おまかせサイバーみまもり

2023年3月　セキュリティ対応状況と検知状況

2023年4月
東日本電信電話株式会社

セキュリティ対応状況

2023年3月8日にJPCERTコーディネーションセンター（JPCERT/CC）よりマルウェアEmotet※の感染再拡大に関して注意喚起が行われました。今回観測された新たな特徴として、メールに添付されるzipファイルを展開すると500MBを超えるdocファイルが解凍される手法があります。このようなzipファイルは一般的に高圧縮ファイル爆弾やZIP爆弾と呼ばれております。これはzipファイルを読み込んだシステムをクラッシュさせたり、負荷をかけることでシステムを使用不能にすることを目的としており、アンチウィルス製品などの検出回避を図っていると考えられます。

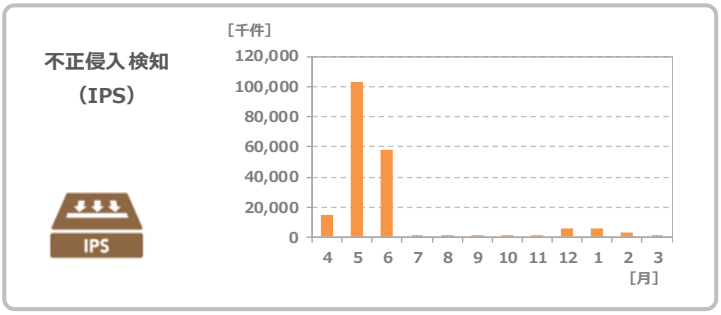
このような従来のセキュリティ対策を回避する仕組みが組み込まれた攻撃などを防ぐセキュリティ対策強化の一環として、感染時の早期発見・被害拡大防止を支援するEDR (Endpoint Detection and Response)製品など複数のセキュリティ対策を組み合わせる事が重要となります。

※　正当な送信者になりすまし被害者にOffice文書を開かせる等の方法によって感染を拡大させるマルウェアです。

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4月～2023年3月

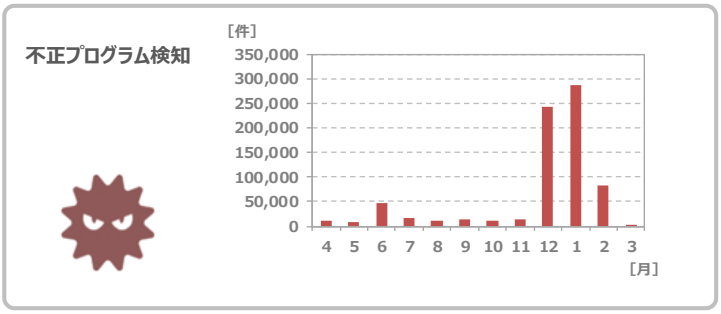
不正侵入検知



直近12カ月平均：16,472,212件
2023年3月：984,003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。

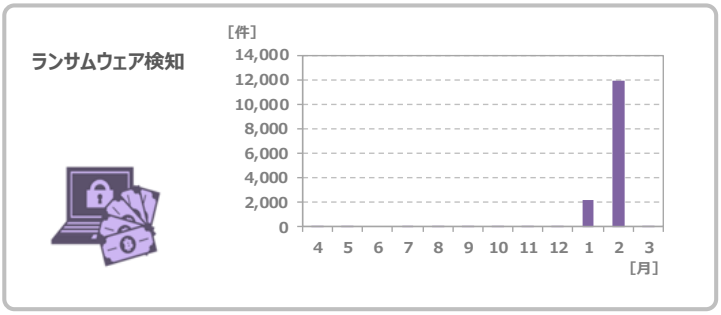
不正プログラム検知



直近12カ月平均：62,538件
2023年3月：4,029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：1,185件
2023年3月：18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。
ランサムウェアには、引き続き十分に注意してください。