2022 年 6 月

2022 年 6 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。

- AutoKMS ハックツール
- Raspberry Robin
- UNC2447 アクティビティ

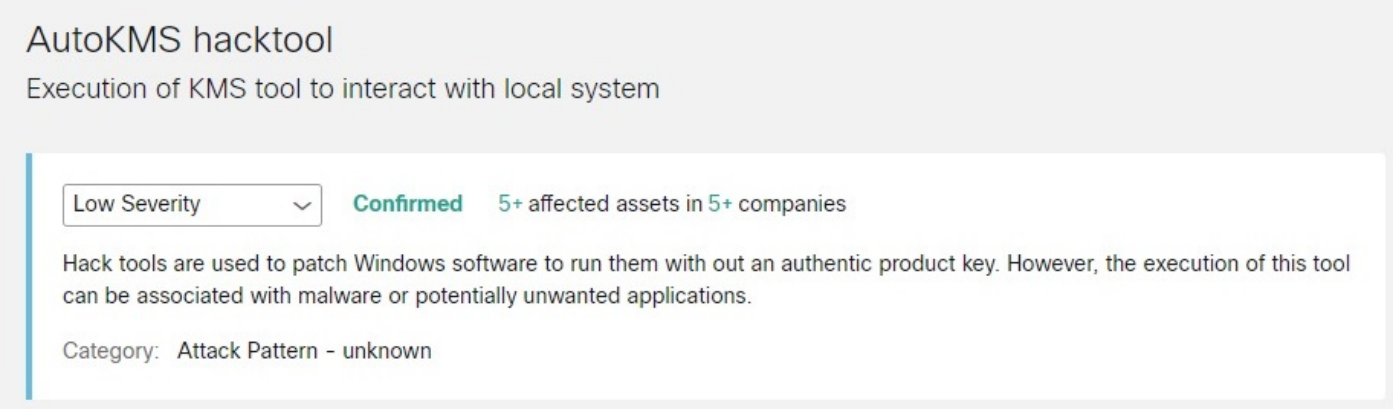
また、既存の脅威検出のインジケーターも更新しました。

AutoKMS ハックツール

ハックツールは、Windows ソフトウェアにパッチを適用して製品認証キーなしで実行するために使用されます。しかし、このツールの実行は、マルウェアや望ましくない可能性のあるアプリケーションに関連付けられている可能性があります。

お使いの環境で AutoKMS ハックツールが検出されたかどうかを確認するには、[AutoKMSハックツール脅威の詳細（AutoKMS HackTool 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*:



Raspberry Robin

Raspberry Robin は、外部ドライブから .lnk（T1204.002）ファイルを介してマシンに感染し、msiexec.exe（T1218.007）で実際のペイロードをダウンロードし、rundll32.exe（T1218.011）でコードを実行し、TOR 接続（S0183）を介して C2 を確立します。そのインフラストラクチャは、侵害された QNAP デバイスに基づくものです。

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

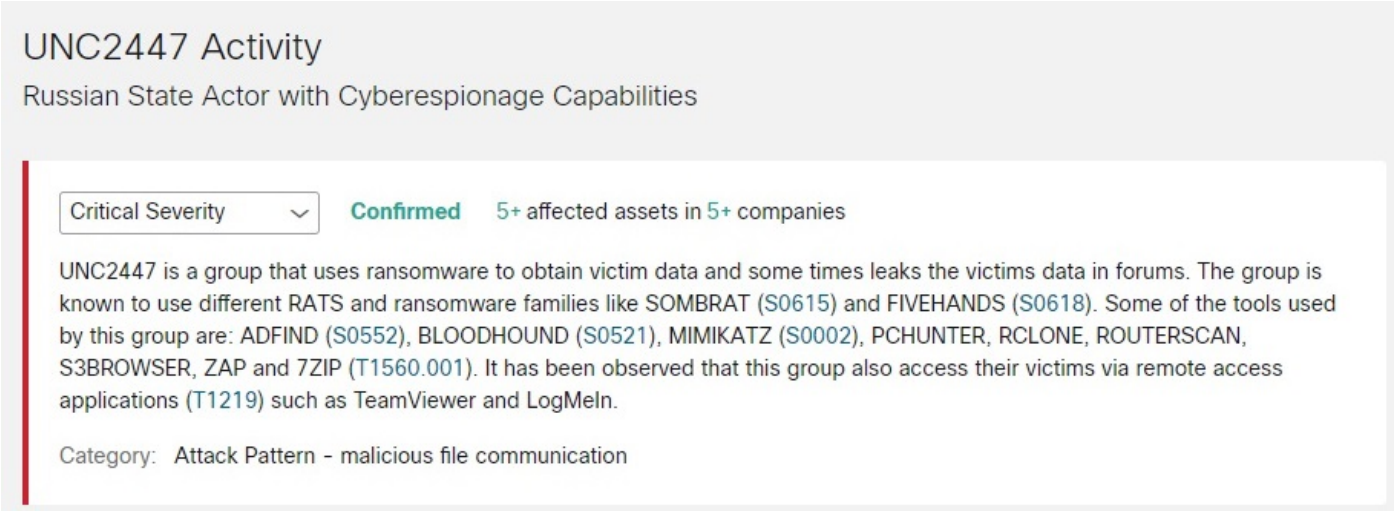
UNC2447 アクティビティ

UNC2447 は、ランサムウェアを使用してデータを取得し、フォーラムで被害者のデータを漏洩する可能性があるグループです。このグループは、さまざまなRATSと、SOMBRAT（S0615）や FIVEHANDS（S0618）などのランサムウェアファミリを使用することが知られています。ADFIND（S0552）、BLOODHOUND（S0521）、MIMIKATZ（S0002）、PCHUNTER、RCLONE、ROUTERSCAN、S3BROWSER、ZAP、7ZIP（T1560.001）などのツールがこのグ

ループに使用されます。また、このグループは、TeamViewer や LogMeIn などのリモート アクセス アプリケーション（T1219）も使用します。

お使いの環境でUNC2447アクティビティが検出されたかどうかを確認するには、[UNC2447アクティビティ脅威の詳細（UNC2447 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 :*



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。