ウイルス注意・最新情報

JJ1SXA/池

1、知人からのメールで感染する「エモテット」

知人から届いたメールの添付ファイルを開いてウイルス感染…半ば信じられない状況で被害に遭うウイルス「エモテット」が2019年末に猛威を振るった、既に3200以上の組織が被害を受けたといわれており今なお衰えを知らないようだ。

2014年に発見された「エモテット」は全く新しい手口ではないが、最近になって急に活発化、手口も巧妙化している。

ビジネスメールに添付されたワード文書に仕込まれたマクロを実行すると、感染して「ランサムウエア」などの別のウイルス被害に遭う。

最も確実な対策は、ワード文書を開いたとき安易にマクロを実行しないことだ、感染のトリガーとなるのが添付されたワードに仕込まれたマクロ、文書を開いて、「コンテンツ」の有効化ボタンを押すとエモテットがインストールされる、こうなると、パソコンをコントロールされて情報が不正サーバーに送られてしまう。

マクロ入りの文書が送られてきたら開く前に差出人に確認したほうが良い、開いた直後は、「保護ビュー」となり、「編集を有効にする」を押さないと、「コンテンツの有効化」が表示されないが、注意するに越したことはない。

2、絶対安心の「2段階認証を突破する詐欺」の脅威

「ネットのアカウントは2段階認証を設定しておけば安全」というセキュリティの「常識」を揺るがす事案が2019年に発生した。

攻撃者によってネットバンキングの2段階認証を突破したとみられる不正送金が数多く確認されたからだ、警察庁によると「11月の発生件数は573件、被害金額は7億7,600万円といずれも過去最多だったという、銀行側も利用者に注意を呼びかけているが、今後も被害が増える可能性は極めて高い。

不正送金が増えた最大の要因は、ネットバンキングのIDとパスワードと一緒にワンタイムパスワード（認識コード）を盗むフィッシングの手口が登場したことだ。…

この手の詐欺から身を守るには、SMSやメールなどのリンクから偽のサイトを開かないことに尽きる、ネットバンキングを利用するときは必ず登録しておいたブックマークから開く、スマホでは、各銀行などが用意する専用アプリを使うと良いようだ。

3、「正規ドメインのフィッシングサイト」が出現

正規サイトのURL（ドメイン）が使われているにもかかわらず詐欺サイトであった事例が2019年に見つかった。

開いたサイトがマイクロソフトのクラウドサービス「ワンドライブ」や「オフィス」と同じドメインだっとしても油断は禁物だ。

攻撃者が目を付けたのは、ワンドライブのアンケート機能、これはワンドライブのサイト内にアンケートページを作るというもので、誰が作っても「onedrive」から始まるドメインが割り当てられる、この機能を悪用し、ワンドライブの正規サイトを装ったフィッシングサイトを作ったのだ。

現在はワンドライブ上でのアンケート機能が廃止されているが、同じようにウエブ上でアンケートを作れる「マイクロソフトフォームズ」「グーグルフォーム」は、今（2020年2月）でも使えるので注意が必要、両サイトともに正規のドメイン上に詐欺サイトを作成でき悪用される可能性がある。

良く知られたドメインであっても安易にパスワードを入力しないのが鉄則だ、なお、マイクロソフトとグーグルのアンケート機能ではパスワードの入力欄の作成は禁止しているようだ。

マイクロソフトフォームズはパスワードの収集を禁止しており、作成したすべてのアンケートページに「パスワードを記載しないでください」と注意書きが表示される、それでもパスワードの入力を求められるなら詐欺と疑ったほうが良い、また、アンケートの作成者が誰なのかを確認したほうが良い。

4、iphone使用者は「エアドロップ痴漢」に注意

電車内などでiphoneにわいせつな画像を送り付ける「エアドロップ痴漢」と呼ばれる嫌がらせが話題となっているようだ、標的になると画像が強制的にプレビュー表示され、いやでも目にしてしまう。

「エアドロップ」は、写真などを近距離で受け渡しできるiOSの通信機能、これを悪用して周囲のiphoneユーザーに画像を送り付けているのだ。

送信範囲は約10mあり、混雑した電車内などでは犯人の特定が困難、対策としては、エアドロップを使っていない時は機能をオフにしておくことだ。

詐欺の手口が、本当に巧妙だ、それにしても、悪い奴らは、あの手この手で詐欺を働く、その頭脳を別の場所に活用してもらいたい。

私なんかには、どうしてそんなことができるの？と驚嘆するばかり、情けないなあと思うが、ある部分仕方が無いかと諦めの心境もある。

まあ、できる限りの対策は実施して、被害を最小限に食い止めましょう。