おまかせサイバーみまもり

2024年1月　セキュリティ対応状況と検知状況

2024年2月
東日本電信電話株式会社

セキュリティ対応状況

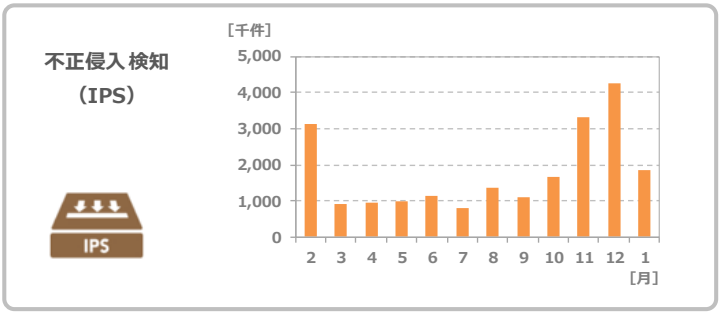
海賊版・違法コピーソフトウェアを装ってダウンロードさせるマルウェア「Lumma Stealer」の亜種の活動が確認されております。
今回確認された手法としてはYouTubeにて海賊版・違法コピーソフトウェアを宣伝する動画をアップロードし、その動画の概要欄や固定コメントにリンク先を記載しダウンロードすることを誘導します。この際、既に侵害した知名度の高いアカウントになりすまして動画をアップロードする事で、ユーザの警戒心を解く手口が用いられます。
また、リンク先はGitHubやMediaFireなどのオープンソースプラットフォームを利用されており、UTMなどのWebフィルタ機能を回避しようとする動きも確認されております。エンドユーザ視点の対策としては信頼できる公式サイトから配布される正規のソフトウェア以外は使用しないといった対策が重要となります。

■参考　マイナビ
https://news.mynavi.jp/techplus/article/20240112-2861136/

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：2023年2月～2024年1月

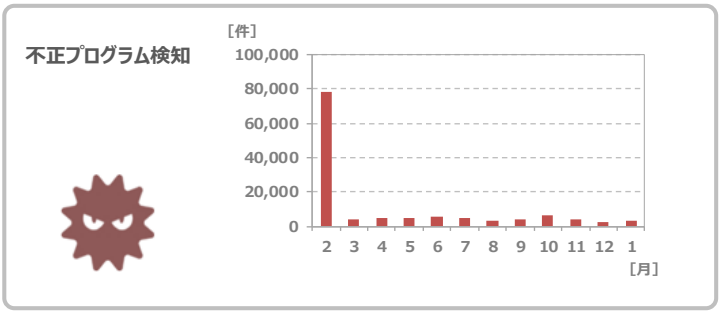
不正侵入検知



直近12カ月平均：1,792,515件
2024年1月：1,849,631件

先月に比べ検知数は減少しましたが、直近12カ月の月平均に比べ高い検知状況が継続しております。
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。

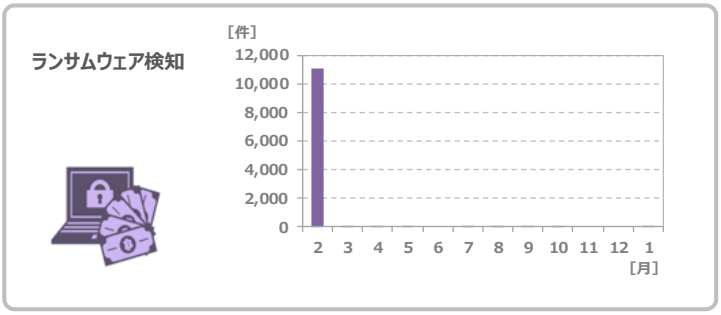
不正プログラム検知



直近12カ月平均：10,286件
2024年1月：3,051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。
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：932件
2024年1月：2件

1月は検知数が2となり、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。
ランサムウェアには、引き続き十分に注意してください。