おまかせサイバーみまもり

2025年8月　セキュリティ対応状況と検知状況

2025年9月
NTT東日本株式会社

セキュリティ対応状況

2025年8月6日（現地時間）にZenity Labsより、ChatGPTの「Connectors」機能を悪用したゼロクリック攻撃手法が報告されています。この攻撃は、ChatGPTがGoogleドライブやSharePointなどのサードパーティアプリケーションに接続できる「Connectors」機能を悪用し、悪意のあるファイルを読み込ませることで機密情報を盗み取る手法となります。

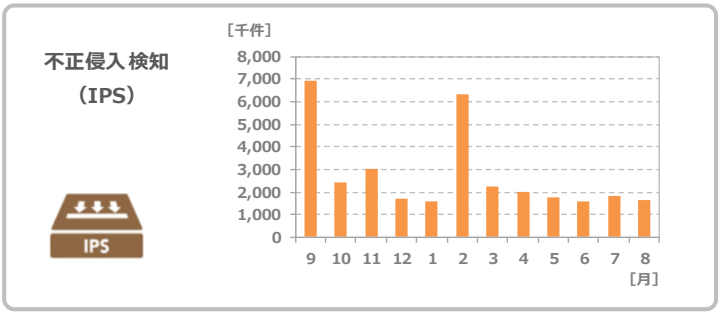
このような攻撃は、AIツールを業務で活用する企業や組織にとって深刻な脅威となり得ます。社内でAIを使って文書の要約や分析を行う場合、意図せず機密情報が外部に漏れるリスクがあるため、読み込ませるファイルについては注意が必要です。特にインターネット上から取得したファイルのアップロードについては、ご注意ください。 エンドユーザの対策としては、ChatGPTなどAIツールへ不必要なファイルのアップロードをしないことがあげられます。

■参考：Zenity Labs
https://labs.zenity.io/p/agentflayer-chatgpt-connectors-0click-attack-5b41

セキュリティ検知状況

- おまかせサイバーみまもり専用BOXで検知したアラート数をNTT東日本が集計
- 集計期間：2024年9月～2025年8月

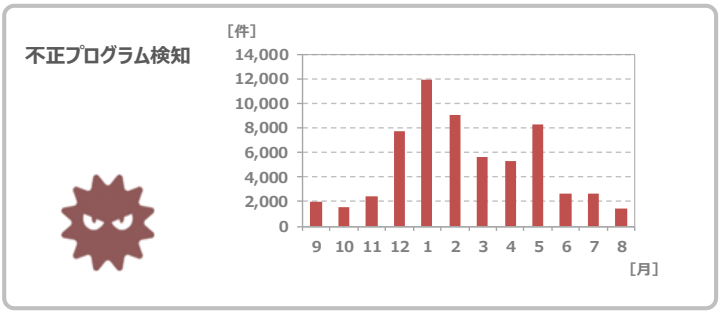
不正侵入検知



直近12カ月平均：2,748,398件
2025年8月：1,633,723件

直近12カ月の月平均に比べ低い検知状況が継続しています。
引き続きサーバ等を公開する際には十分にセキュリティ対策を実施してください。

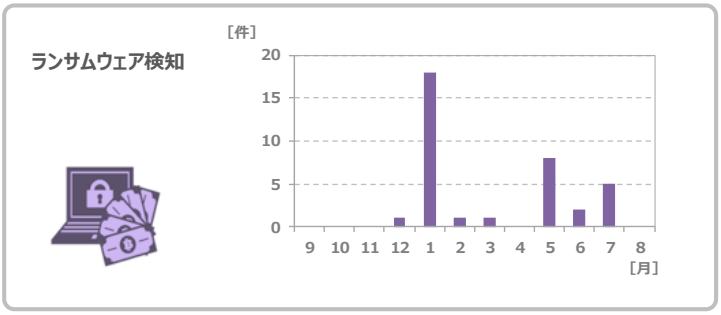
不正プログラム検知



直近12カ月平均：5,069件
2025年8月：1,458件

直近12カ月の月平均に比べ低い検知状況となりました。
インフォスティーラー(Infostealer)※1などの不正プログラムについては、引き続き十分に注意してください。

ランサムウェア検知



直近12カ月平均：3件
2025年8月：0件

8月は検知数が0件となり、直近12カ月の月平均に比べ低い検知状況となっています。
ランサムウェアには、引き続き十分に注意してください。

※1：感染した端末から機密情報を密かに盗み出すことを目的としたマルウェア(不正プログラム)の一種。
パスワード、クレジットカード情報、内部ファイルなど、あらゆる情報を盗み取るために設計されたマルウェアのこと。