2022 年 11 月

2022 年 11 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。

- ChromeLoader
- CryptBot
- Mispadu
- Pterodo

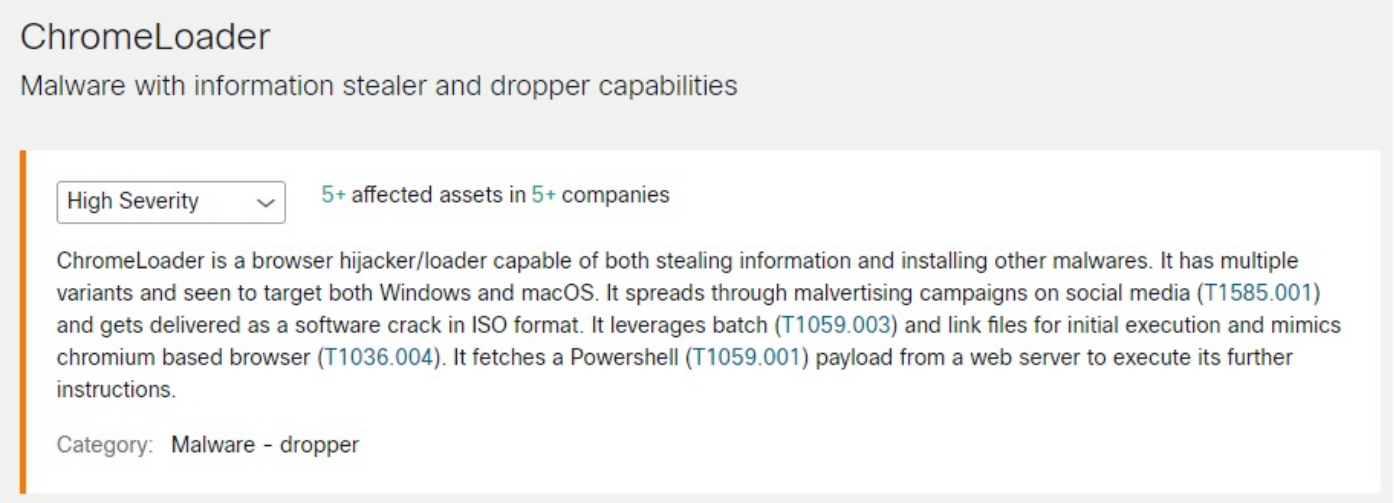
また、既存の脅威検出のインジケーターも更新しました。

ChromeLoader

ChromeLoader は、情報を盗み、他のマルウェアをインストールすることができるブラウザハイジャッカー/ローダーです。複数のバリアントがあり、Windows と macOS の両方を標的としています。ソーシャルメディア（T1585.001）上のマルバタイジング攻撃を通じて拡散し、ISO 形式のソフトウェアクラックとして配信されます。バッチ（T1059.003）とリンクファイルを初期実行に活用し、Chromium ベースのブラウザ（T1036.004）を模倣します。Web サーバーから Powershell（T1059.001）ペイロードを取得して、さらに命令を実行します。

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

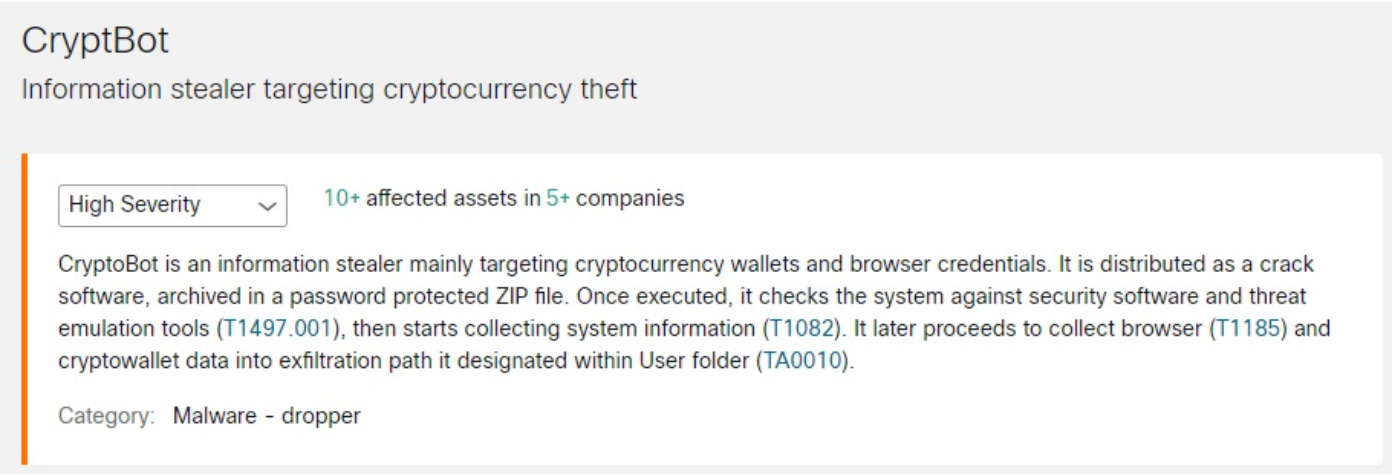


CryptBot

CryptBot は、主に暗号通貨ウォレットとブラウザのログイン情報を標的とする情報窃盗マルウェアです。これはクラックソフトウェアとして配布され、パスワードで保護された ZIP ファイルにアーカイブされています。実行されると、セキュリティソフトウェアと脅威エミュレーションツール（T1497.001）に対してシステムをチェックし、システム情報（T1082）の収集を開始します。その後、ブラウザ（T1185）と暗号ウォレットのデータを収集し、ユーザーフォルダ（TA0010）内で指定した漏洩パスに移動します。

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

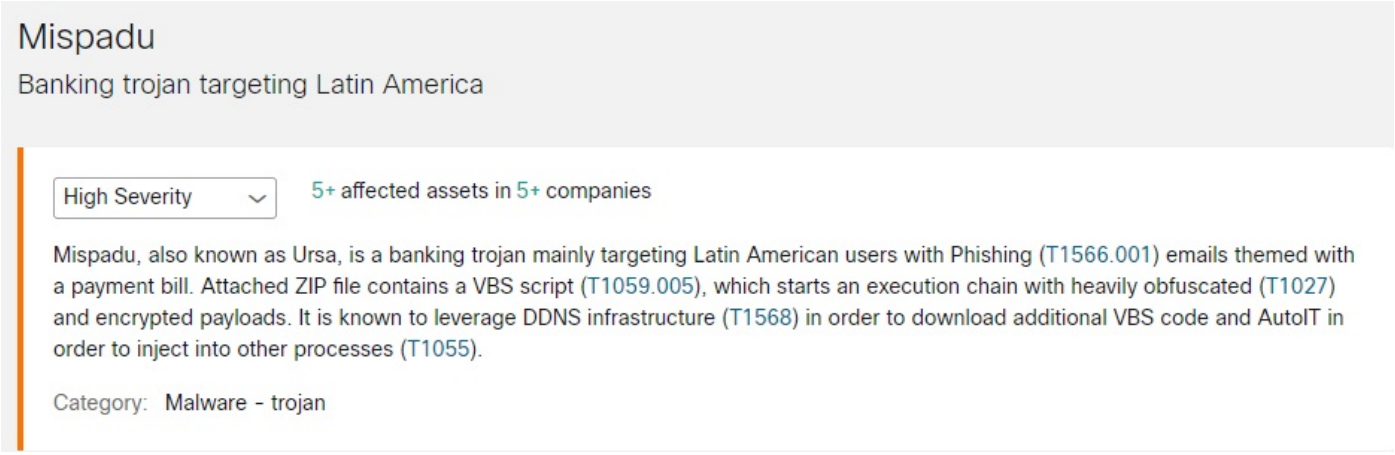


Mispadu

Ursa としても知られる Mispadu は、支払い請求書をテーマにしたフィッシング（T1566.001）メールで主に南米のユーザーを標的にしたバンキング型トロイの木馬です。添付の ZIP ファイルには、高度に難読化（T1027）され暗号化されたペイロードで実行チェーンを開始する VBS スクリプト（T1059.005）が含まれています。DNS インフラストラクチャ（T1568）を利用して、追加の VBS コードと AutoIT をダウンロードして、他のプロセス（T1055）に挿入することが知られています。

お使いの環境で Mispadu が検出されたかどうかを確認するには、[Mispadu 脅威の詳細（Mispadu 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 *3 :*

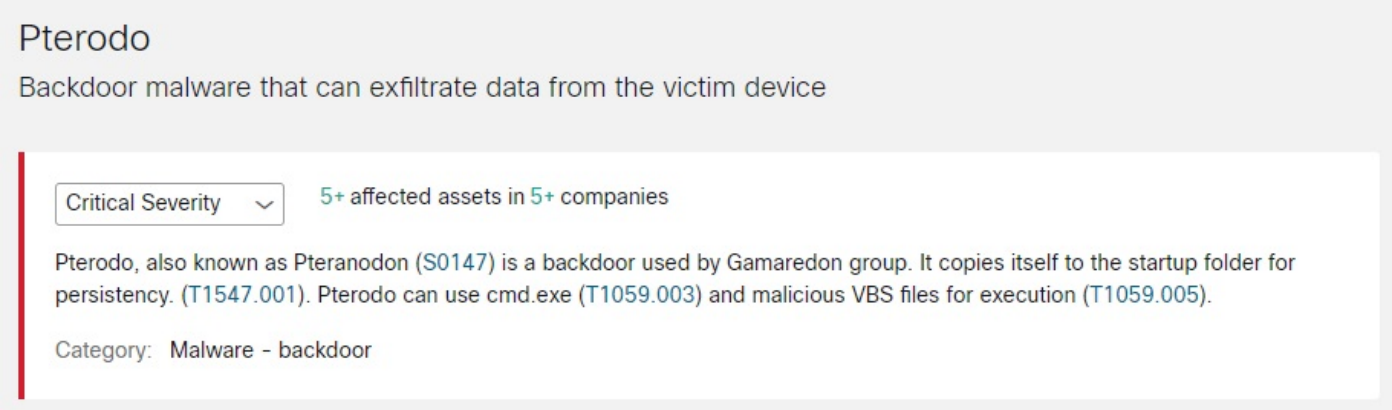


Pterodo

Pteranodon としても知られる Pterodo（S0147）は、Gamaredon グループが使用するバックドアです。永続化（T1547.001）のために自身をスタートアップフォルダにコピーし、cmd.exe（T1059.003）と悪意のある VBS ファイル（T1059.005）を実行に使用します。

お使いの環境で Pterodo が検出されたかどうかを確認するには、[Pterodo 脅威の詳細（Pterodo 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 *4 :*


Pterodo
Backdoor malware that can exfiltrate data from the victim device
Critical Severity
5+ affected assets in 5+ companies
Pterodo, also known as Pteranodon (S0147) is a backdoor used by Gamaredon group. It copies itself to the startup folder for persistency. (T1547.001). Pterodo can use cmd.exe (T1059.003) and malicious VBS files for execution (T1059.005).
Category: Malware - backdoor

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。