おまかせサイバーみまもり

2024年7月　セキュリティ対応状況と検知状況

2024年8月
東日本電信電話株式会社

セキュリティ対応状況

2024年7月21日（現地時間）にTrend Microより「CrowdStrike社のセキュリティ製品のアップデートを起因とする世界的ブルースクリーン障害（BSoD）に便乗したサイバー攻撃」について注意喚起が行われております。

本障害の原因は、CrowdStrike社のセキュリティ製品であるFalconと呼ばれるエンドポイントセキュリティソリューションのセンサー設定の更新であると発表されており、世界的にも多くの企業に導入されていること、Windows端末が影響を受けることから世界的に話題となっております。そのため、これらに便乗したサイバー攻撃が報告されております。

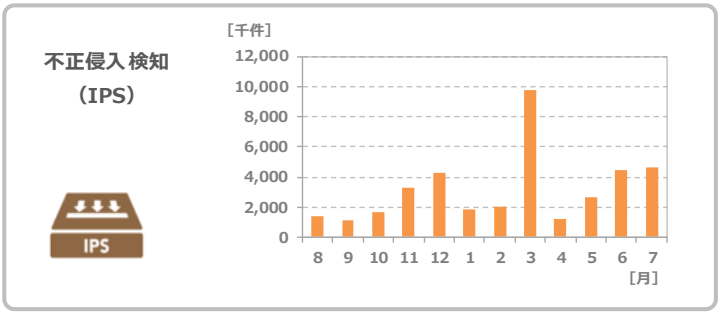
特に、影響を受けた企業等に支援を提供するといった技術サポートを装った詐欺や、リンクのクリックや添付ファイルを開くことを狙ったフィッシングメール等に注意が必要です。エンドユーザ視点の対策としては、リンク先のURLが正規のWebサイトかを確認する、不審なメールに添付されているリンクやファイルを開かないことが重要となります。

※参考　Trend Micro：　https://www.trendmicro.com/ja_jp/research/24/g/crowdstrike-windows-outage-insights.html

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8月～2024年7月

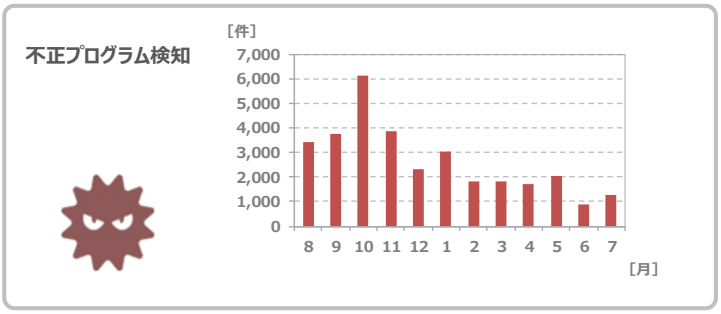
不正侵入検知



直近12カ月平均：3,189,360件
2024年7月：4,649,571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。
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。

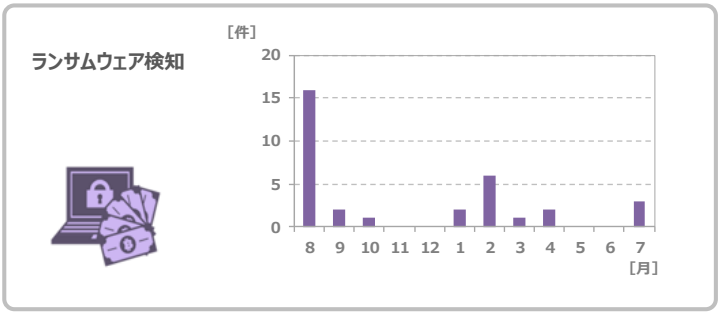
不正プログラム検知



直近12カ月平均：2,683件
2024年7月：1,256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7月：3件

7月は検知数が3件となり、直近12カ月の月平均と同等の検知状況となっています。
ランサムウェアには、引き続き十分に注意してください。