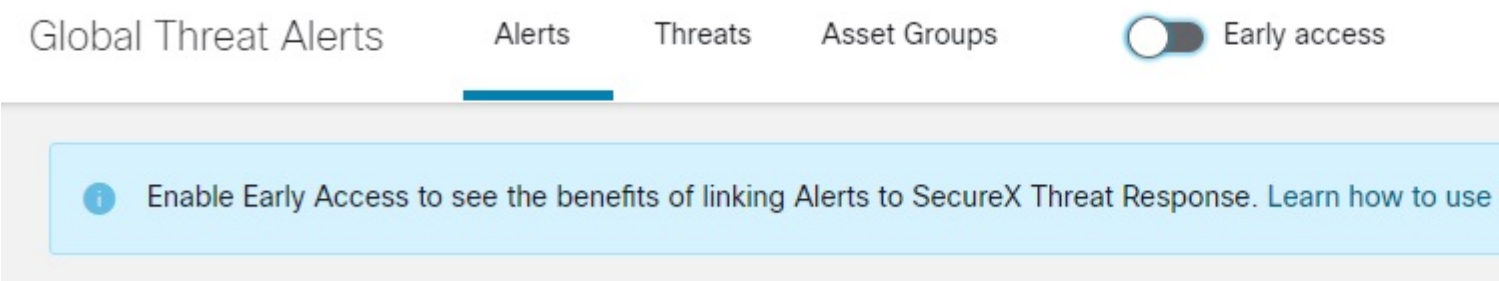
2022 年 1 月

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

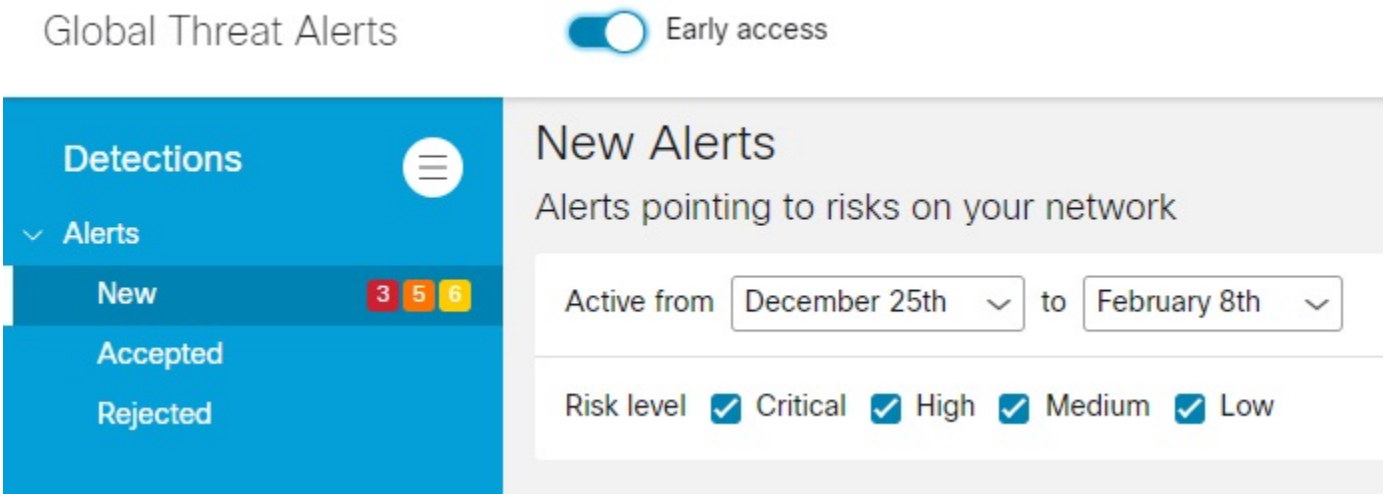
SecureX Incident Manager へグローバル脅威アラートでアラートをプロモートする機能を追加しました。この機能を有効にするには、グローバル脅威アラートコンソールのヘッダーで [早期アクセス（Early access）] を有効にします。

図 *1 : [*早期アクセス（*Early access***）*]* をクリックして新機能を有効化**



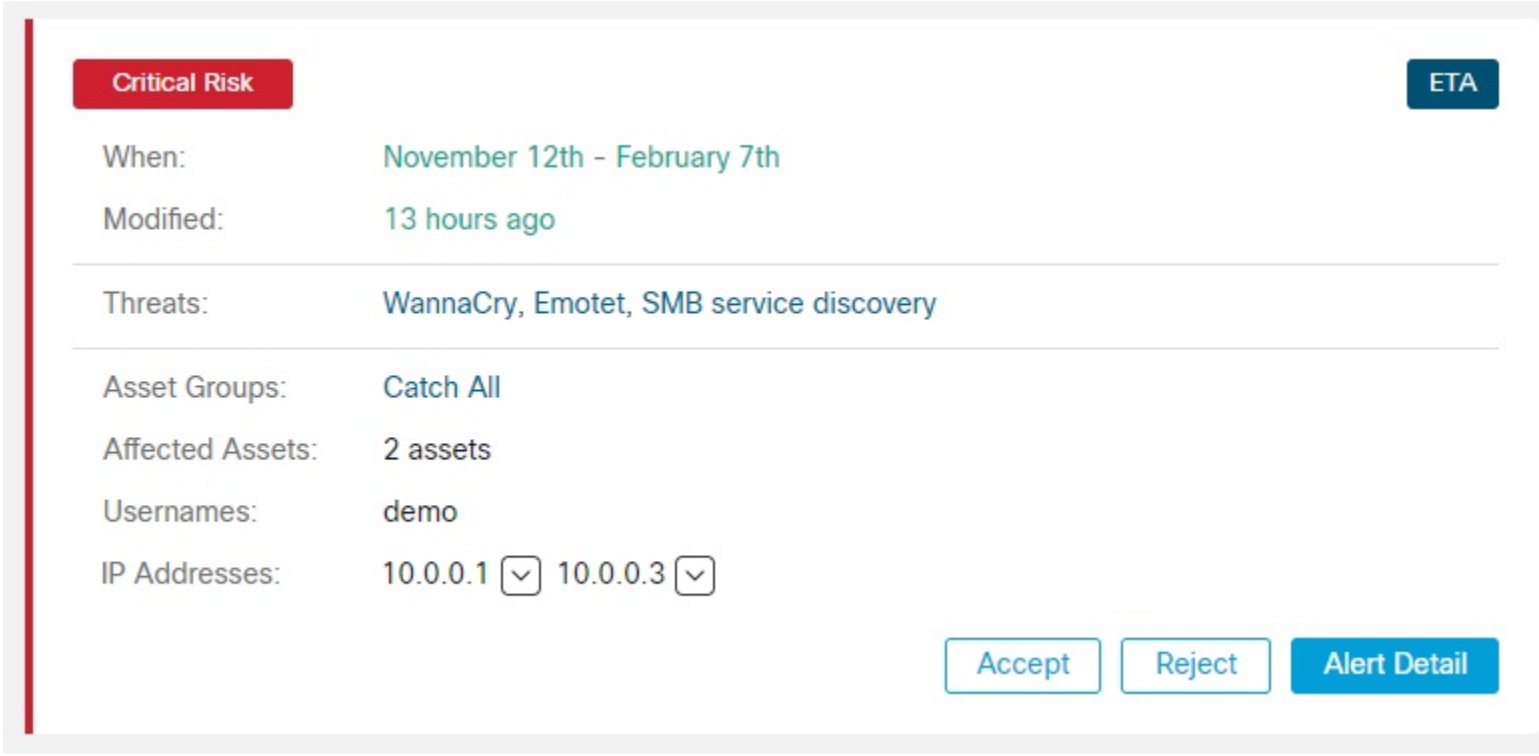
有効にすると、SecureX Incident Manager は、グローバル脅威アラートの既存のワークフローを置き換えます。アラートは、[新規（New）]、[承認（Accepted）]、または [拒否（Rejected）] に分類されます。

図 *2 : 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。

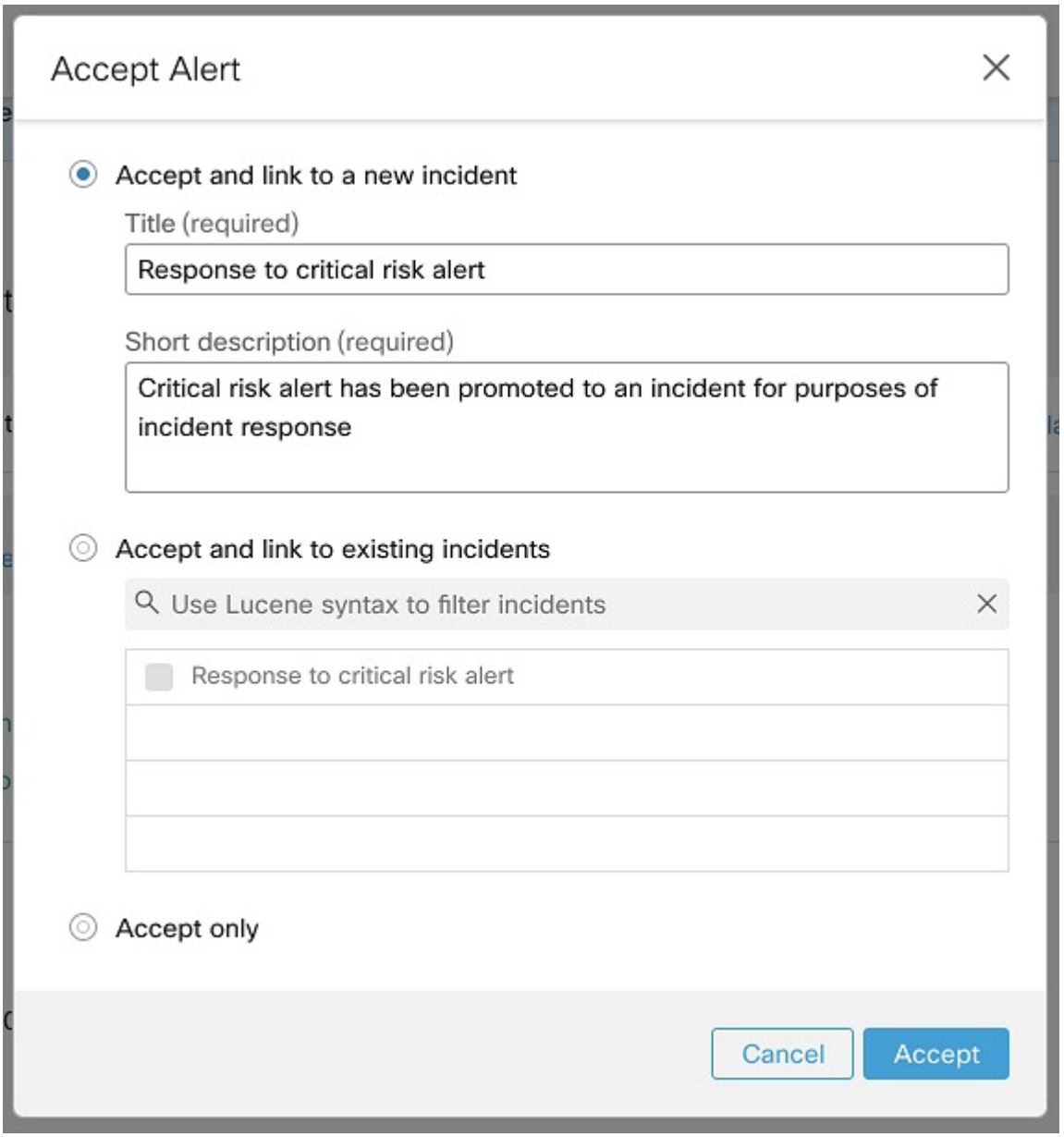
図 *3 :* アラートの承認または拒否



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。

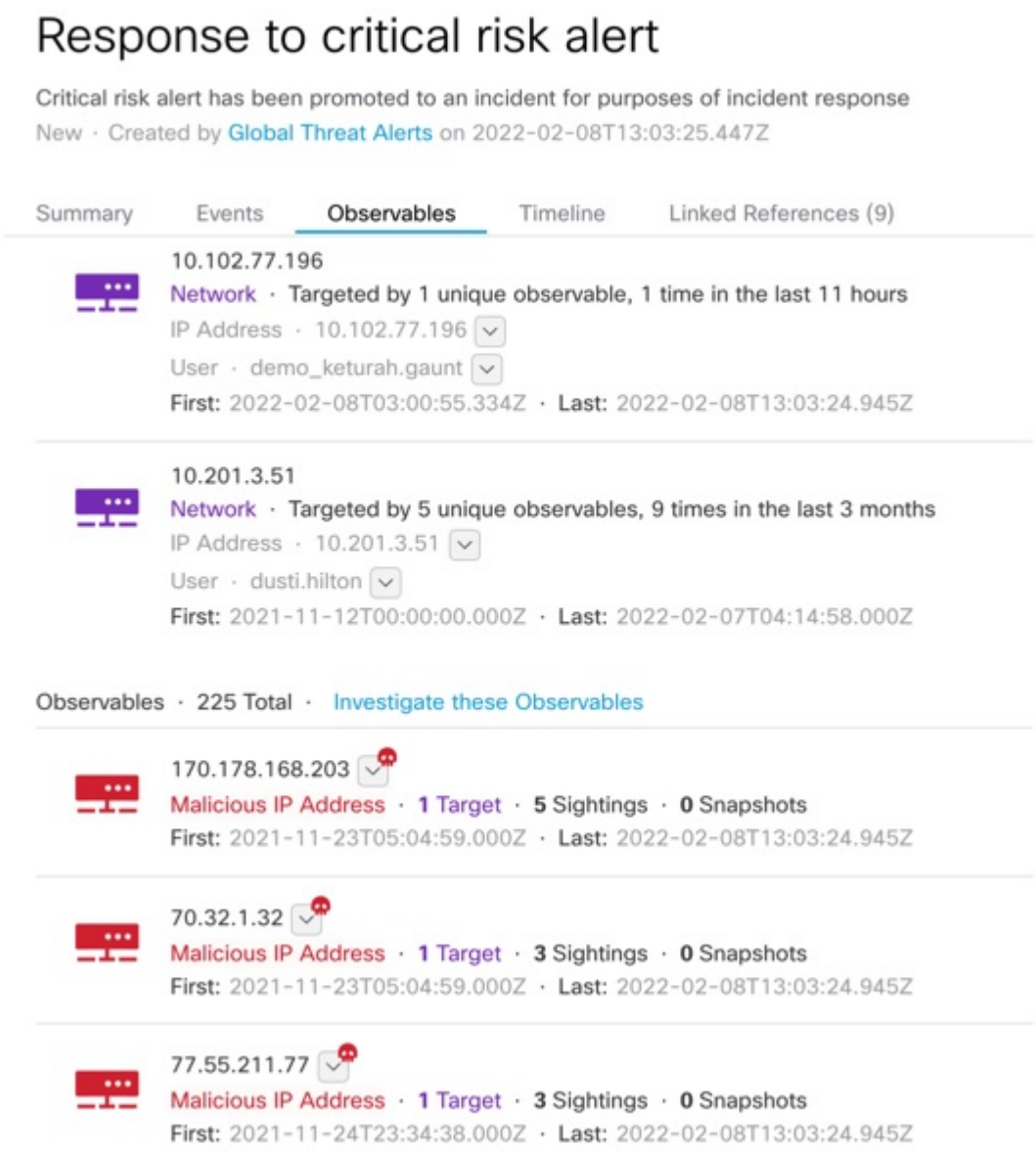
図 *4*: インシデントにリンクするオプションでアラートを承認



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。

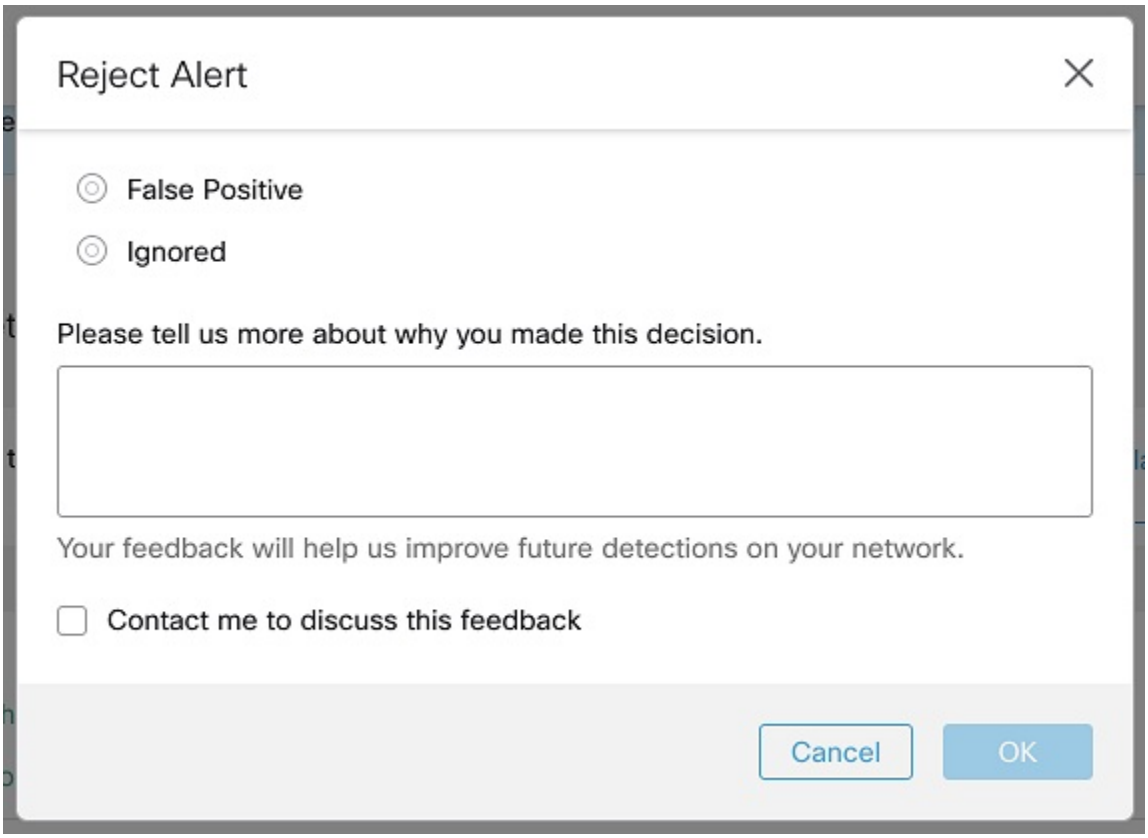
図 *5:* インシデントサマリーの例

図 *6* : 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 7: 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

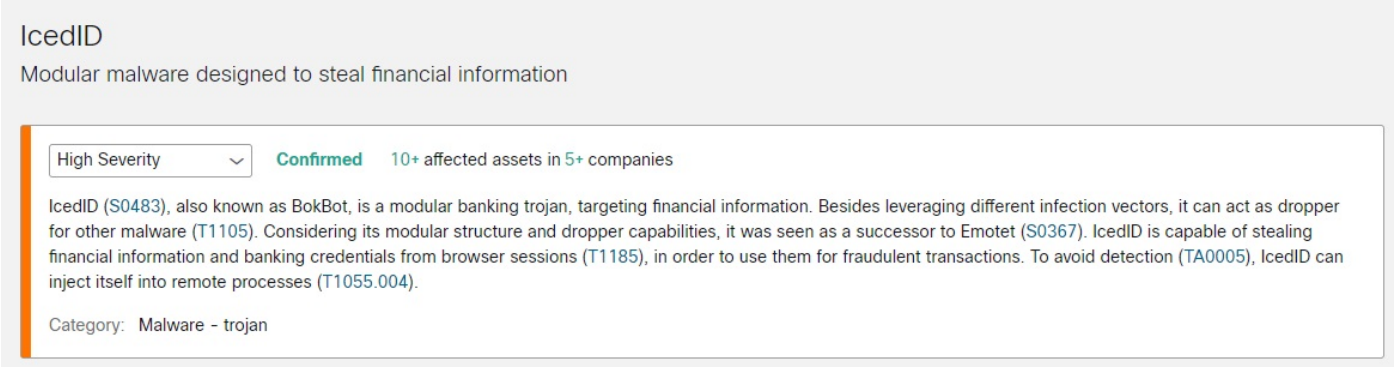
低リスクの脅威検出も多数強化されています。

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 *8 :*

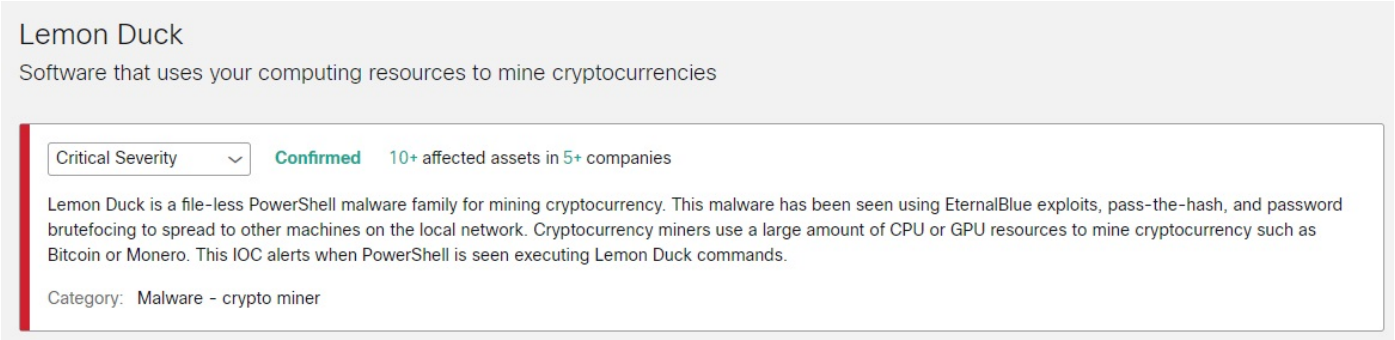


Lemon Duck

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 *9 :*



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。