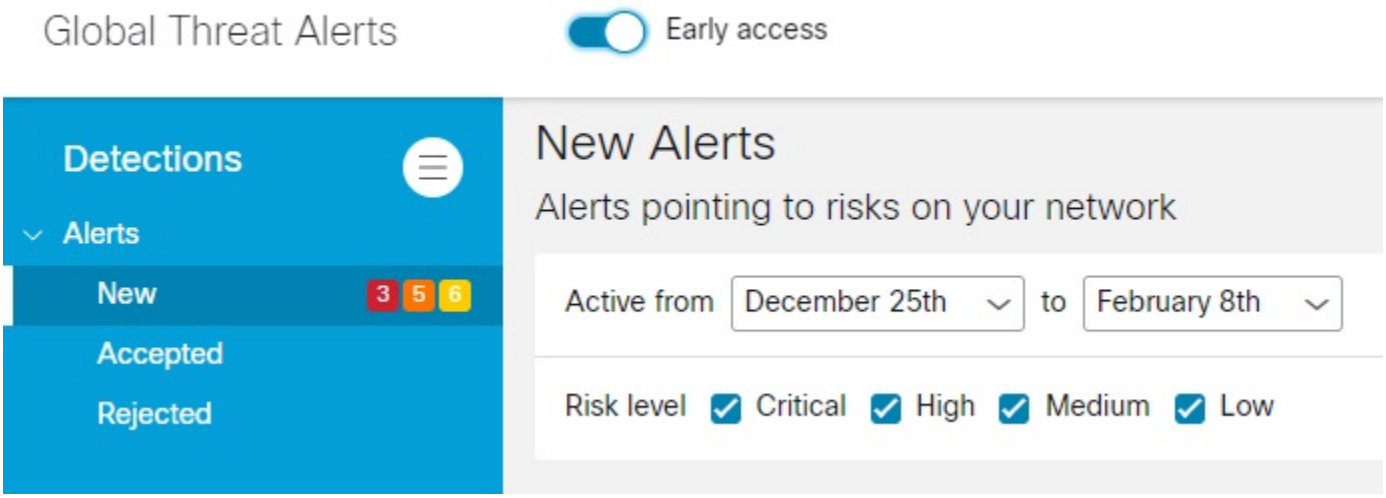
SecureX Incident Manager へグローバル脅威アラートでアラートをプロモートする機能を追加しました。この機能を有効にするには、グローバル脅威アラートコンソールのヘッダーで [早期アクセス（Early access）] を有効にします。

図 *59 : [*早期アクセス（*Early access***）*]* をクリックして新機能を有効化**



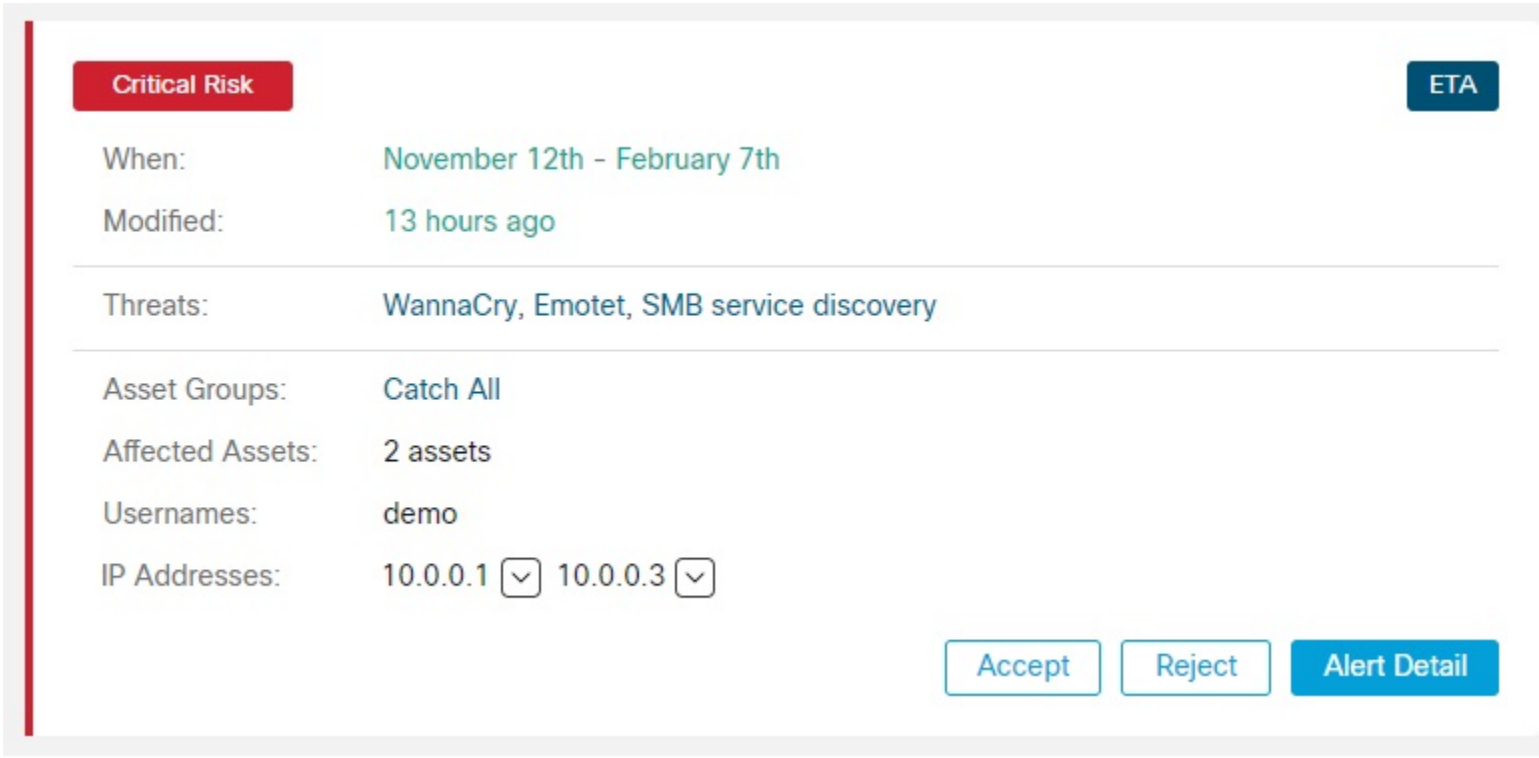
有効にすると、SecureX Incident Manager は、グローバル脅威アラートの既存のワークフローを置き換えます。アラートは、[新規（New）]、[承認（Accepted）]、または [拒否（Rejected）] に分類されます。

図 *60 : SecureX Incident Manager* のアラート



[承認（Accepted）] または [拒否（Rejected）] ボタンを使用して、新しいアラートをいずれかの状態に移動できます。

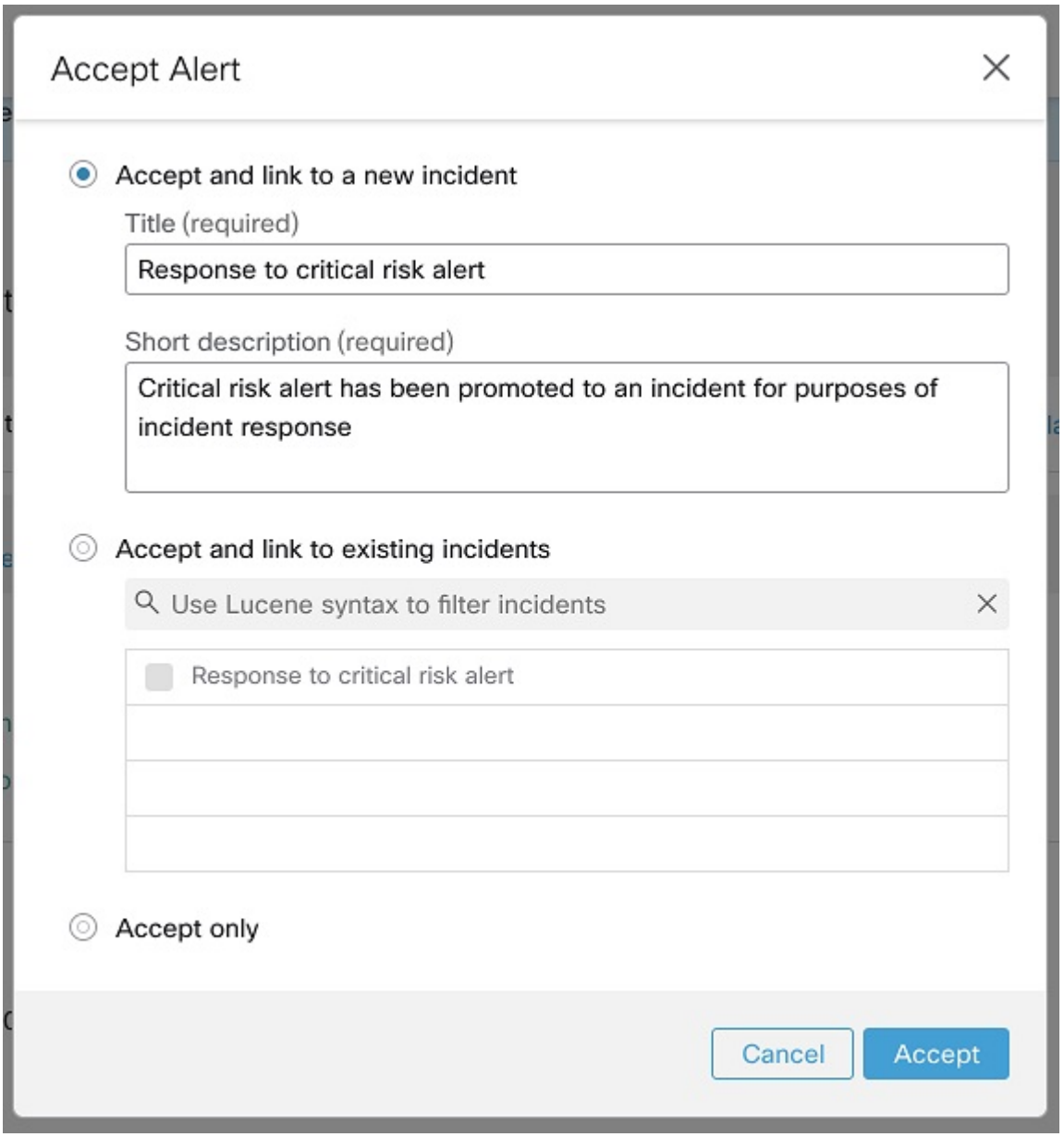
図 *61 :* アラートの承認または拒否



グローバル脅威アラートは、拡張された検出や効率的なアラートトリアージなどのコアコンピテンシーに引き続き重点を置いていますが、現在はSecureXエコシステムとより緊密に統合され、ワンクリックで SecureX のインシデント対応ワークフローへ検出をプロモートします。

アラートを承認すると、SecureX Incident Manager の既存または新しいインシデントにリンクできます。

図 *62*：インシデントにリンクするオプションでアラートを承認



SecureX incident manager では、インシデントには、[概要（Summary）] や、元のアラートからのすべてのセキュリティ [イベント（Events）] と [監視対象（Observables）] などの詳細が含まれています。その後、調査、エンリッチメント、オーケストレーションといった SecureX の機能を使用して、より詳細に調査して対応することができます。

図 *63 :* インシデントサマリーの例

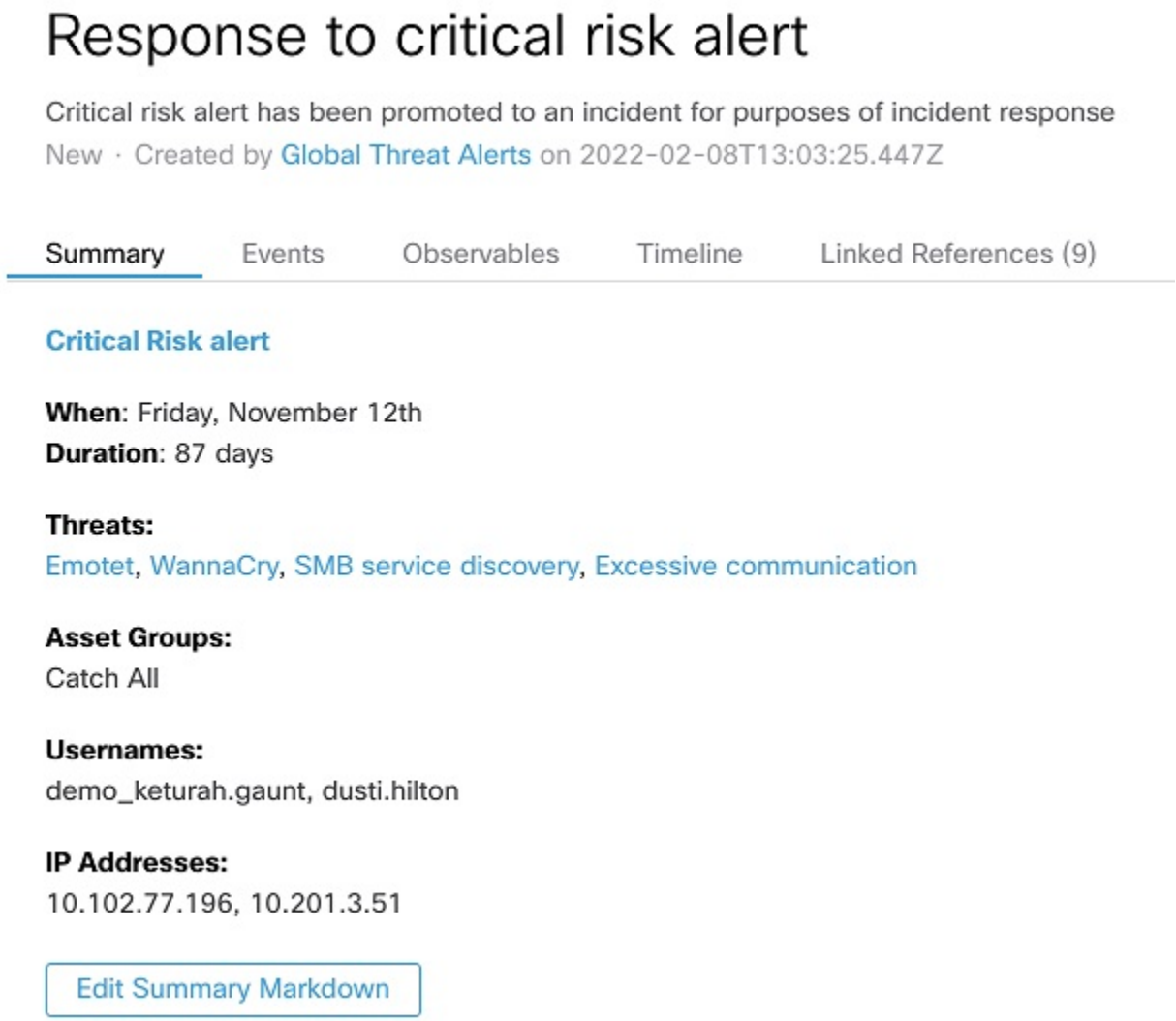
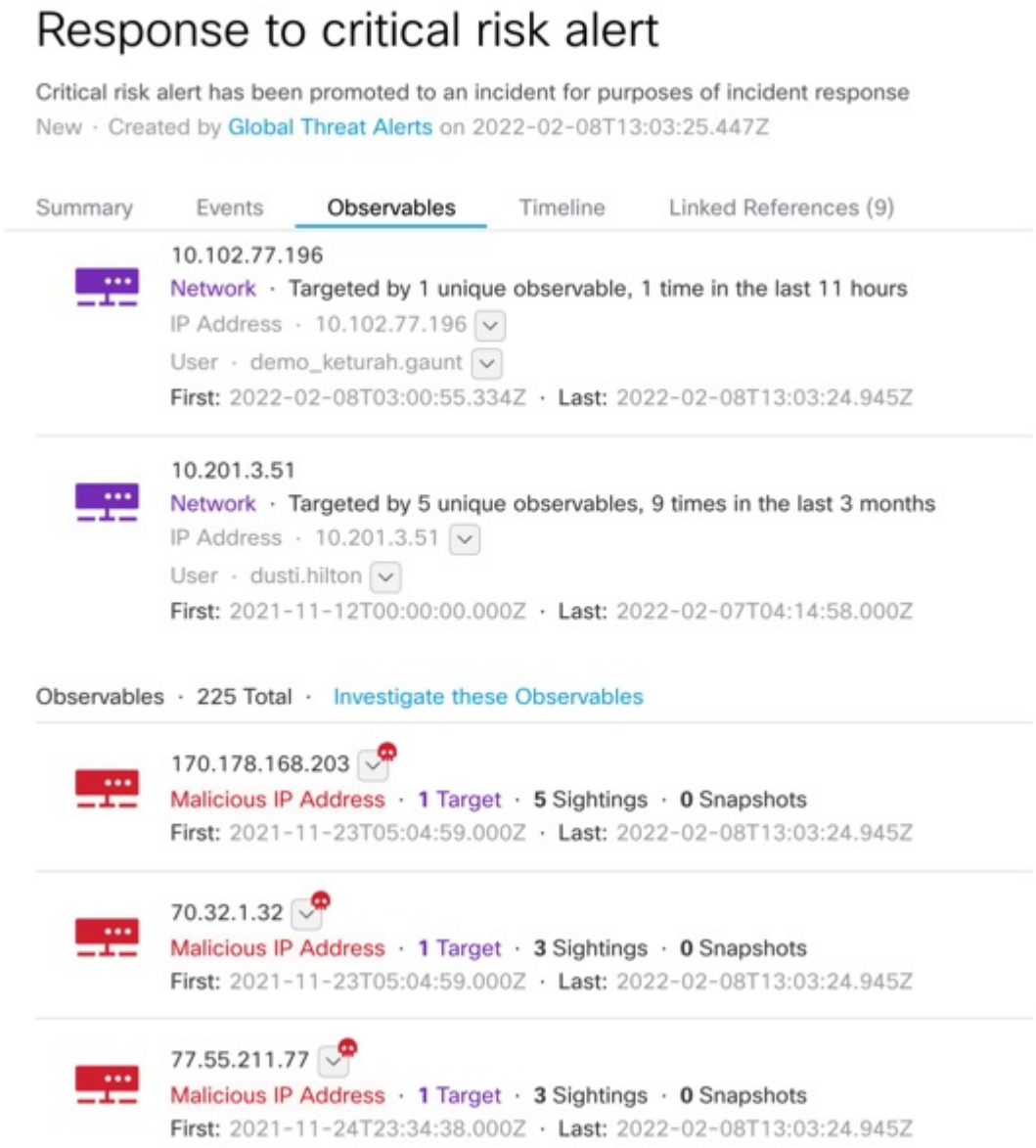
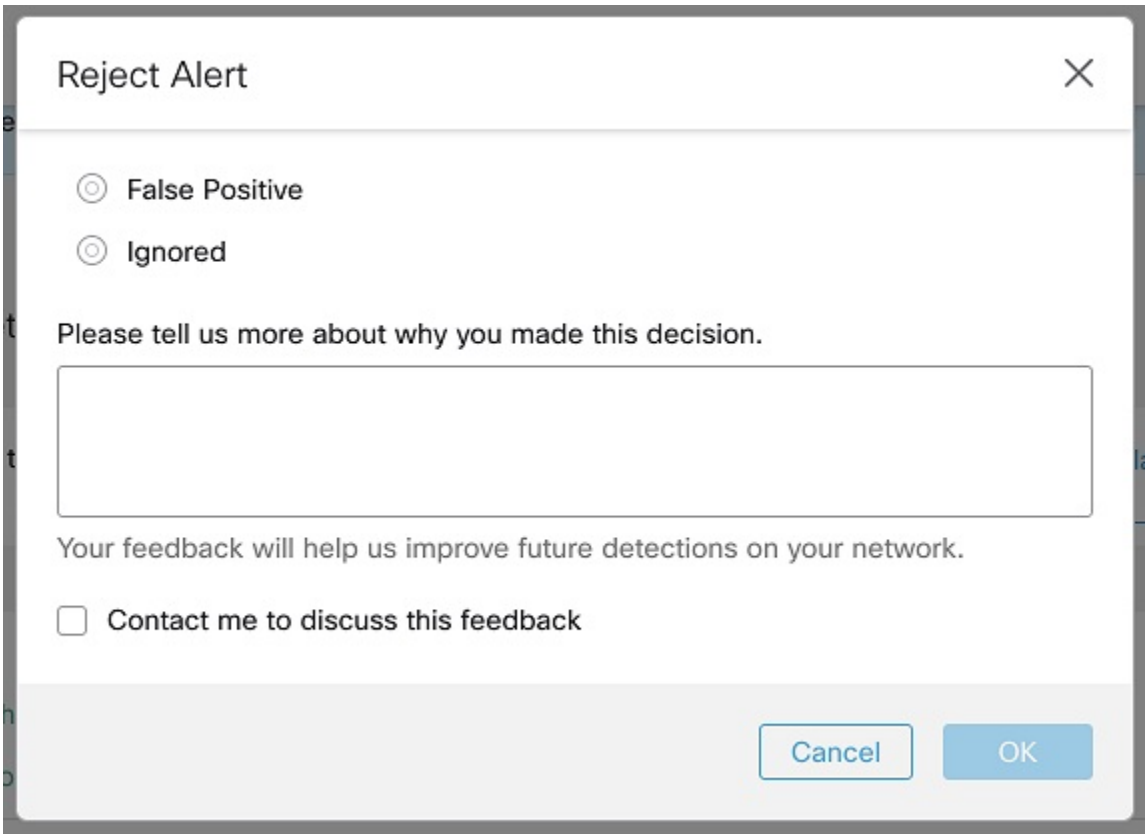


図 *64* : インシデントオブザーバブルの例



アラートをインシデントとしてプロモートすることが望ましくない場合は、拒否できます。この場合、アラートを拒否した理由をシスコのチームにフィードバックすることもできます。貴重なフィードバックは、ネットワークでの今後の検出を改善に活用されます。

図 *65 :* アラートを拒否してフィードバックを提供



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。

- IcedID
- Lemon Duck

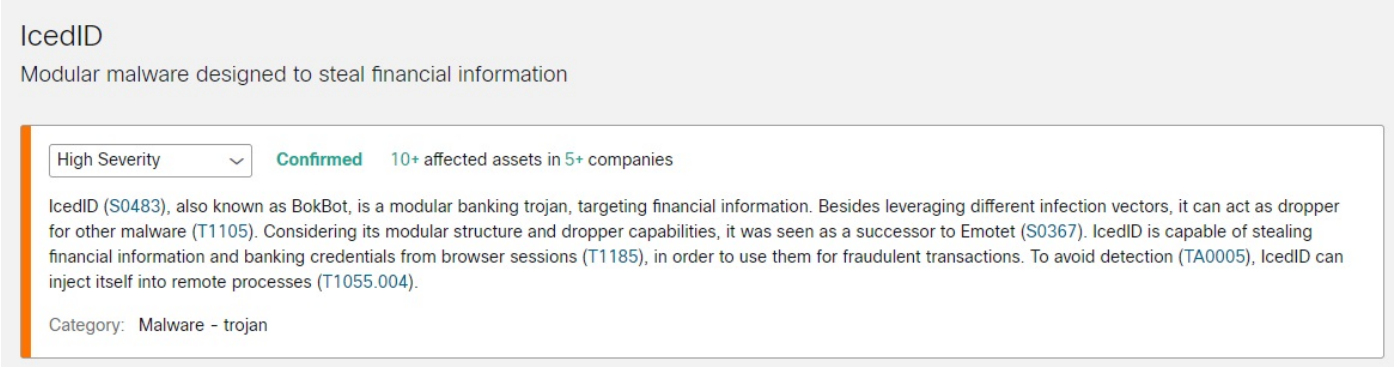
低リスクの脅威検出も多数強化されています。

IcedID

BokBot とも呼ばれる IcedID（S0483）は、金融情報を標的とするモジュール型のバンキング型トロイの木馬です。さまざまな感染ベクトルを利用するだけでなく、他のマルウェア（T1105）のドロッパーとしても機能します。そのモジュール構造とドロッパー機能から、Emotet（S0367）の後継と見なされていました。IcedIDは、不正取引への使用を目的とし、ブラウザセッション（T1185）から財務情報と銀行のログイン情報を盗むことができます。検出（TA0005）を回避するために、IcedID は自身をリモートプロセス（T1055.004）に挿入できます。

お使いの環境で IcedID が検出されたかどうかを確認するには、[IcedID 脅威の詳細（IcedID 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 *66 :*

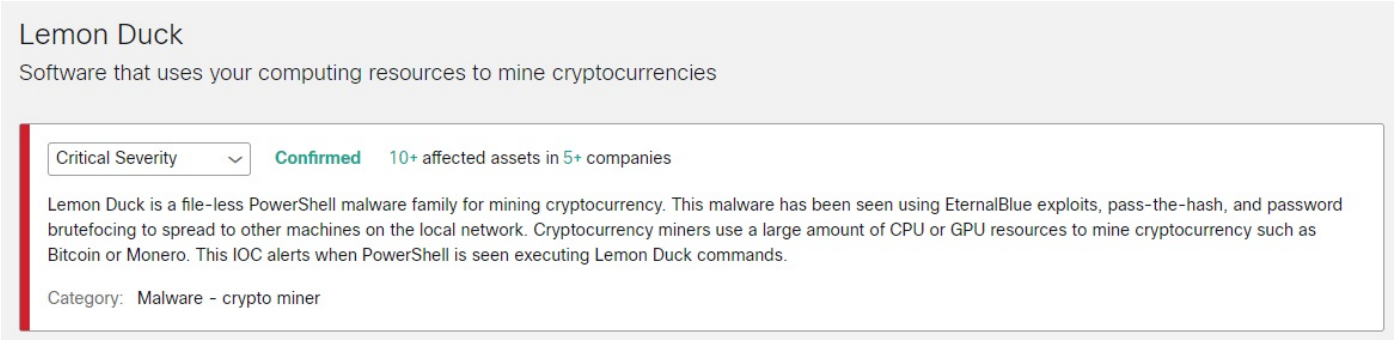


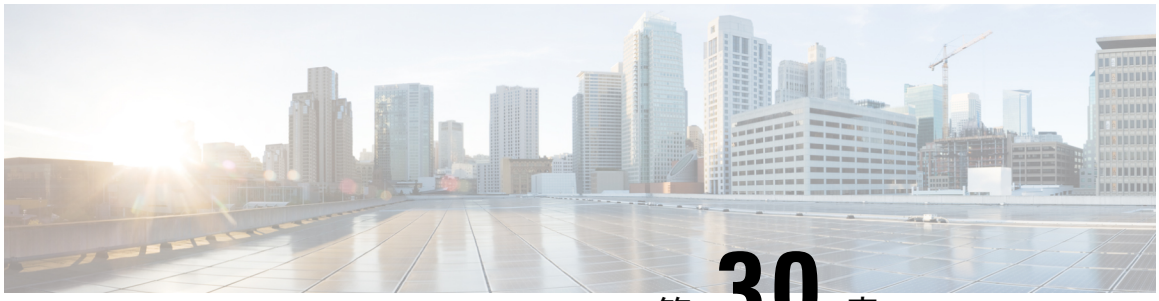
Lemon Duck

Lemon Duck は、暗号通貨をマイニングするためのファイルレス PowerShell マルウェアファミリです。このマルウェアは、EternalBlue エクスプロイト、pass-the-hash、パスワードブルートフォースを使用して、ローカルネットワーク上の他のマシンに拡散することが確認されています。暗号通貨マイナーは、大量の CPU または GPU リソースを使用して、ビットコインや Monero などの暗号通貨をマイニングします。

お使いの環境で Lemon Duck が検出されたかどうかを確認するには、[Lemon Duck 脅威の詳細（Lemon Duck 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 *67 :*





第 30 章

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。

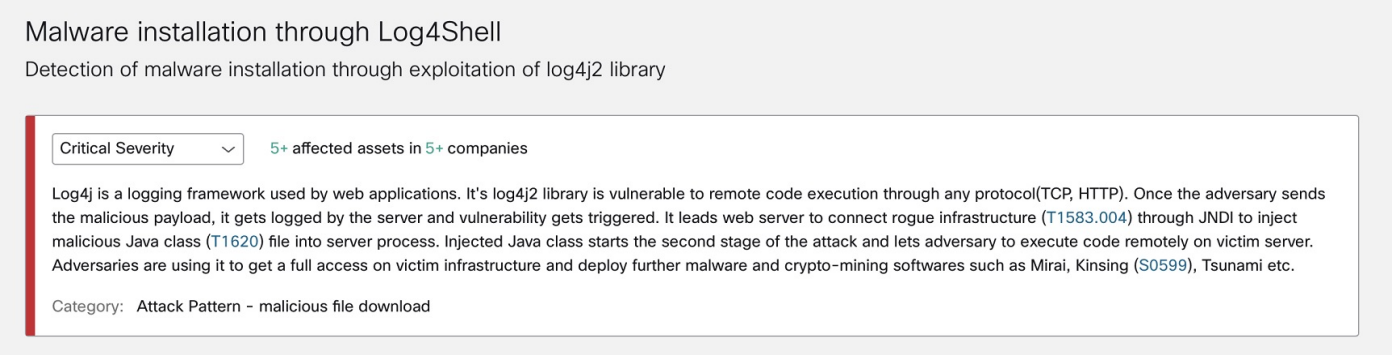
新しい Log4Shell 検出

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 *68 :*

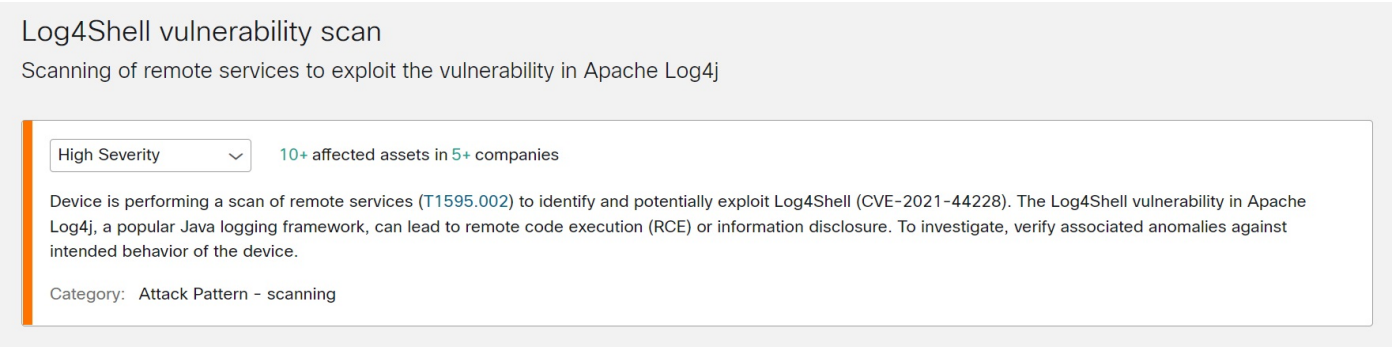


お使いの環境で [Log4Shell を介したマルウェアのインストール（Malware installation through Log4Shell）] が検出されたかどうかを確認するには、[Log4Shell を介したマルウェアのインストール（Malware installation through Log4Shell）] をクリックして、グローバル脅威アラートで詳細を表示します。

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 *69 :*



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 *70 :*

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

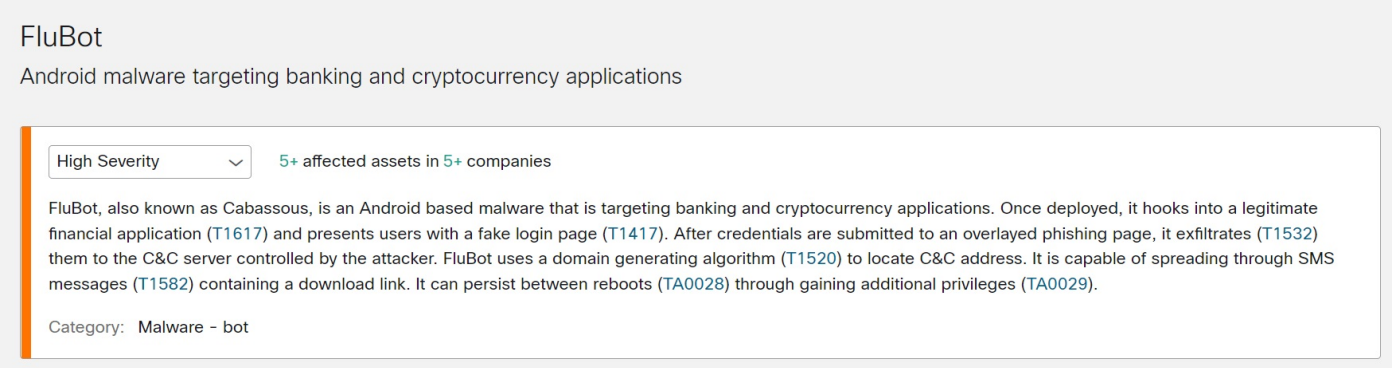
広告インジェクタ、暗号通貨マイナー、悪意のある広告、マルウェアの配布、スパムトラッキングなど、リスクの低い数多くの脅威検出も強化されています。

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 *71 :*

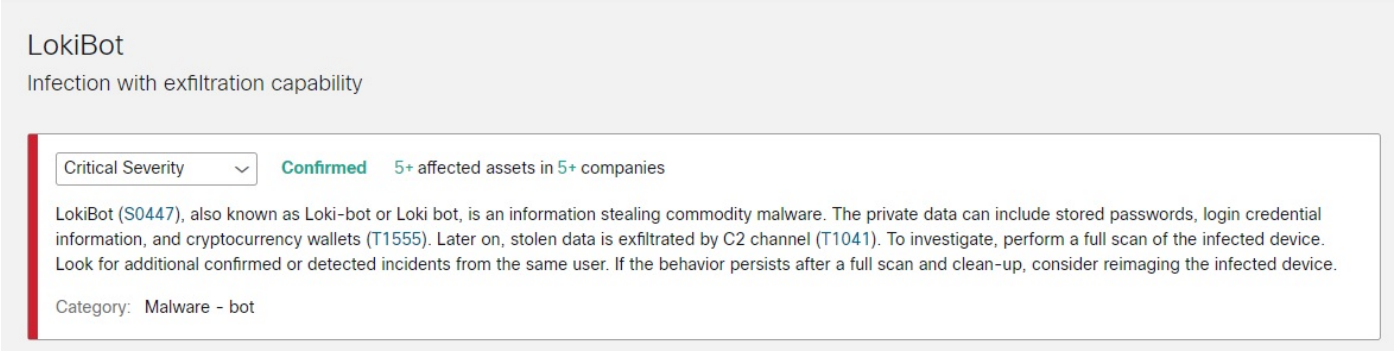


LokiBot

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 *72 :*

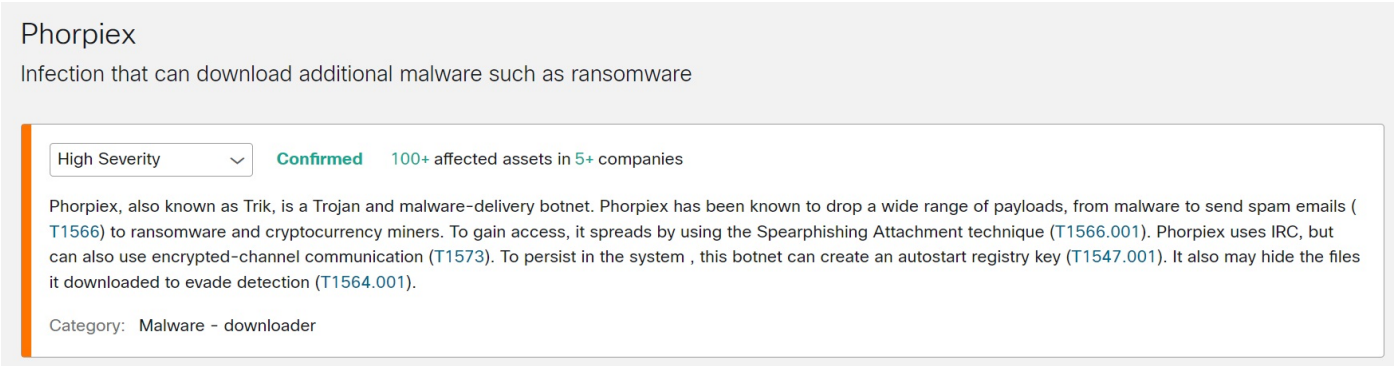


Phorpiex

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 *73 :*



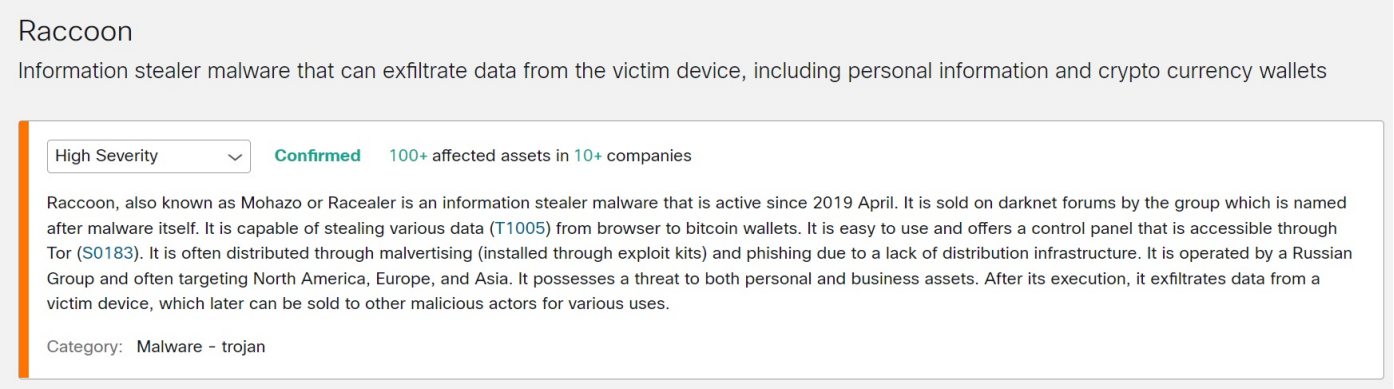
Raccoon

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 *74 :*

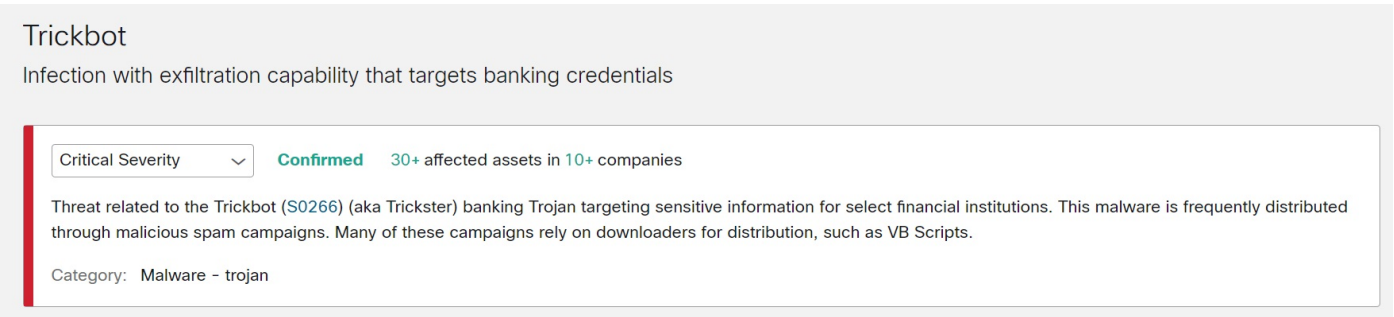


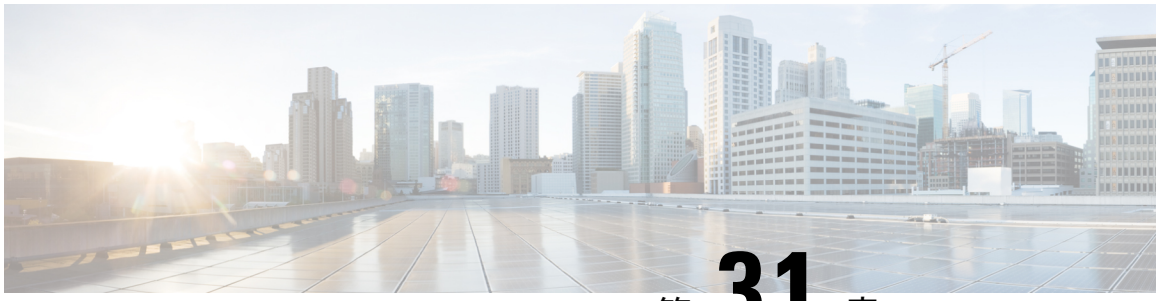
TrickBot

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 *75 :*





第 31 章

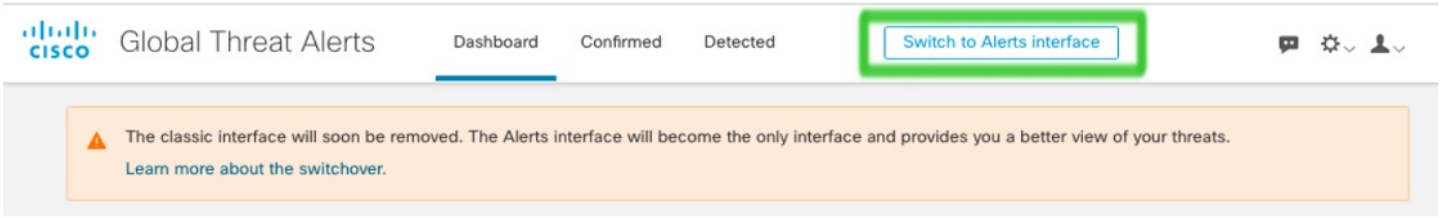
2021 年 8 月

2021 年 8 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。

廃止された従来のインターフェイス

6 月に、従来のインターフェイスからアラートインターフェイスに切り替えることをお勧めしました。

図 *76 :*



古い従来のインターフェイスは廃止され、新しいアラートインターフェイスが唯一のインターフェイスになり、ネットワーク上の脅威の拡張表示を提供します。

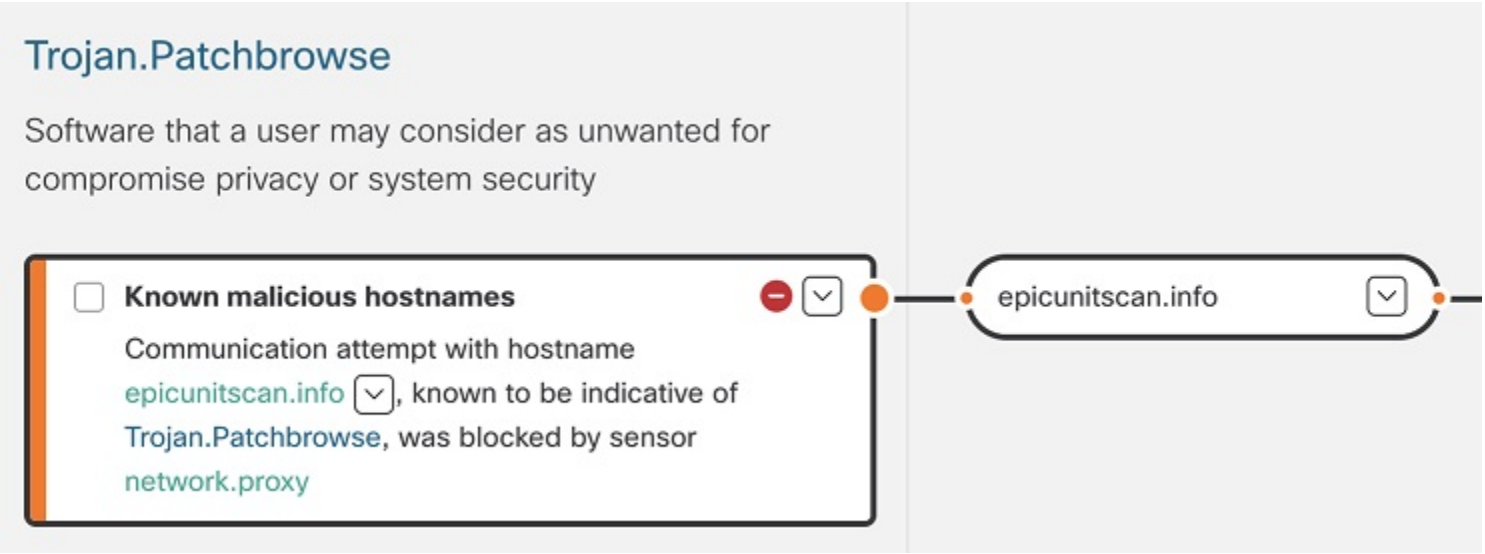
スキャンとブロックされた通信の処理の改善

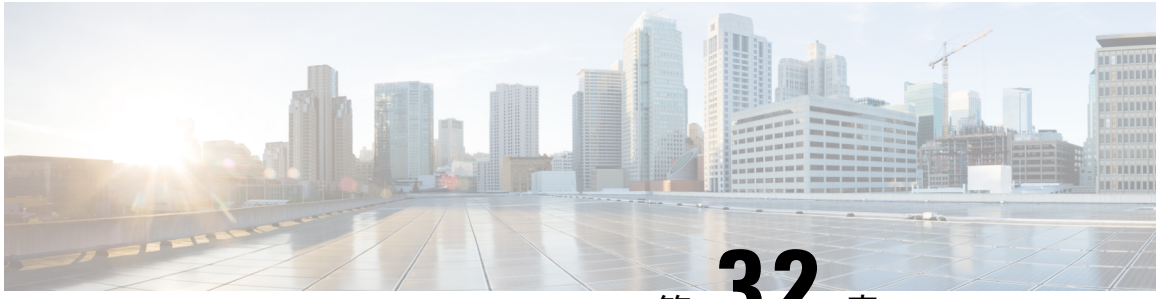
誤検知の数を減らすために、グローバル脅威アラートは、水平スキャン通信によってトリガーされる脅威検出を抑制できるようになりました。また、感染の初期段階でプロキシでブロックされた通信の脅威検出を抑制することもできます。

ケースの視覚化を改善するため、感染がエンドポイントで持続し、アウトバウンド通信の一部がプロキシ（または他のアウトバウンド制御プロセス）によってブロックされている場合、グローバル脅威アラートは脅威検出の一部として提示される特定のセキュリティイベントを説明します。

この例では、（トロイの木馬に感染していることがわかっている）ホストと通信しようとすると、プロキシセンサーによってブロックされます。セキュリティイベントは、このソフトウェアがユーザーのプライバシーまたはシステムのセキュリティを危険にさらす可能性があるため、望ましくないと見なされると通知します。

図 77: 例：通信がプロキシによってブロックされたことを通知するセキュリティイベント





第 32 章

2021 年 6 月

2021 年 6 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。

自動化サポート用の新しい REST API

グローバル脅威アラートのダッシュボードに表示されるすべてのデータが、新しい REST API を介して使用できるようになりました。これを使用して、単一のアラートの内容をダウンロードしたり、すべてのアラートをネットワーク内のサードパーティ SIEM にストリーミングすることで、データ収集プロセス全体を自動化したりすることもできます。

API は読み取り専用ではないため、グローバル脅威アラート環境の設定を変更できます。たとえば、重要なアセットグループの特定のビジネス価値を高めたり、脅威に割り当てられた重大度を変更したりできます。

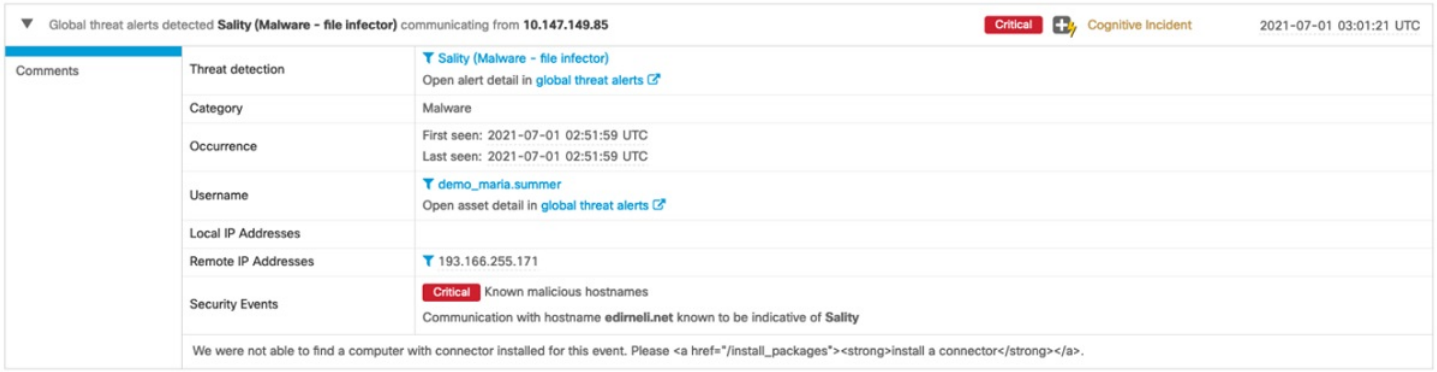
API の機能については、https://api.cta.eu.amp.cisco.com を参照してください。API の機能をより詳細に説明する仕様や使用例、追加の統合のためのサンプルスクリプトを確認することができます。

新しい REST API の詳細については、「global threat alerts REST API is now released!」[英語] を参照してください。

Secure Endpoint 統合の更新

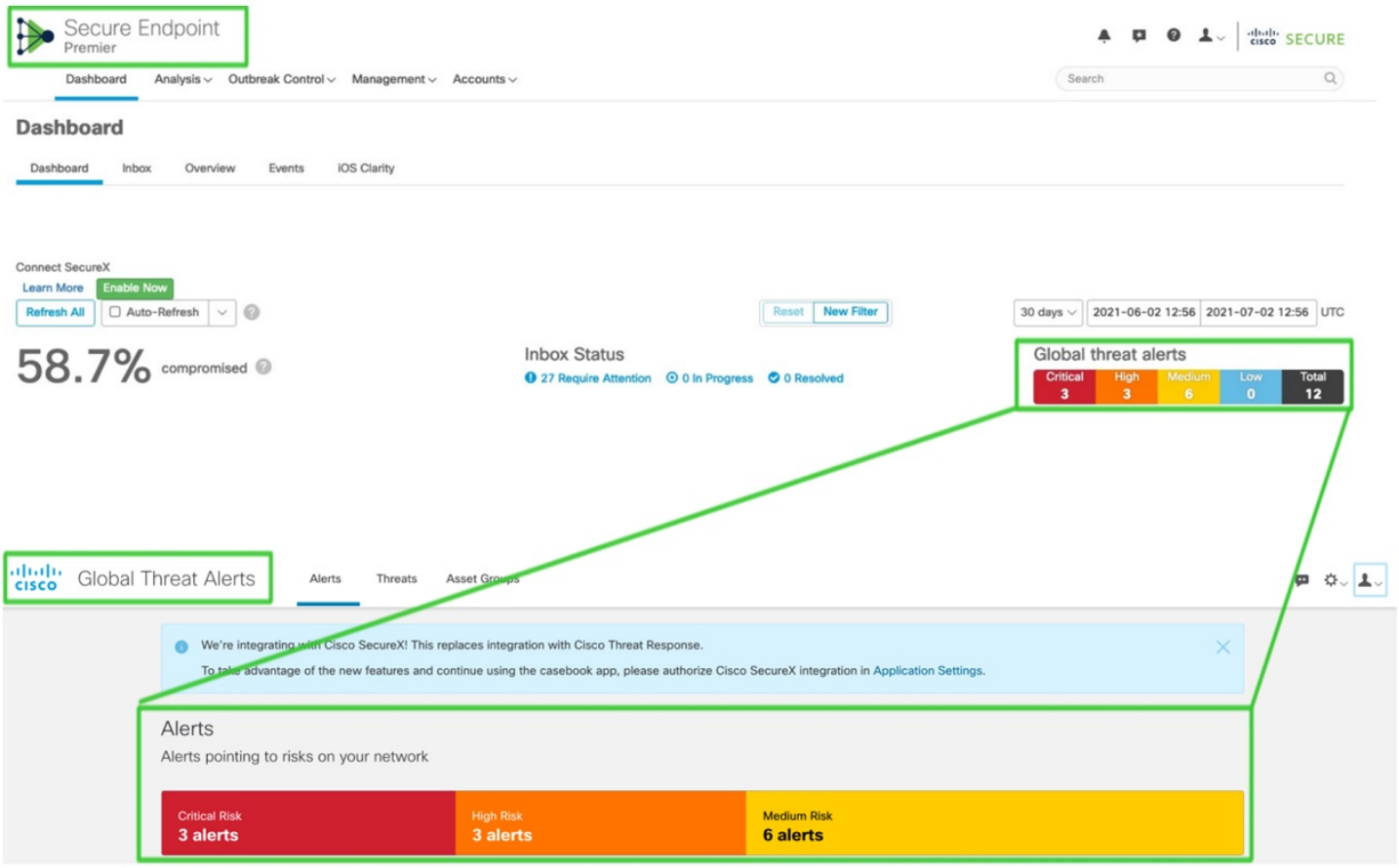
グローバル脅威アラートからの検出内容を Secure Endpoint で表示する方法が更新されました。現在、検出内容はコンソールにイベントとして表示され、アラートインターフェイスに直接リンクされています。その結果、アラートインターフェイスでの脅威の重大度が変更されると、その変更がこれらのイベントで反映されます。

図 *78 :* グローバル脅威アラートの検出内容は、***Secure Endpoint*** コンソールでイベントとして表示されるようになりました。



グローバル脅威アラートインターフェイスでアラートの状態またはリスクが変更されると、その変更が Secure Endpoint コンソールのアラートの概要で反映されます。

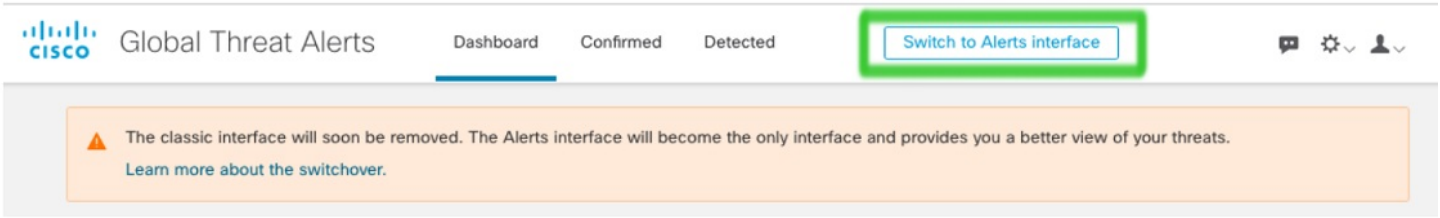
図 *79 :*



互換性の問題を回避するため、従来のインターフェイスは間もなく廃止されます。そのため、従来のインターフェイスからアラートインターフェイスに切り替えることをお勧めします。グ

ローバル脅威アラートダッシュボードで、[アラートインターフェイスに切り替え（Switch to Alerts interface）] ボタンをクリックします。

図 *80 :*

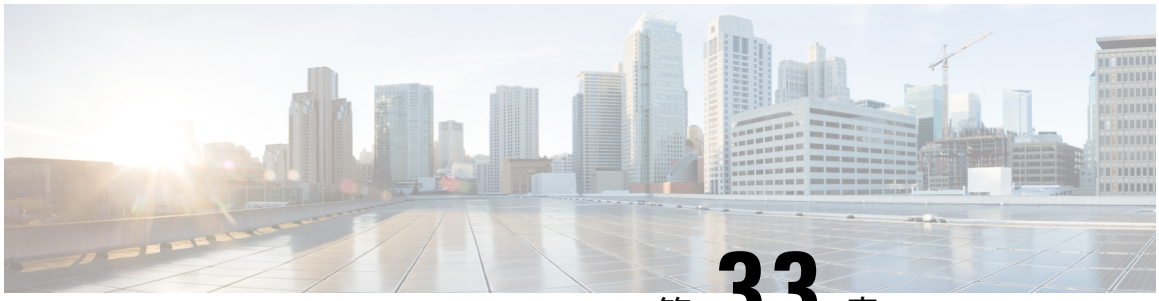


STIX/TAXII API の更新

STIX/TAXII API フィードによって提供される検出リンクと脅威に関する用語が、グローバル脅威アラートダッシュボードのアラートインターフェイスと互換性を持つようになりました。

図 *81 :*

脅威に関する表現と分類が変更されたため、STIX/TAXII API によって提供されるツールと SIEM で、非互換性の問題や依存関係の破損がないか確認することをお勧めします。



第 33 章

2021 年 5 月

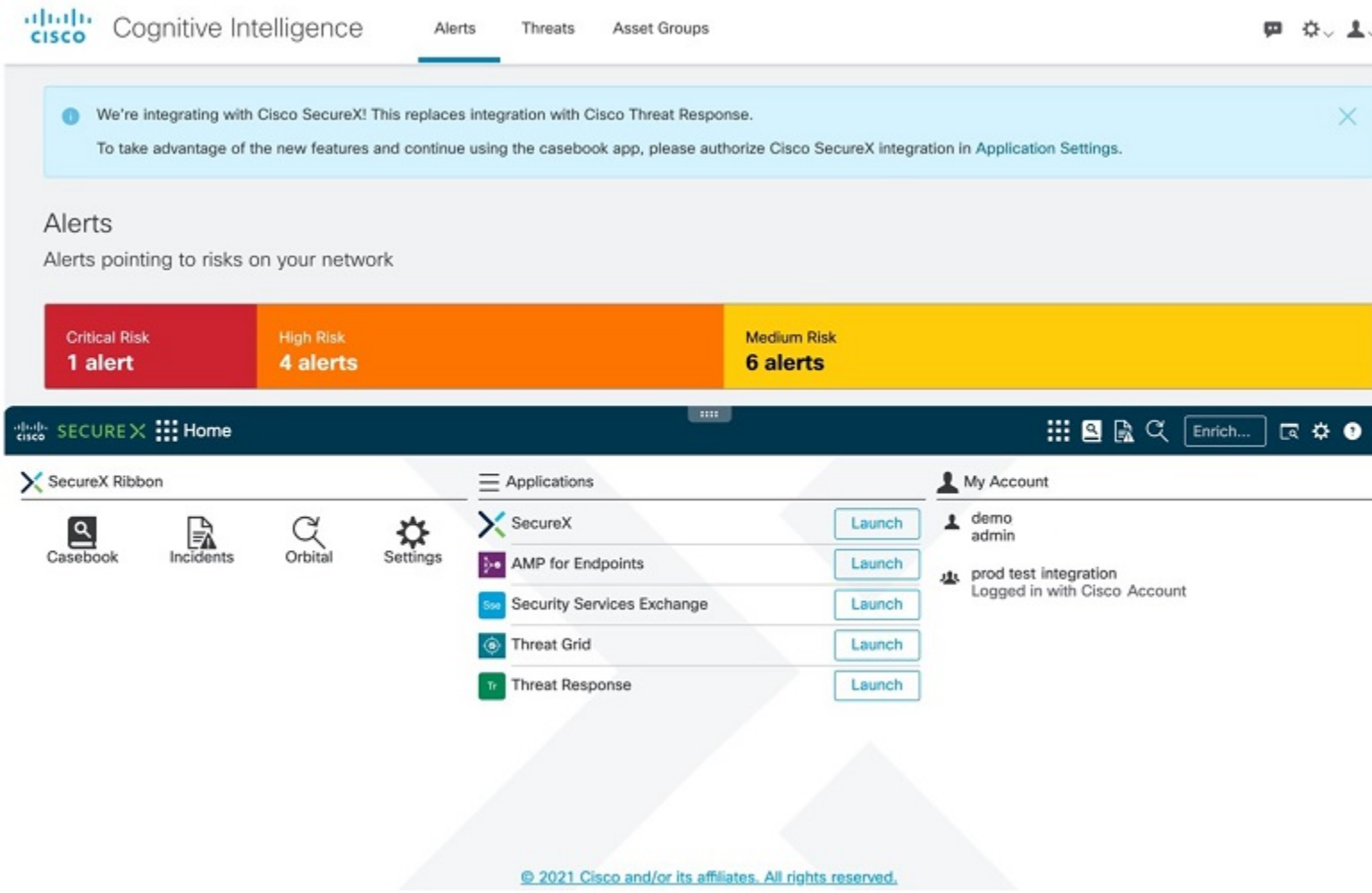
2021 年 5 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

SecureX リボンのサポート

SecureX は、中央管理型コンソールであると同時に、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散機能でもあります。これらの分散機能は、SecureX リボンでアプリケーションおよびツールの形式で表示されます。

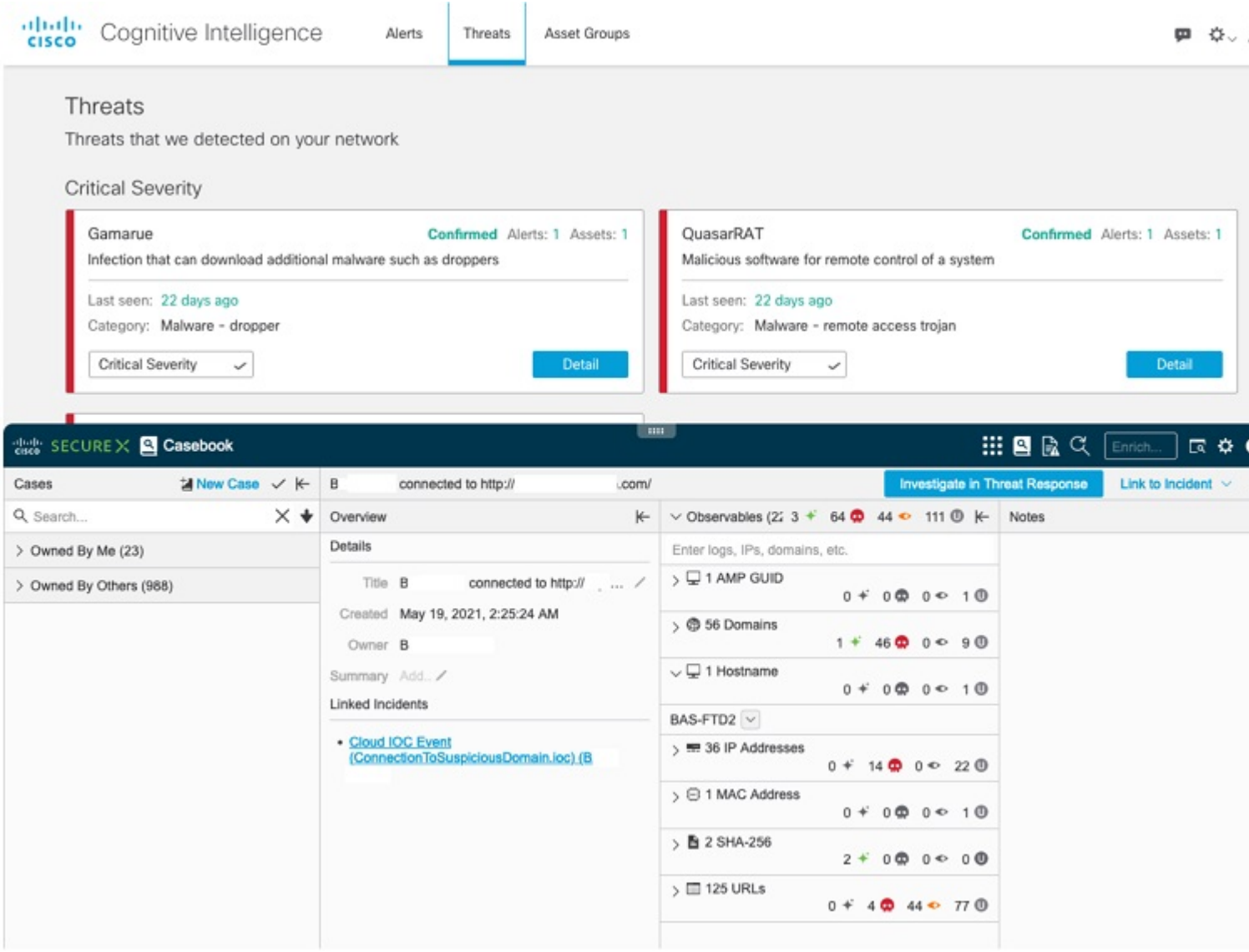
SecureX リボンがページ下部にあるグローバル脅威アラートでも使用できるようになり、環境内のダッシュボードと他のセキュリティ製品間を移動しても保持されます。これは、事例集やインシデントと調査結果を関連付けるのに役立ちます。

図 *82 :* ページの下部にある *SecureX* リボン



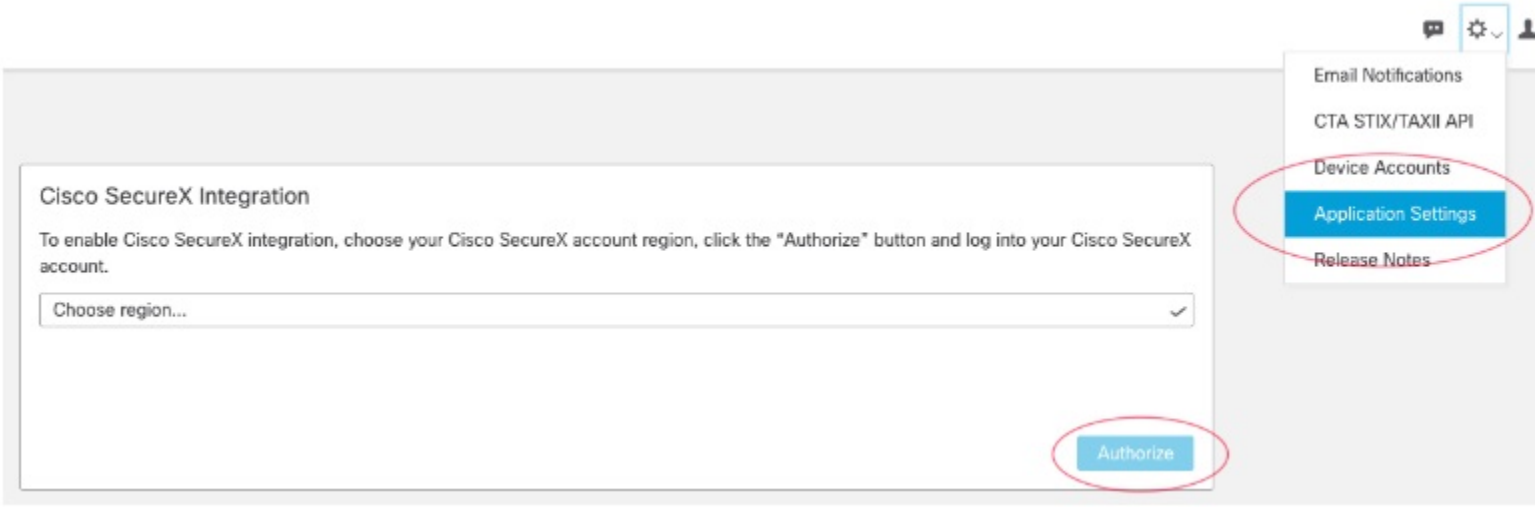
リボンを使用して、事例集、設定、およびその他のアプリケーションにアクセスできます。また、インシデントを表示し、監視対象を検索してエンリッチメントを追加することもできます。

図 *83 :* 例：*SecureX* リボンを使用して事例集にアクセスする



この機能を有効にするには、ユーザが SecureX アカウントを持ち、アプリケーション設定で統合を承認する必要があります。

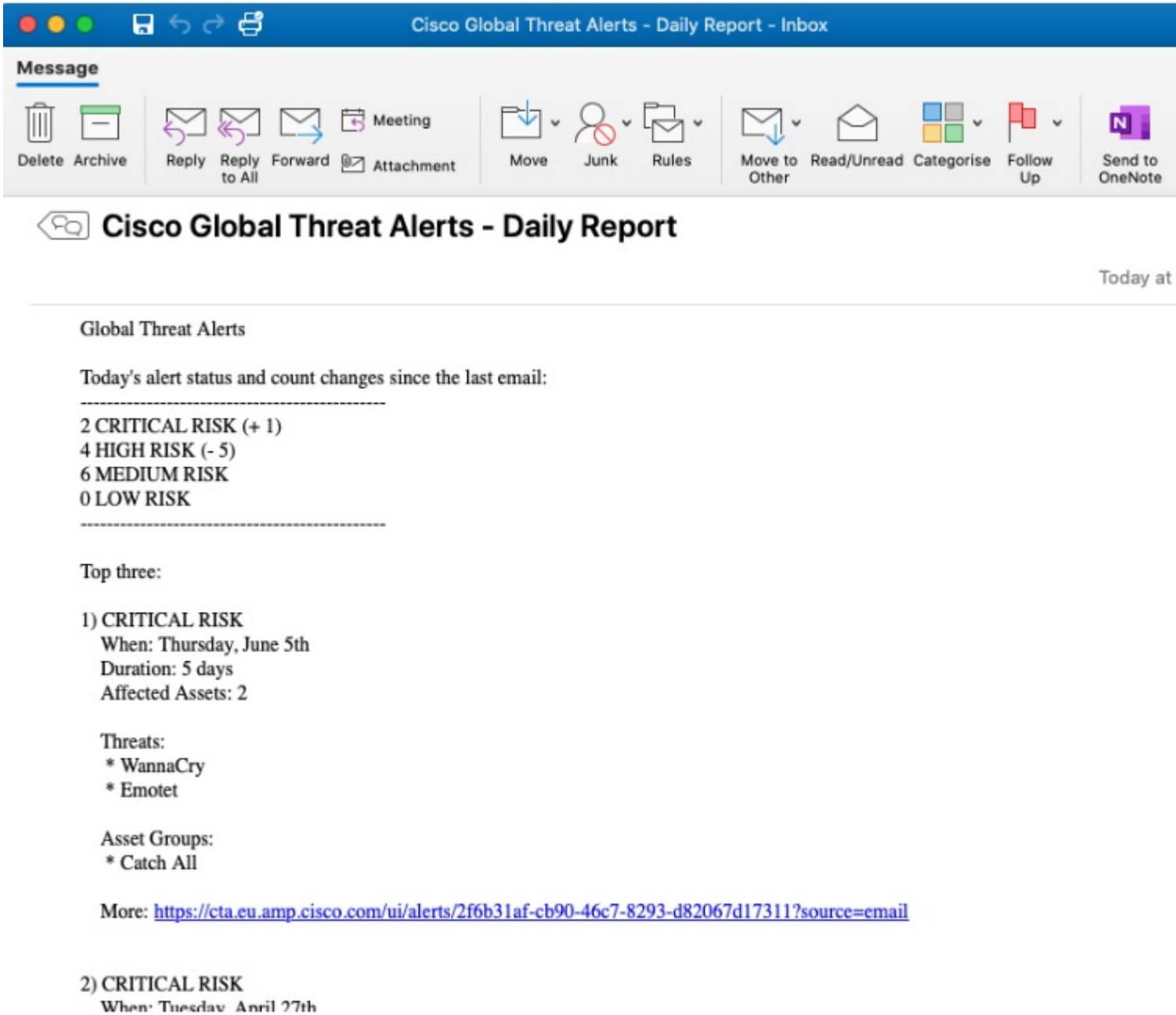
図 *84 : [*アプリケーション設定（***Application Settings***）*]*に移動し、***SecureX***との統合を承認します。



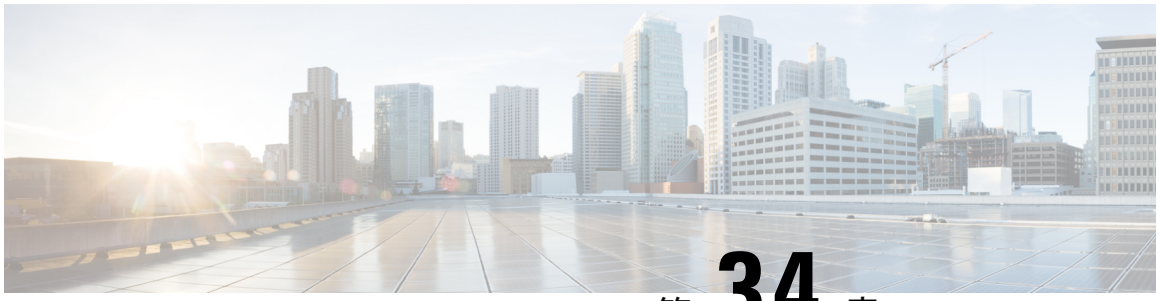
更新された日次レポート電子メール

電子メール通知サービスが更新され、アラートダッシュボードと互換性のあるコンテンツが電子メールで送信されるようなりました。日次レポートの電子メールでは、アラートの現在のステータスと、報告されたアラート数の最近の変化が通知されます。

図 *85 :* 例：更新された日次レポートの電子メール



このサービスを有効にするには、グローバル設定メニューから [電子メール通知（Email Notifications）] を選択し、日次レポートを受信する電子メールアドレスを入力します。



第 34 章

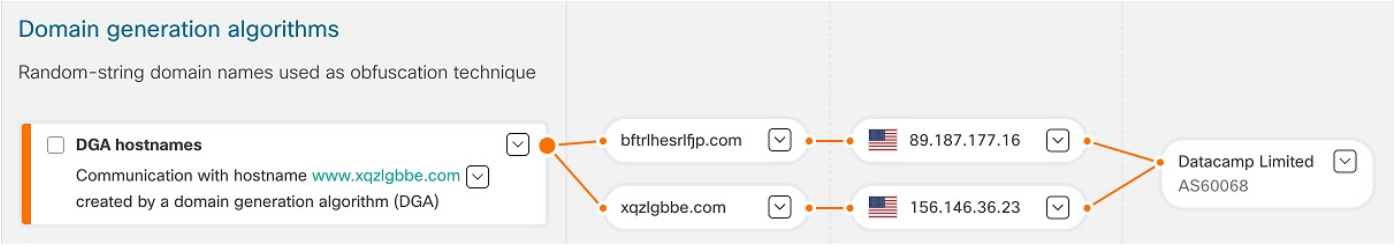
2021 年 4 月

2021 年 4 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 DGA 2.0 分類子

ドメイン生成アルゴリズム（DGA）は、攻撃者がホスト名をランダムに生成して、ブロッキング機能を備えたセキュリティ製品をバイパスするために使用されます。これらのアルゴリズムは、一般にボットネットやアドウェアの通信に使用されます。これらは動的に生成されるため、静的な署名ベースのウォッチリストに依存する、本来ならブロックする機能を果たすはずのセキュリティ製品がバイパスされてしまいます。

図 *86* : 例：ブロッカーを難読化するために *DGA* によって生成されたランダム文字列ドメイン



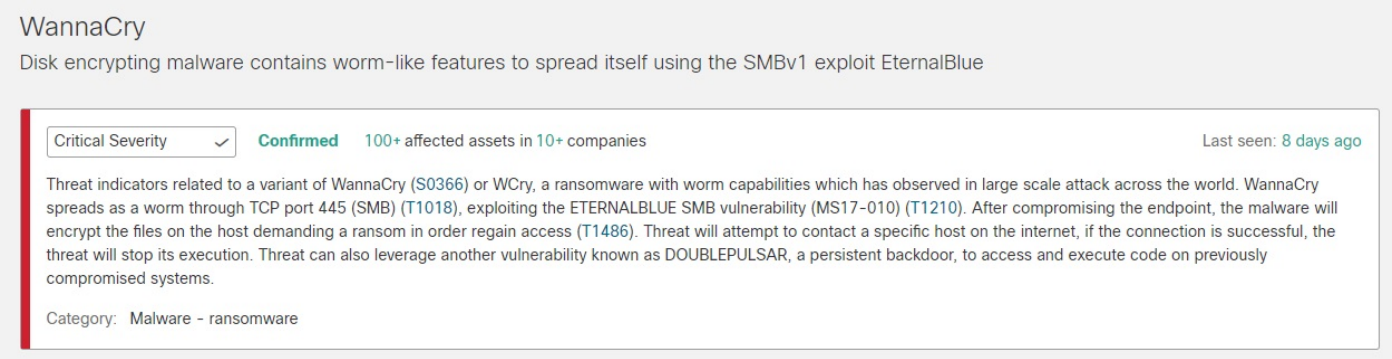
グローバル脅威アラートは 2015 年から DGA ドメインの検出をサポートしていますが、DGA 2.0 分類子は、古いランダムフォレストではなく、ニュートラルネットワーク（テキスト処理の最先端ソリューション）上に構築された新しいモデルです。このアーキテクチャの更新と新しく作成されたトレーニングセットにより、誤検出が少なくなり、再現率（偽陽性の数）が倍増しました。

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。

アラートの説明で新しい MITER への言及

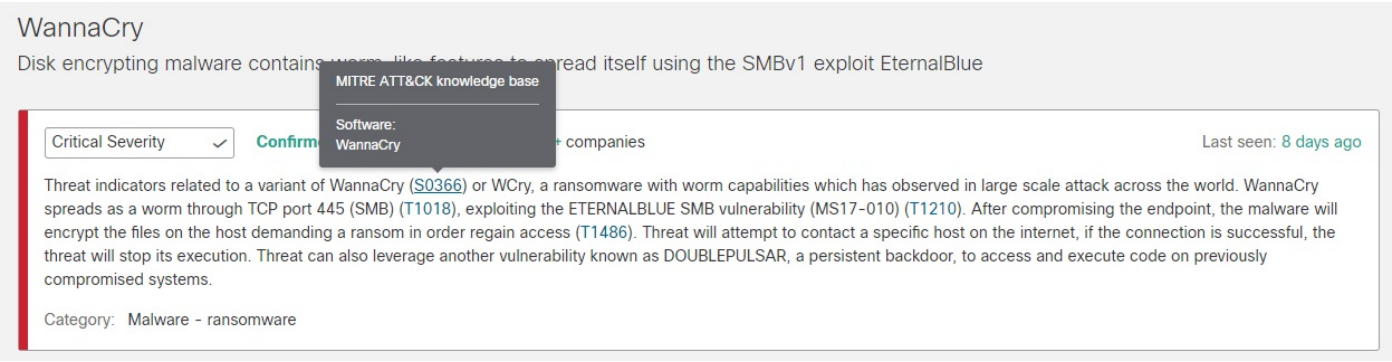
補足情報に簡単にアクセスできるように、MITER の参考資料をアラートの説明に直接追加しました。

図 *87 :* 例：*WannaCry* の説明内の *4* つの *MITER* 参考資料（*S0366*、*T1018*、*T1210*、*T1486*）



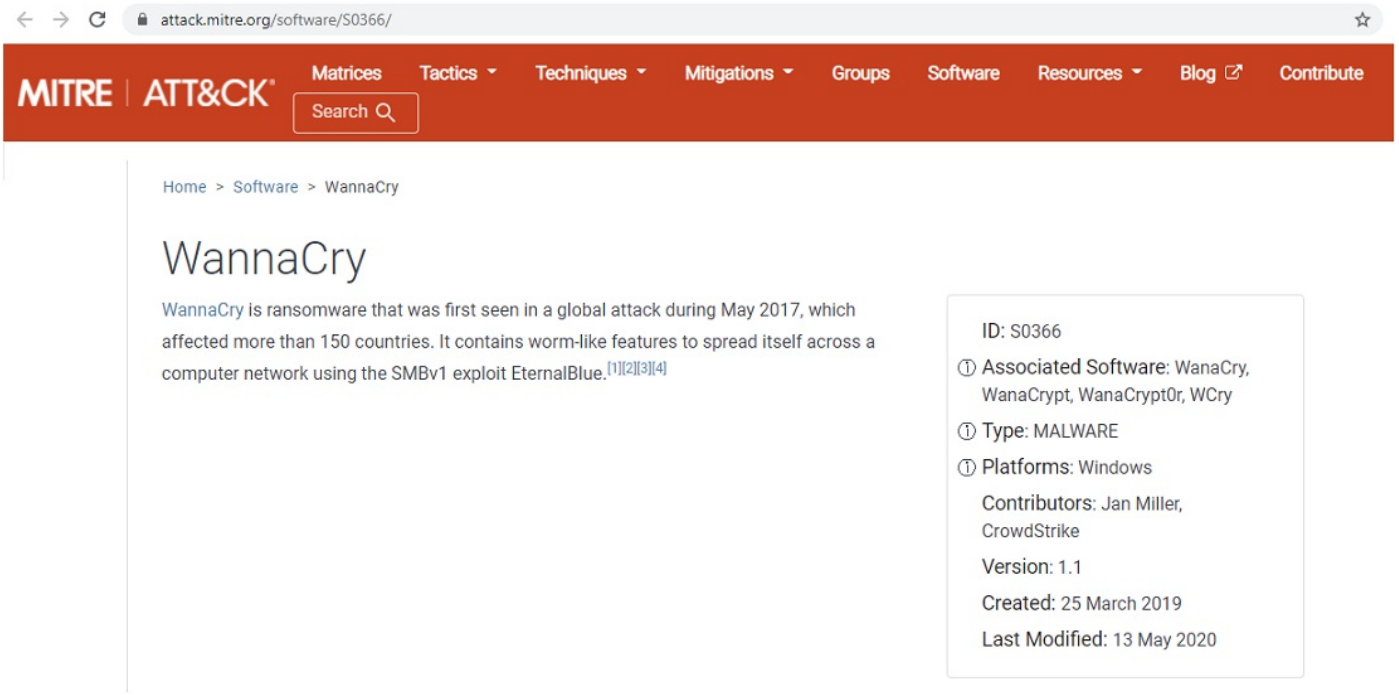
アラートやその説明に関する詳細情報を知りたい場合、ID 番号をクリックします。

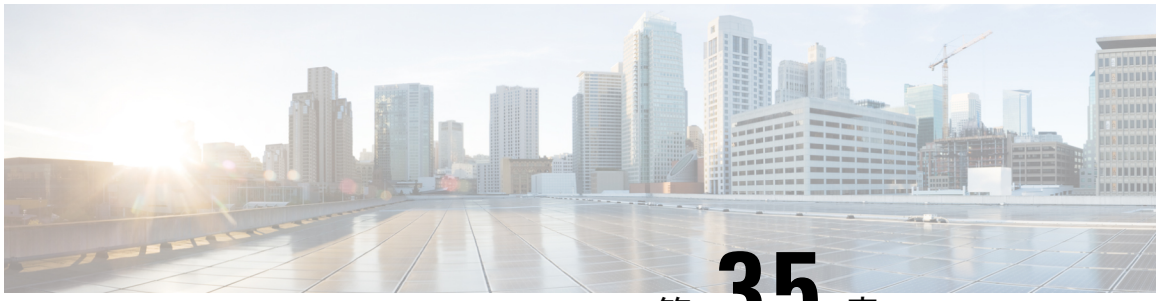
図 *88 :* 例：*S0366* の *MITER ATT&CK* ナレッジベースへの埋め込みリンク



...新しいブラウザページが開き、MITRE ATT&CK のナレッジベースと特定の脅威に関する詳細情報が表示されます。

図 *89 : S0366* に関する詳細情報を示す *MITER ATT&CK* のページ





第 35 章

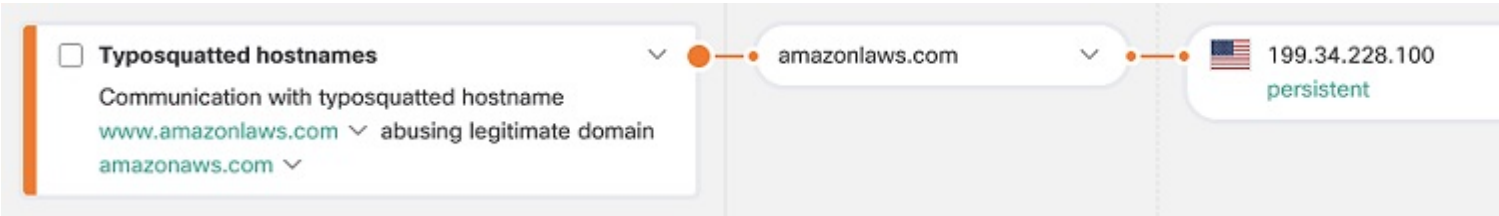
2021 年 3 月

2021 年 3 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。

新しいタイポスクワッティング分類子

タイポスクワッティングとは、ユーザが Web ブラウザに URL を入力する際の入力ミス（タイプミス）を利用する URL ハイジャックの一種です。これにより、ユーザは攻撃者が所有する別の Web サイトに誘導されます。タイポスクワッティング URL は、次のように、正規の URL に視覚的に似ています。

図 *90 :* 例：余分な文字が追加されたタイポスクワッティングのホスト名



通常、タイポスクワッティング URL は、広告から利益を得るために使用される広告ページや、ユーザから情報を盗むために使用されるフィッシングページなどのオンライン詐欺に誘導します。

図 *91 :* 例：*Amazon AWS* にアクセスしようとするユーザをターゲットとする広告ページ

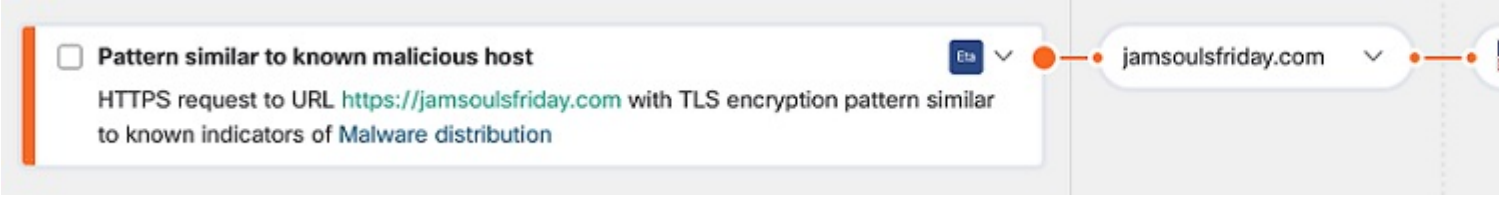
新しい分類子は、最も一般的なドメインをターゲットとするタイポスクワッティングドメインからユーザを保護することを目的としています。分類子は、ドメインの類似性を計算することで、最も一般的なドメインに類似するドメインを効率的に識別します。その後、タイポスクワッティング ドメインの運用期間などの追加パラメータに基づいて脅威の重大度を決定します。

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。

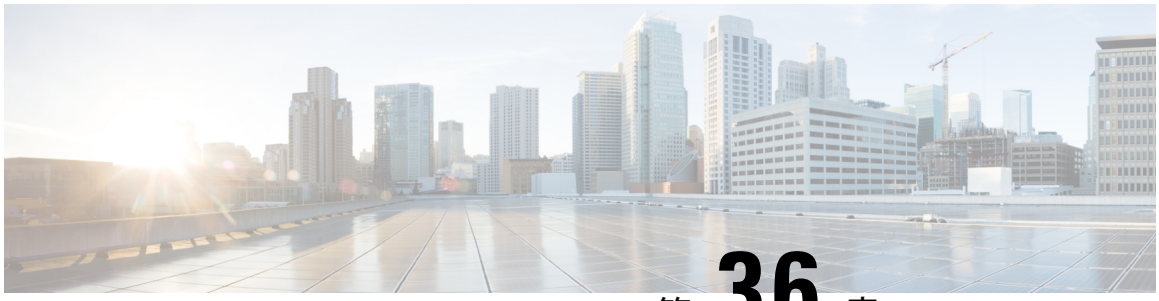
新しい TLS パターン分類子

新しい分類子は、Transport Layer Security（TLS）フィンガープリントテクノロジーの上に構築されています。https://en.wikipedia.org/wiki/Transport_Layer_Security暗号化トラフィック分析（ETA）からのTLSヘッダーと追加のグローバルおよびローカルコンテキストの機能を考慮して、分類子は TLS フットプリントに基づいて疑わしいアプリケーションおよび悪意のあるアプリケーションを検出します。https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.html分類子は、暗号化された通信を分析することで、HTTP で通信する脅威を対象としたモデルの機能を拡張します。

図 *92 :* 例：悪意のあることが知られているホストに類似した *TLS* パターン



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。



第 36 章

2021年 3 月以前

2021年 3 月以前

2021年3月より前にリリースされたアップデートは、シスココミュニティのセキュリティブログで **Cognitive Intelligence** ラベルと **cognitive-release-notes** タグ付きでアーカイブされています。

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。