



2024年10月 セキュリティ対応状況と検知状況

2024年11月
東日本電信電話株式会社

セキュリティ対応状況

2024年10月17日（現地時間）にSekoiaよりオンライン会議サービス「Google Meet」のWebサイトを詐称してマルウェアを配布する、新たな攻撃キャンペーンが報告されております。本攻撃キャンペーンでは、Webブラウザに偽のエラーを表示し、修復手順に見せかけた攻撃手順をユーザ自身に実行させる手法であるClickFix戦術が使用されております。

確認されている攻撃手法としては、攻撃者は最初にユーザへ偽の会議への招待状を送付し、Google Meetの正規URLに似せたWebサイトに誘導します。ユーザがWebサイトにアクセスするとマイクやカメラの異常を通知し、修復を促すポップアップが表示され、この時に表示される修復手順の案内に従い操作を実施することで最終的にマルウェアに感染します。

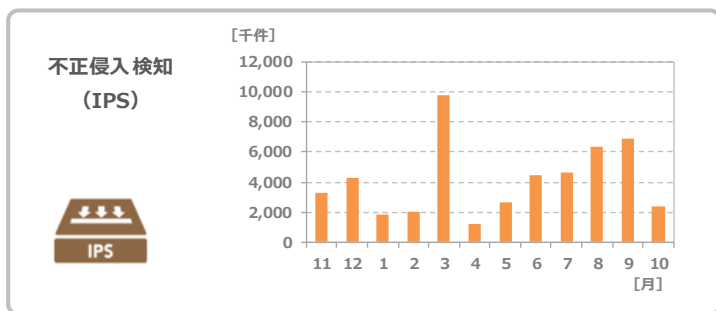
エンドユーザ視点の対策としては、招待状のリンク先のURLが正規のWebサイトかを確認する、不審なメールに添付されているリンクやファイルを開かないことが重要となります。

■参考マイナビ： <https://news.mynavi.jp/techplus/article/20241021-3047078/>

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11月～2024年10月

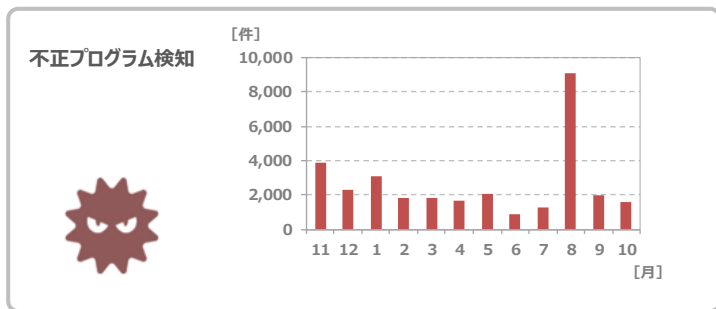
不正侵入検知



直近12カ月平均：4,147,353件
2024年10月：2,421,198件

直近12カ月の月平均に比べ低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。

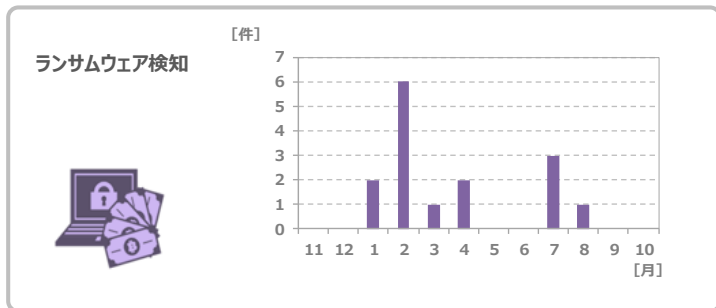
不正プログラム検知



直近12カ月平均：2,623件
2024年10月：1,547件

直近12カ月の月平均に比べ低い検知状況となりました。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件
2024年10月：0件

10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。