令和3年12月1日

サイバーセキュリティ関連情報（12月号）

鳥取県警察本部サイバー犯罪対策課

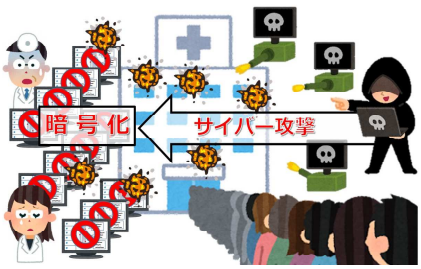
○ 医療機関のシステムがランサムウェアに感染！

令和3年10月末、徳島県つるぎ町の町立病院のシステムがランサムウェアに感染し、約8万5,000人分の電子カルテが閲覧できなくなるなどの深刻な事態となっています。診療費の会計ができず、診察内容は手書きで記載するなどの対応に追われ、外来患者の新規受け入れを停止しているとのことであり、現時点で復旧の見通しは立っていない状況です。

異変に気付いたのは、同月31日未明、院内のプリンターが一斉に印刷をし始め、用紙には、「データを盗んで暗号化した。データは公開される。復元してほしければ連絡しろ」との脅迫文が英語で記されていました。確認した結果、メインシステムのサーバのみならず､バックアップ用のサーバ内のデータもすべて暗号化されていたとのことで、災害レベルの大打撃で被害は甚大な状況です。

脅迫文には、世界中で攻撃を繰り返すハッカー集団「ロックビット」の記載があり、攻撃者は石油パイプラインなどのインフラ企業と同様、診療記録などの重要データを取扱う医療機関も標的対象とみている可能性があります。

警察庁、JC3（日本サイバー犯罪対策センター）、NISC（内閣サイバーセキュリティセンター）では、公式ウェブサイトにおきまして、ランサムウェアの特設サイトをそれぞれ開設しています。被害の未然防止対策、感染に備えた被害軽減対策等のために、ご活用下さい。



参考　警察庁　https://www.npa.go.jp/cyber/ransom/index.html
JC3　https://www.jc3.or.jp/threats/topics/article-375.html
NISC　https://security-portal.nisc.go.jp/stopransomware/

○ 「Emotet（エモテット）」攻撃活動再開！

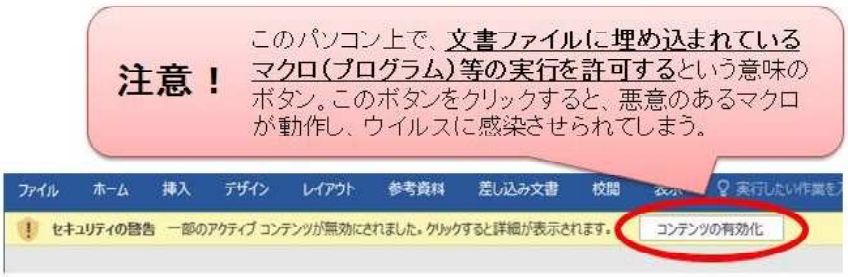
IPA（独立行政法人情報処理推進機構）は、マルウェア「Emotet（エモテット）」の攻撃活動再開の兆候が確認されたとして、注意を呼び掛けています。

Emotet（エモテット）は、令和元年12月ころから日本国内で流行するコンピュータウイルスで、過去にやり取りした実在する相手の氏名、メールアドレス、メール内容等が攻撃メールに流用され、あたかもその相手からの返信であるかのように見せかける巧妙な手口によって、ウイルスが添付されたファイルを開かせようとするものです。

令和3年1月27日、EUROPOL（欧州刑事警察機構）が、Emotetの攻撃基盤を停止させたと発表し、日本国内における被害等も大幅に減少したことを確認していました。

しかし、令和3年11月14日ころから、攻撃活動再開の兆候を確認し、複数の攻撃メールを観測している状況であるとのことです。

攻撃メールには、これまでの手口と同様、悪意のあるマクロが仕込まれたWord文書ファイルやExcelファイルが添付されており、クリックすることでEmotetに感染してしまいます。過去、メールの件名や添付ファイル名が、「クリスマス」、「賞与支給」等のキーワードが使われ、特に年末時期に合わせて、多くの企業・組織が被害に遭っていることから、再び、警戒をお願いします。



※　信用できる文書と判断できる場合でなければ、「コンテンツの有効化」「編集を有効にする」というボタンはクリックしないで下さい。

引用　IPA　https://www.ipa.go.jp/security/announce/20191202.html