おまかせサイバーみまもり

2024年2月　セキュリティ対応状況と検知状況

2024年3月
東日本電信電話株式会社

セキュリティ対応状況

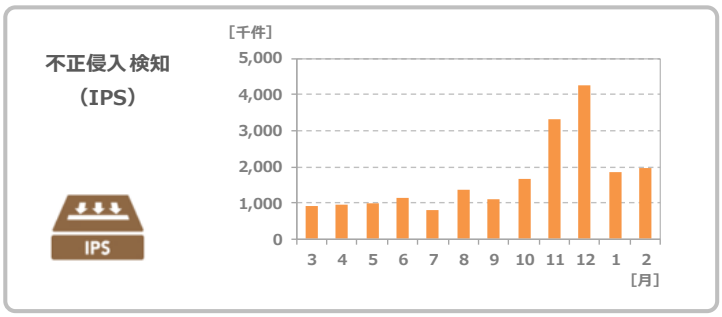
企業に人気のクラウドアプリケーションであるTeamsやSkypeのユーザーにマルウェア「DarkGate」をインストールさせる手口が活性化しております。確認されている手口としてはTeams上で外部ユーザーとしてメッセージを標的に送信し、二重拡張子を持つファイル(“XXX.pdf.msi”というように、.pdfと.msiの2つの拡張子が設定されたファイル)をダウンロードさせます。このファイルを実行してしまうとDarkGateのC&Cドメイン（攻撃者がマルウェアに指令を出したりするサーバ群）へ接続されてしまいます。どのアプリケーションから入手したファイルであっても不審なファイルは開かないといった基本対策を徹底することが重要です。また、ブラウザの更新を騙ったWebサイト（広告）へ誘導してDarkGateに感染させるといった手口も確認されています。ブラウザの更新などを実施する必要があるときは、「信頼できる正規のサイトからのみダウンロードする」※ことも重要な対策です。

参考1_Yahooニュース：https://news.yahoo.co.jp/expert/articles/c3cefcc8a6b302ff90471f6dcd00e4e52bccd89b
参考2_日本サイバー犯罪対策センター：https://www.jc3.or.jp/threats/examples/article-535.html
※　https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/enduser/enduser_case_17.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3月～2024年2月

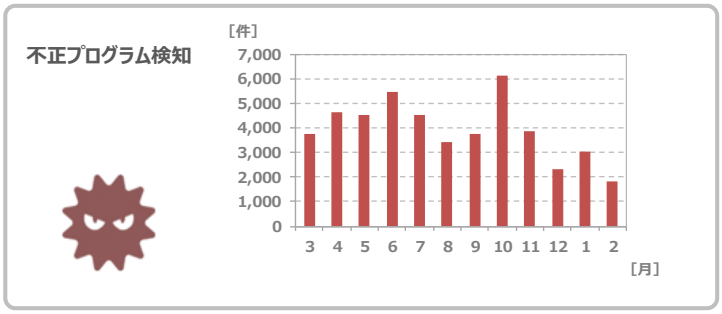
不正侵入検知



直近12カ月平均：1,697,357件
2024年2月：1,976,709件

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。

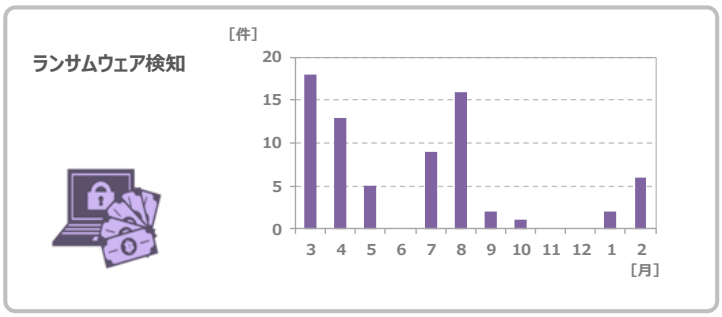
不正プログラム検知



直近12カ月平均：3,951件
2024年2月：1,852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：6件
2024年2月：6件

2月は検知数が6件となり、直近12カ月の月平均に比べ同等の検知状況となります。
ランサムウェアには、引き続き十分に注意してください。