あなたの会社を守る情報発信基地

CyberSecurityStation

サイバーセキュリティステーション

「ランサムウェア」と「エモテット」

サイバー攻撃による個人情報の漏えいなどにより社会的損失が生じた場合、経営責任が問われることになりかねません。そこで、最近のサイバー空間の脅威について2つご紹介するとともに、誰でも取り組みやすい対策についてご紹介させていただきます

ランサムウェア

【主な感染経路】
○メールの添付ファイルやメール本文中のリンクを開かせる
○改ざんしたウェブサイトにアクセスさせて、ランサムウェアをダウンロードさせる

データの暗号化

社内ネットワーク上のパソコン等の端末やサーバ上のデータが利用不能に…

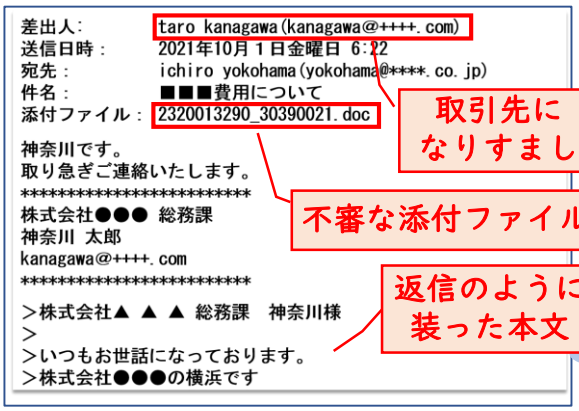
データを人質に身代金を要求

データの復旧したければ…
データを暴露されたくなければ…

更に詳しくは「サイバーセキュリティステーション 二次元コード紹介」の二次元コードからご確認下さい。

エモテット

【主な手口】
○メールに添付されたOffice文書（WordやExcel等）ファイルを開かせて「コンテンツの有効化」ボタンをクリックさせる（パスワード付きZipファイルが送付される場合もあります）



なりすましメールの送付

実在する企業や人物になりすましたメールが取引先に送付される

他のウイルスへの感染

～感染しないために、基本に立ち返りましょう～

- ●ＯＳ等の修正プログラムの適用
- ●メールの添付ファイルやＵＲＬに注意
- ●定期的なバックアップの実施

このプロジェクトは、神奈川県警察が事務局を務め、神奈川県内の企業、団体、学術機関、行政機関が緊密に連携し、県内企業のサイバー空間の脅威への対処能力向上を図ることを目的に活動しています。

産 学 官
神奈川県企業サイバーセキュリティ対策官民合同プロジェクト

あなたの会社を守る情報発信基地

CyberSecurityStation

サイバーセキュリティステーション

二次元コード紹介

脅威

情報処理推進機構（ＩＰＡ）
ランサムウェア対策特設ページ
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.htm

情報処理推進機構（ＩＰＡ）
「Emotet（エモテット）」
と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html

このチラシの二次元コードからは、それぞれの情報へ直接アクセスできます。

対策

神奈川県警察ホームページ
『テレワークのサイバーセキュリティ対策』
https://www.police.pref.kanagawa.jp/mes/mesd7041.htm

神奈川県警察ホームページ
『メールに注意して、リスクの低減を図る』
https://www.police.pref.kanagawa.jp/mes/mesd7040.htm

神奈川県警察ホームページ
『事業者の皆さんへ「セパレートしてますか？」』
https://www.police.pref.kanagawa.jp/mes/mesd7033.htm

このプロジェクトは、神奈川県警察が事務局を務め、神奈川県内の企業、団体、学術機関、行政機関が緊密に連携し、県内企業のサイバー空間の脅威への対処能力向上を図ることを目的に活動しています。

産 学 官

神奈川県企業サイバーセキュリティ対策官民合同プロジェクト