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。

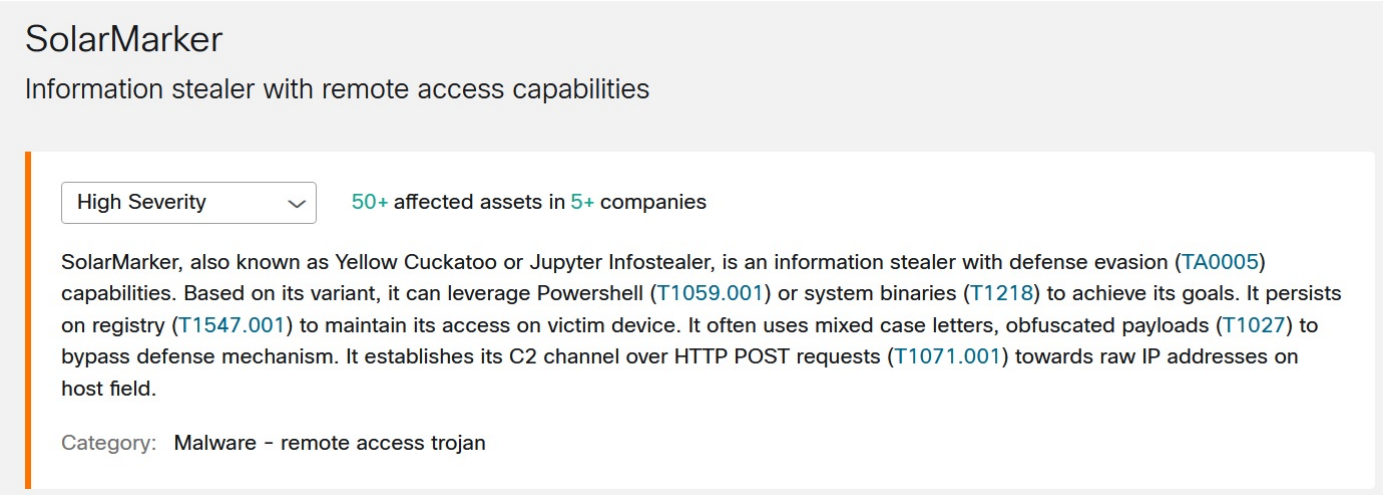
SolarMarker

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 *1*:



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。