2023 年 1 月

2023 年 1 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。

- GootLoader
- Laplas Clipper
- Neoreklami
- Rhadamanthys

また、既存の脅威検出のインジケーターも更新しました。

GootLoader

GootLoader は、ドロッパーマルウェアであり、SEO ポイズニングを介して拡散します（T1608.006）。ユーザーをだまして、悪意のある JS ファイルを含む無害に見える ZIP ファイルをダウンロードさせます。wscript と cscript（T1059.005）を使用して、この初期ペイロードを実行します。スケジュールされたタスク（T1053.005）を通じて永続性を獲得し、C2 トラフィックに Powershell（T1059.001）を活用します。攻撃対象デバイスで CobaltStrike（S0154）をドロップすることが確認されています。そのコマンドアンドコントロールインフラストラクチャは、侵害された WordPress Web サイト（T1584.004）で構成されています。

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

Laplas Clipper

Laplas Clipper は、暗号通貨を盗むマルウェアです。SmokeLoader（S0226）またはフィッシング（T1566）によって配信されます。永続化のために、schtasks（T1053.005）を使用してスケジュールタスクを作成します。 Laplas Clipper は、攻撃対象を模倣したウォレットアドレスを

生成して、通貨トランザクションをハイジャックします。このマルウェアは、ビットコイン、イーサリアム、ビットコインキャッシュ、ライトコイン、ドージコインなど、さまざまなウォレットから盗み出します。

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

Neoreklami

Neoreklami は、ユーザーのブラウザセッションを制御するために AdBlocker を模倣することが知られています（T1185）。永続化のために WSF（T1059.005）および DLL（T1218.011）ファイルを実行するタスク（T1053.005）をスケジュールします。これらのファイルを保存するために、ProgramData および Program Files（x86）内にランダムな英数字で名前が付けられたフォルダが作成されます。ユーザーのブラウザセッションに感染すると、難読化されたペイロード（T1027）をダウンロードして次のアクションを決定します。感染したデバイスは、ハイパーリンクに変換されたランダムな Web ページテキスト、正当な Web ページが挿入された広告バナー、偽の更新を推奨するポップアップなどを表示する可能性があります。

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

Rhadamanthys

Rhadamanthys は、感染したデバイスから情報を抽出して抜き取る情報窃取プログラムです。最初のアクセスは、AnyDesk、Zoom、Notepad++ などのアプリケーションの偽のソフトウェア配布（T1036）によって行われます。このマルウェアを配布するドメインは、Google 広告を悪用し、それらのアプリケーションを偽装することが確認されています。Rhadamanthys マルウェアは、オペレーティングシステムのバージョン、デバイス名、インストールされているソフトウェアなどのデバイス情報とともに、暗号通貨ウォレットに関連する情報を盗みます。このマルウェアは、コマンドアンドコントロール（T1041）を介してデータを盗み出します。

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