



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 \(1 ページ\)](#)

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。

- 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 1:

Private Loader

Modular malware downloader

High Severity

5+ affected assets in 5+ companies

Private Loader is a modular downloader that distributes information stealers, banking trojans, ransomware and other loaders. This malware was first seen in 2021 and is still active. Private Loader is distributed via malicious links (T1204.001) that distributes cracked software and games. Once the victim downloads and execute the file (T1204.002), the victim device contacts a dead drop resolver (T1102.001). Private Loader contacts the Command and Control served (T1071.001) and downloads other payloads (T1105).

Category: Malware - downloader

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 2:

PlugX (S0013)

Remote Access Trojan with self replicating capabilities

High Severity

5+ affected assets in 5+ companies

PlugX (S0013) is a remote access trojan, often leveraged by Chinese threat actors. It is similar to PoisonIvy (S0012), with a modular structure. PlugX can hide itself within Recycle Bin (T1564.001) of the victim device. It can abuse benign software to side-load malicious DLL (T1574.002). It is capable of replicating itself to multiple directories (T1091). It can gain persistence through scheduled tasks (T1053.005).

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。