2022 年 3 月

2022 年 3 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。

- Cyclops Blink
- FormBook
- Gamaredon
- MuddyWater

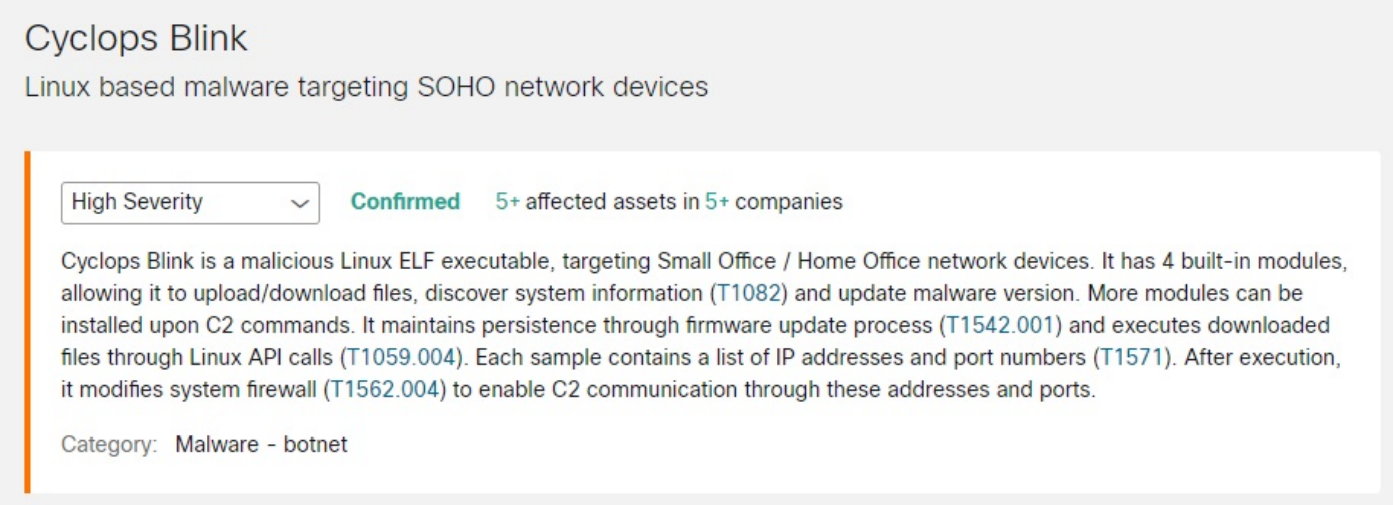
低リスクの脅威検出も多数強化されています。

Cyclops Blink

Cyclops Blink は、悪意のある Linux ELF 実行ファイルであり、スモールオフィス、ホームオフィスのネットワークデバイスをターゲットにしています。4つの組み込みモジュールがあり、ファイルのアップロードとダウンロード、システム情報（T1082）の発見、マルウェアのバージョンの更新を行うことができます。C2 コマンドを使用して、さらに多くのモジュールをインストールできます。ファームウェア更新プロセス（T1542.001）を通じて永続性を維持し、Linux API コール（T1059.004）を通じてダウンロードされたファイルを実行します。各サンプルには、IP アドレスとポート番号（T1571）のリストが含まれています。実行後、システムのファイアウォール（T1562.004）を変更して、これらの IP アドレスとポートを介した C2 通信を有効にします。

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

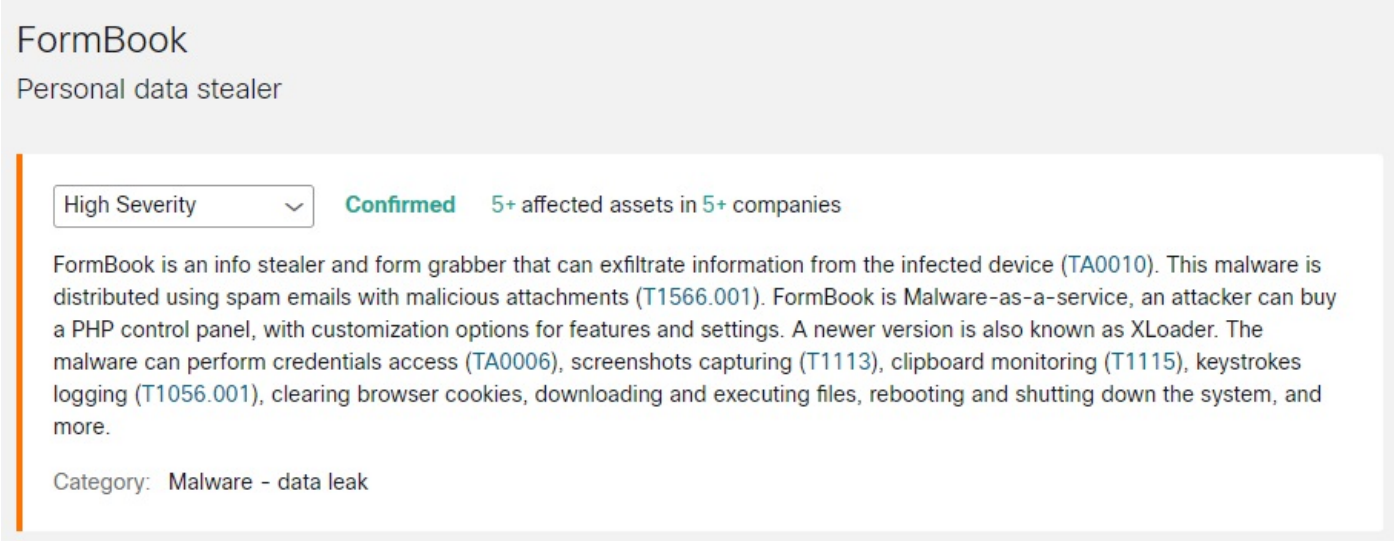


FormBook

FormBook は、感染したデバイス（TA0010）から情報を盗み出す情報窃取およびフォームグラバーです。このマルウェアは、悪意のある添付ファイル（T1566.001）を含むスパムメールを使用して配布されます。FormBook はサービスとしてのマルウェアであり、攻撃者は機能と設定のカスタマイズオプションを備えた PHP コントロールパネルを購入できます。新しいバージョンは XLoader とも呼ばれます。このマルウェアは、ログイン情報（TA0006）へのアクセス、スクリーンショット（T1113）のキャプチャ、クリップボード（T1115）の監視、キーストローク（T1056.001）のログ、ブラウザ Cookie のクリア、ファイルのダウンロードと実行、システムの再起動とシャットダウンなどを行うことができます。

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



Gamaredon

Primitive Bear としても知られる Gamaredon は、サイバースパイ活動の目的で政府組織を標的にすることが多い、国家レベルの攻撃者です。ロシアとウクライナの間の緊張が高まった後、グループの活動が活発になりました。Gamaredon は、攻撃の第 1 段階として、スピアフィッシング（T1566.001）を介して配布された悪意のある Office ファイル（T1204.002）を利用することがよくあります。彼らは、次の段階で PowerPunch と呼ばれる Powershell（T1059.001）ビーコンを使用して、マルウェア（T1204.002）をダウンロードして実行することが知られています。Pterodo（S0147）と QuietSieve は、情報（TA0010）を盗んだりその他のさまざまなアクションを目的としてよく導入されるマルウェアファミリです。

お使いの環境で Gamaredon アクティビティが検出されたかどうかを確認するには、[Gamaredon アクティビティの脅威の詳細（Gamaredon Activity 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。

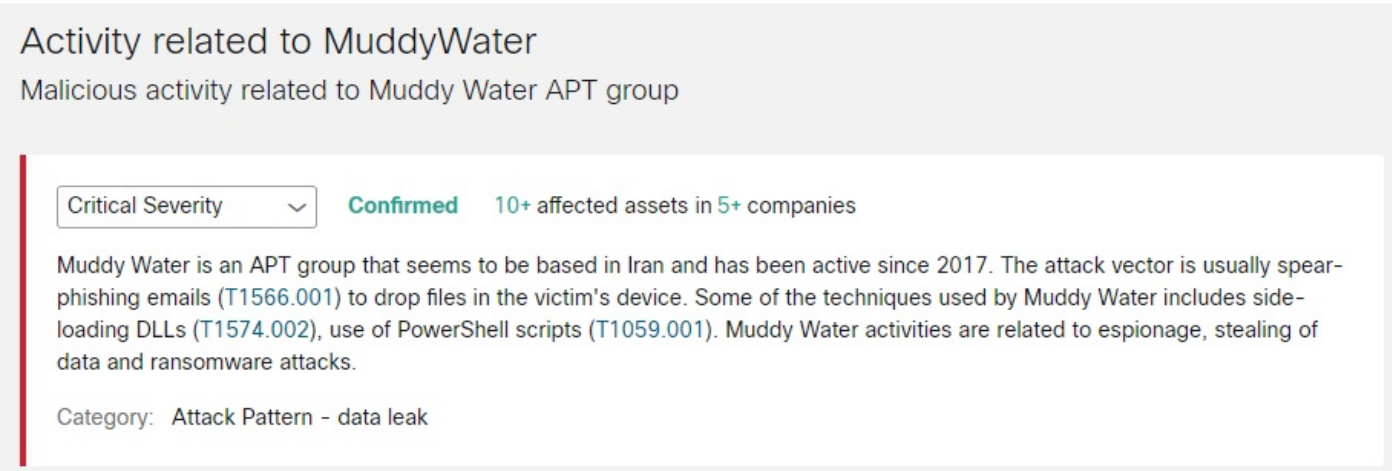
図 *3*:

MuddyWater

MuddyWaterは、イランを拠点としていると思われる高度で連続的な脅威（APT）グループで、2017年から活動しています。攻撃ベクトルは通常、攻撃対象のデバイスにファイルをドロップするスピアフィッシングメール（T1566.001）です。MuddyWater で使用されるテクニックには、サイドローディング DLL（T1574.002）や PowerShell スクリプト（T1059.001）の使用などがあります。MuddyWater の活動は、スパイ活動、データの盗難、ランサムウェア攻撃に関連しています。

お使いの環境でMuddyWaterアクティビティが検出されたかどうかを確認するには、[MuddyWaterアクティビティの脅威の詳細（MuddyWater Activity Threat Detail）] をクリックして、グローバル脅威アラートでその詳細を表示します。

図 *4*:



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。