



## 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 \(1 ページ\)](#)
- [追加の脅威検出 \(1 ページ\)](#)

### 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を更新しました。

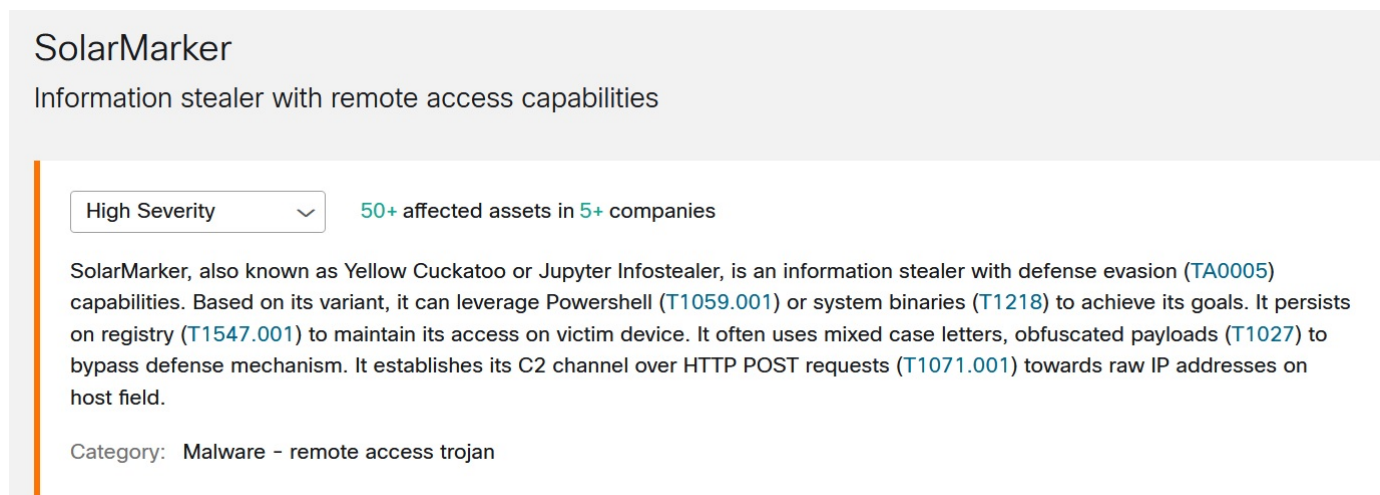
#### SolarMarker

SolarMarker は、Yellow Cuckatoo または Jupyter Infostealer と呼ばれ、防御を回避 (TA0005) できる情報窃取マルウェアです。そのバリエーションに基づいて、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チャンネルを確立します。

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:



The screenshot shows a security tool interface for a threat named "SolarMarker". The title is "SolarMarker" with the subtitle "Information stealer with remote access capabilities". Below the title, there is a severity dropdown menu set to "High Severity" and a status indicator "50+ affected assets in 5+ companies". The main text describes SolarMarker as an information stealer with defense evasion capabilities, mentioning its variants like Yellow Cuckatoo and Jupyter Infostealer, and its use of Powershell, system binaries, registry, and obfuscated payloads to establish a C2 channel over HTTP POST requests. The category is listed as "Malware - remote access trojan".

## SolarMarker

Information stealer with remote access capabilities

High Severity 50+ affected assets in 5+ companies

SolarMarker, also known as Yellow Cuckatoo or Jupyter Infostealer, is an information stealer with defense evasion (TA0005) capabilities. Based on its variant, it can leverage Powershell (T1059.001) or system binaries (T1218) to achieve its goals. It persists on registry (T1547.001) to maintain its access on victim device. It often uses mixed case letters, obfuscated payloads (T1027) to bypass defense mechanism. It establishes its C2 channel over HTTP POST requests (T1071.001) towards raw IP addresses on host field.

Category: Malware - remote access trojan

## 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。