おまかせサイバーみまもり

2023年2月　セキュリティ対応状況と検知状況

2023年3月
東日本電信電話株式会社

セキュリティ対応状況

Emotetに類似したマルウェアである「IcedID」について、従来の添付付きメールによる手口ではなく、マルバタイジング※手法を用いて感染を狙った手口が増加しております。Google検索では、キーワード検索をした際の最上部など目立つ場所に、キーワードに関連する「広告」とタグがついたリンクが表示されます。この広告欄に、ユーザが検索したアプリケーションの配布サイトを装った偽のリンクを広告として掲載することで広告を1件目の検索結果だと誤認したユーザにそのリンクをクリックさせ、正規のアプリケーションに偽装されたマルウェアをインストールしてしまうという手口が確認されています。

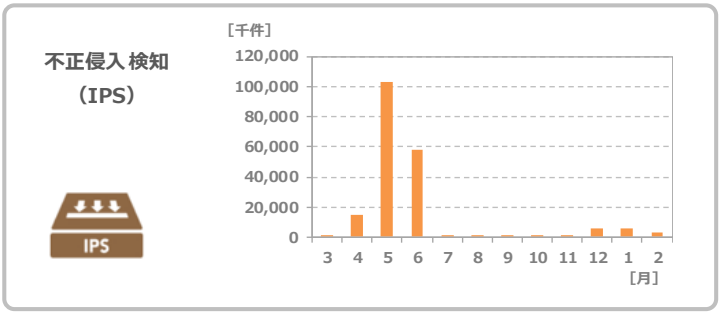
対策としては、検索結果として表示された「広告」とついたリンクを不用意にクリックしない、リンクをクリックする前にドメインやURLの確認を行う、といった基本的な対策が重要となります。

※ マルウェアの拡散や不正なサイトへのリダイレクトを目的とした悪質なWeb広告を掲載する手法

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：2022年3月～2023年2月

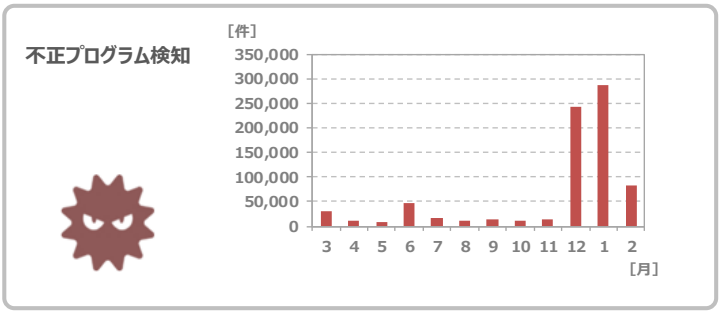
不正侵入検知



直近12カ月平均：16,493,693件
2023年2月：3,377,512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。

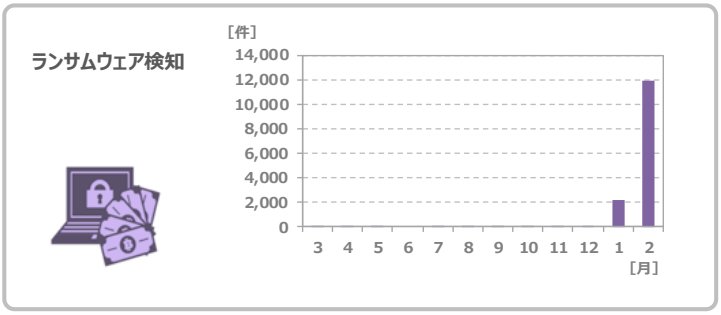
不正プログラム検知



直近12カ月平均：64,778件
2023年2月：83,826件

直近12カ月の月平均と比べ高い検知数となりました。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：1,183件
2023年2月：11,944件

直近12カ月の中で最大の検知数となりました。ランサムウェアには、引き続き十分に注意してください。