おまかせサイバーみまもり

2025年12月　セキュリティ対応状況と検知状況

2026年1月
NTT東日本株式会社

セキュリティ対応状況

BlackFog社より、「Matrix Push C2」と呼ばれる新しいC2（コマンド＆コントロール）ツールを利用した攻撃について報告されております。実際の攻撃手法としては、ブラウザのプッシュ通知機能を悪用することで、正規の電子決済サービスやセキュリティアラートなどを装った偽の通知を表示し、ユーザをフィッシングサイトやマルウェアのダウンロードサイトへ誘導するものとなります。その結果、認証情報や機密情報などの漏洩や、ランサムウェア感染による端末のファイル暗号化などにつながる可能性があります。

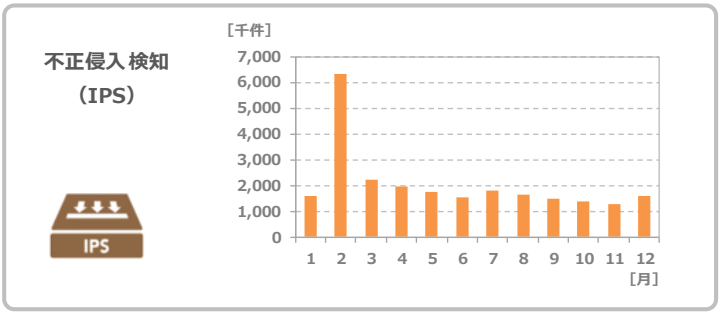
エンドユーザ視点の対策としては、通知許可を求めるポップアップが表示された場合においても安易に承認しないこと、ポップアップが表示されたサイトのドメインが正規のドメインであるか確認することが重要です。

■参考BlackFog
https://www.blackfog.com/new-matrix-push-c2-deliver-malware/

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：2025年1月～2025年12月

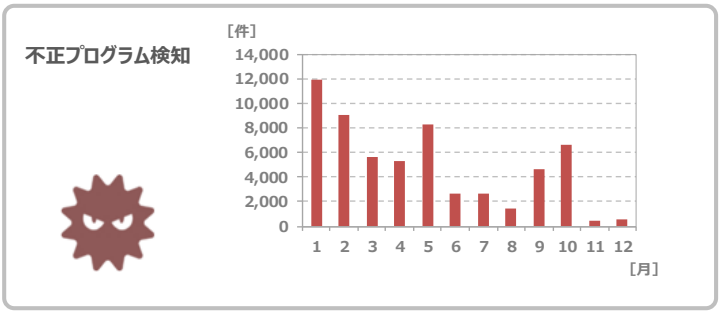
不正侵入検知



直近12カ月平均：2,056,568件
2025年12月：1,610,554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。

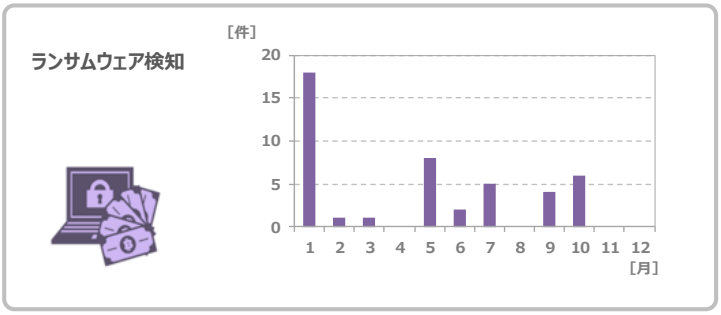
不正プログラム検知



直近12カ月平均：4,949件
2025年12月：　602件

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。
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：4件
2025年12月：0件

12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。