2023 年 10 月

2023 年 10 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

新しい脅威検出をポートフォリオに追加しました。

- DarkGate Loader

また、既存の脅威検出のインジケーターも更新しました。

DarkGate Loader

DarkGate Loader（MehCrypter とも呼ばれます）は、QakBot の亜種です。このローダーは、Microsoft Teams メッセージを悪用して、DarkGate Loader をインストールする悪意のある添付ファイルを送信するフィッシングキャンペーン（T1566）によって配布されます。マルウェアがエンドポイントで実行されると（T1204.002）、リモートアクセス（T1219）、暗号通貨マイニング（T1496）、キーロギング（T1056.001）、クリップボード窃盗、情報窃盗など、さまざまな悪意のあるアクティビティが発生する可能性があります。

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