おまかせサイバーみまもり

2024年6月　セキュリティ対応状況と検知状況

2024年7月
東日本電信電話株式会社

セキュリティ対応状況

2024年5月21日（現地時間）に、SecuronixよりDropboxやGoogle Driveを悪用してマルウェアを配布し、機密情報を窃取する新たな攻撃キャンペーン「CLOUD#REVERSER」が報告されております。本攻撃キャンペーン「CLOUD#REVERSER」では、攻撃者がフィッシングメールをユーザへ送信し、ユーザにフィッシングメールに添付された悪意ある添付ファイル（zipアーカイブ）を展開・ファイルの実行をさせることでマルウェアへの感染を狙っております。特徴的な手法としては、古くから存在する「横文字の流れを右から左へ変更するRLO制御文字」を用いたファイル種別（ファイル拡張子）の偽装、アイコンの偽装、及びDropboxやGoogle Driveを悪用したマルウェアの追加ダウンロード、機密情報のアップロードがあげられます。

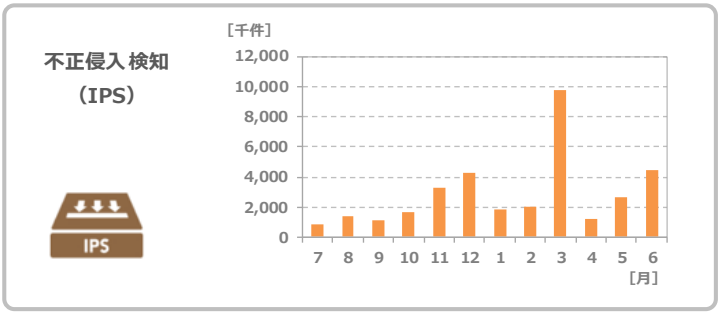
対策としては端末の不審な挙動を検知可能とするEDR（Endpoint Detection and Response）が攻撃の早期発見・防御への有効な手段の1つとなります。

■参考　マイナビ　https://news.mynavi.jp/techplus/article/20240531-2950851/

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7月～2024年6月

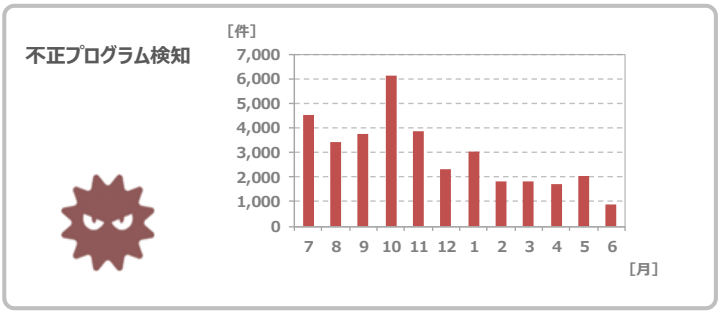
不正侵入検知



直近12カ月平均：2,869,990件
2024年6月：4,433,606件

直近12カ月の月平均に比べ高い検知状況となりました。
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。

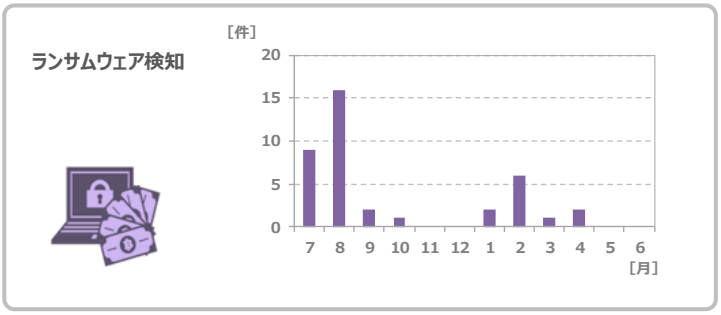
不正プログラム検知



直近12カ月平均：2,954件
2024年6月：0,888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：3件
2024年6月：0件

6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。