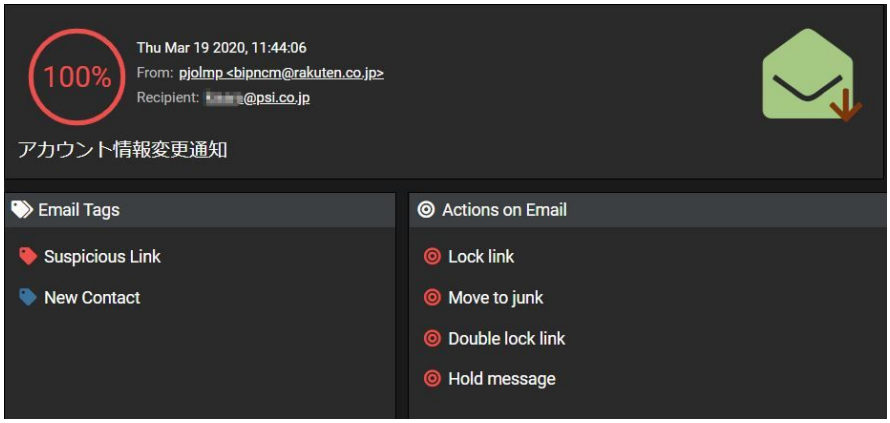
Antigena Email 脅威一例：ソーシャルエンジニアリング

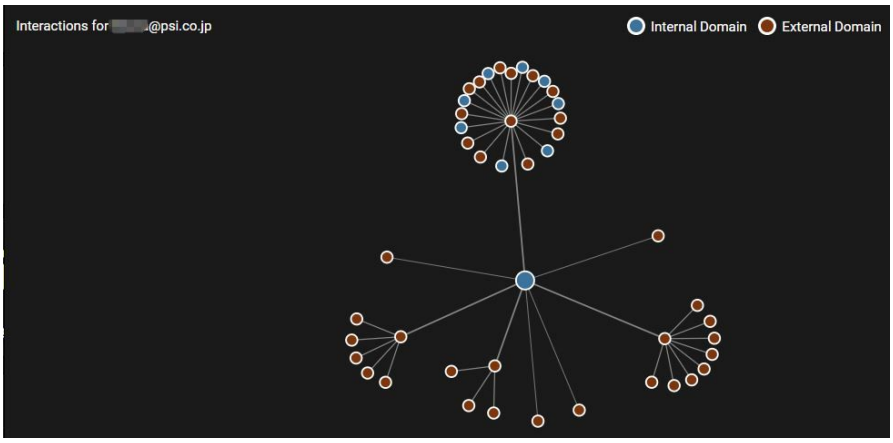
なりすまされたフィッシングメール

Antigena Email は、PSI の役員を宛先とした標的型攻撃性の E メールを検知しました。
一見すると正常に見受けられる E メールですが、Antigena Email はソーシャルエンジニアリング攻撃であるものと判断し、Darktrace の AI はこの E メールが宛先へ届かないようリアルタイムに適切な対処をしました。

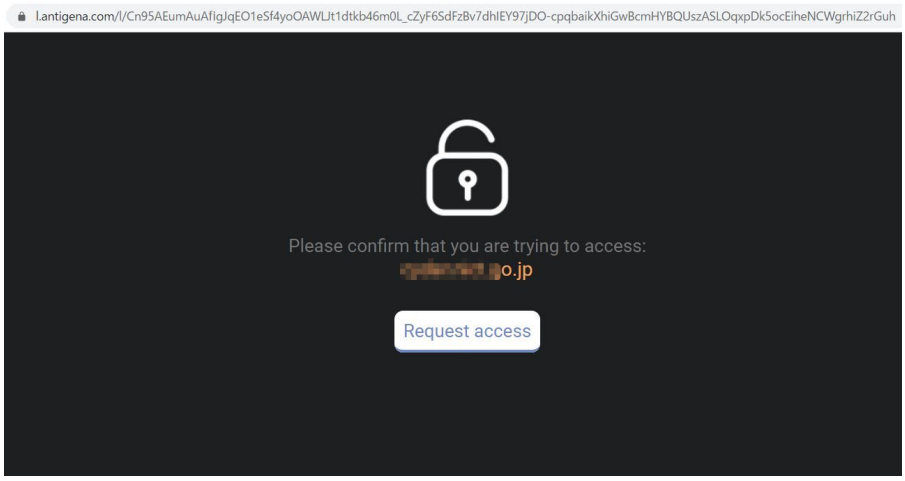
1. メールの件名からは、アカウント情報に関する何かしらの通知のように見受けられ、送信元は正常な EC サイトのドメインを使用していましたが、Antigena Email はこの E メールを 100%定常から逸脱した悪意あるものと識別することができました。



2. Darktrace Antigena Email は、偽装されたドメイン名を識別しただけではなく、この E メールがこれまで見受けられなかった新規のやり取りとなる相手（New Contact）であると識別しました。これは、PSI が利用している E メールとネットワーク環境全体の定常と照らし合わせて、送信元と PSI の間に関係があるという証拠が見つからなかったことを表します。



3. また、E メール内のペイロードには悪意ある URL リンクがあるものとも判断し、この様な複数のインジケータを相関付け、Antigena Email はこの E メールを攻撃の要素であると認識し、E メールを保留するとともに URL リンクをアクセスできないようロックしました。



図：ロックされた E メール内の疑わしい URL リンクをクリックした際の表示

以上