



2022年7月

2022年7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。

- [SSO を CCI に移行 \(1 ページ\)](#)
- [追加の脅威検出 \(1 ページ\)](#)

SSO を CCI に移行

カスタマーエクスペリエンスを向上させるために、シングルサインオンが Cisco Customer Identity (CCI) ポータルに移行されました。引き続き [Cisco SSO] をクリックし、[id.cisco.com] で電子メールとパスワードを入力してログインします。

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。

- Conti
- REvil

また、既存の脅威検出のインジケータも更新しました。

Conti

Conti (S0575) は、通常 Trickbot (S0266) とともに導入されるサービスとしてのランサムウェア (RaaS) です。ビジネスや政府機関のネットワークに侵入することで知られています。Conti は、SMB (サーバーメッセージブロック) (T1021.002) およびファイルの暗号化 (T1486) を使用して水平方向に移動します。データを暗号化するために、Conti はファイルごとに異なる AES-256 暗号化キーと攻撃対象ごとに固有のハードコーディングされた RAS-4096 公開暗号化キーを使用します。暗号化されたファイルの拡張子はランダムに生成され、作成される身代金要求メッセージは「readme.txt」と呼ばれます。Conti には、感染したデバイス (T1049) のネットワーク設定 (T1016) とネットワーク接続を発見する能力があります。

お使いの環境で Conti が検出されたかどうかを確認するには、[\[Conti脅威の詳細 \(Conti Threat Detail\)\]](#) 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:

Conti
Infection with disk encrypting malware

Critical Severity ▼ 5+ affected assets in 5+ companies

Conti (S0575) is a Ransomware as a Service (RaaS) and it is usually deployed with Trickbot (S0266). It is known for breaching networks of businesses and government agencies. Conti moves laterally via SMB (Server Message Block) (T1021.002) and encrypts files (T1486). To encrypt the data, Conti uses a different AES-256 encryption key per file with a hardcoded RAS-40 public encryption key that is unique for each victim. The extension of the files encrypted are randomly generated and the ransom note created is called "readme.txt". Conti has the capacity to discover the network configuration (T1016) and the network connections of the infected device. (T1049).

Category: Malware - ransomware

REvil

REvil (S0496) は、Sodinokibi および Sodin としても知られるサービスとしてのランサムウェア (RaaS) です。感染は通常、攻撃対象が感染した Web サイト (T1189) または悪意のある MS Word 添付ファイル (T1204) を含むフィッシングメール (T1566) にアクセスしたときに始まります。REvil には、攻撃対象のデバイス上のファイルを暗号化 (T1486) および破壊 (T1485) する能力があります。

お使いの環境で REvil が検出されたかどうかを確認するには、[\[REvil脅威の詳細 \(REvil Threat Detail\)\]](#) 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:

REvil

Infection with disk encrypting malware

Critical Severity



5+ affected assets in 5+ companies

REvil (S0496) is a Ransomware, also known as Sodinokibi and Sodin. It has been operated as Ransomware as a Service (RaaS). The infection usually starts when the victim access to infected websites (T1189) or via phishing e-mails (T1566) with malicious MS Word attachments (T1204). REvil has the capacity to encrypt (T1486) and destroy (T1485) the files in the victims device.

Category: Malware - ransomware

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。