



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 \(1 ページ\)](#)

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。

- Lumma
- PYbot

また、既存の脅威検出のインジケータも更新しました。

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)、メッセージング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、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。

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。