2023 年 8 月

2023 年 8 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

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。

- Spyder Backdoor
- AsyncRAT

また、既存の脅威検出のインジケーターも更新しました。

Spyder Backdoor

Spyder は、WarHawk と同様のバックドアであり、主に攻撃者である SideWinder によって使用されます。このマルウェアは、Word、Excel、PDF、またはその他のドキュメントファイルを装った実行ファイルです。バックドアがインストールされると、マシン GUID、ユーザー名、CPU、ウイルス対策情報などのシステム情報を収集し（T1082）、HTTP/HTTPS（T1071.001）を使用したコマンドアンドコントロールによって漏洩します。Spyderは、翌日に実行されるようにスケジュールされたタスクを作成できます（T1053.005）。また、追加のペイロードをダウンロードすることもできます（T1105）。

お使いの環境で Spyder が検出されたかどうかを確認するには、[Spyder Backdoor 脅威の詳細（Spyder Backdoor 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。

AsyncRAT

AsyncRAT は当初、NYAN-x-CAT によってオープンソースのリモート管理ツールとして開発されました。当初は C# で記述されていましたが、他の開発者が Python と Java に適応させました。DcRAT（別名 DarkCrystal RAT）などのマルウェアは、AsyncRAT のクローンです。その汎用性の高い機能から、攻撃者の間で人気があります。AsyncRAT は、画面の録画と表示

（T1113）、コマンドの実行（T1059）、ファイルのアップロードとダウンロード（T1105）、および被害デバイスでのパスワードの回復（T1003）を実行できます。.NET フレームワークバイナリに挿入され（T1055.002）、ダイナミック DNS ベースのコマンドアンドコントロールサーバーに接続される（T1583.001）ことが確認されています。

お使いの環境で AsyncRAT が検出されたかどうかを確認するには、[AsyncRAT 脅威の詳細（AsyncRAT 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。