



2025年5月 セキュリティ対応状況と検知状況

2025年6月
東日本電信電話株式会社

セキュリティ対応状況

Morphisecより、偽のAIツールを装い、情報窃取を目的としたマルウェア「Noodlophile」に感染させるサイバー攻撃について報告がされています。今回の攻撃では、ソーシャルメディア上にてAIを活用したコンテンツ制作ツールを宣伝し、ユーザが当該ツールを利用した際の生成物としてマルウェアが含まれたzipファイルをダウンロードするように誘導しています。

その後、ユーザがダウンロードしたzipファイルを展開・実行すると、ブラウザの認証情報・機密データ等の情報窃取を目的としたマルウェア「Noodlophile」に感染するものとなっています。

対策としては、業務上不要なAIツールを利用しないことが挙げられます。また、市中のAIツールを利用する際は、その提供元を慎重に確認するとともに、特にソーシャルメディアの投稿や第三者サイトで提供されるAIツールにご注意ください。

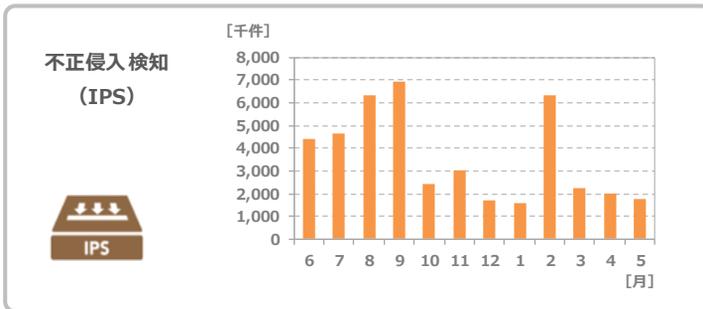
■参考 Morphisec

<https://www.morphisec.com/blog/new-noodlophile-stealer-fake-ai-video-generation-platforms/>

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6月～2025年5月

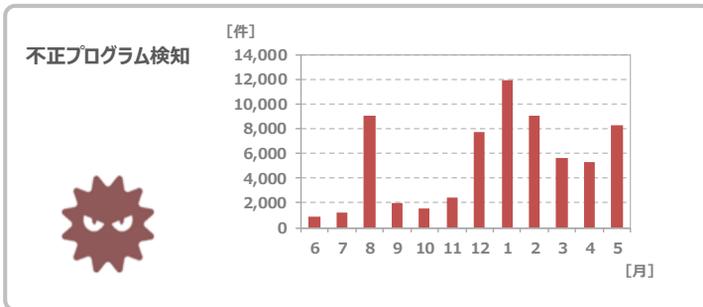
不正侵入検知



直近12カ月平均：3,611,911件
2025年5月：1,767,971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。

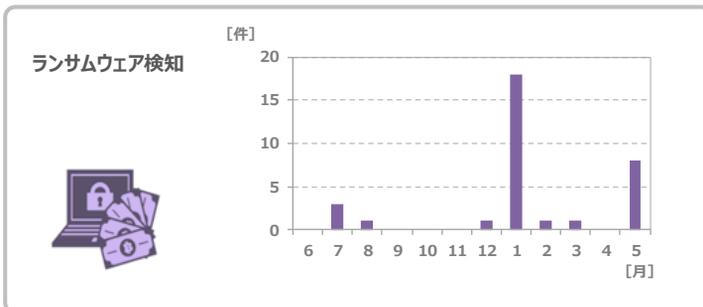
不正プログラム検知



直近12カ月平均：5,440件
2025年5月：8,264件

直近12カ月の月平均に比べ高い検知状況が継続しています。Emotet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5月：8件

5月は検知数が8件となり、直近12カ月の月平均に比べ高い検知状況となりました。ランサムウェアには、引き続き十分に注意してください。