令和４年１２月９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

○　マルウェアEmotetの活動再開について

マルウェアEmotetは、令和４年７月中旬頃から活動を停止していましたが、今般、警察庁では、Emotetメールを複数確認するなど、国内において活動が再開したとみられる事象を確認しております。

Emotetは、主にメールを感染経路としたマルウェア（不正プログラム）です。

メールソフトに登録されている連絡先から知り合いのメールアドレスを盗んで使うなどして、本人作成のメールであると信じ込ませ、不審に思わず開封してしまいそうなメールの返信を装うなど巧妙化が進んでいます。

感染すると、情報を盗まれる、ランサムウェア等の他のマルウェアにも感染するといった被害に遭うおそれがあります。

今回の手口では、添付ファイルを指定されたフォルダにコピーするよう指示を行い、マクロを実行可能とさせEmotetに感染させるといった特徴があります。

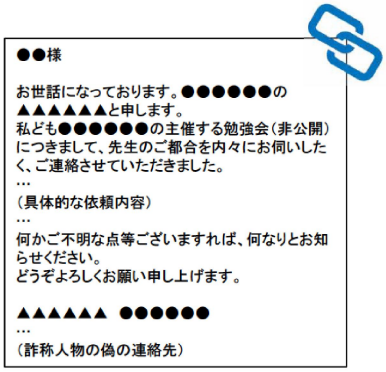
なお、これまで、添付ファイルのマクロを有効化した場合に、Emotetに感染させる手口や、ショートカットファイル（LNKファイル）を添付し、これをダブルクリックなどで開いた場合にEmotetに感染させる手口が確認されています。

不用意にメールの添付ファイルを開かないないようにするなど、マルウェアに感染しないように注意してください。

引用：警察庁　https://www.npa.go.jp/cybersecurity/pdf/20221104press.pdf

○ 学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について

近年、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム（マルウェア）を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されています。



また、以前より、WEBメールサービスへの不正ログインの発生を警告する内容のメールを模したメールを送付し、当該WEBメールサービスの正規サイトを装ったフィッシングサイトに誘導してID及びパスワードを窃取することで、保存されているメールを盗み見たり、受信するメールを他のメールアドレスに自動転送する設定を施したりするサイバー攻撃の手法も確認されています。

標的型攻撃メールは、様々な企業や地方公共団体等が対象となります。

少しでも怪しいと感じた場合は、

・当該メールの返信以外の方法で送信者に内容の確認を行う。
・ウイルス対策ソフトのフルスキャンを行う。
・WEBメールサービスのアクセス履歴を確認し、身に覚えのないログインがあれば、パスワードを変更する。
・WEBメールの転送設定がなされていないか確認する。

などの措置を実施するようお願いいたします。

また、被害に遭わないためにも、日頃から、

・ウイルス対策ソフトの定義ファイルを更新し、定期的にフルスキャンを行う。
・WEBメールサービス等のログインアラートを設定する。
・WEBメールサービス等のログインに二要素認証を設定する。
・パスワードは、長く複雑なものを設定し、他のサービスと使い回しをしない。

などのリスク低減のための対策をお願いいたします。

引用：警察庁　https://www.npa.go.jp/cyber/pdf/R041130_cyder_alert_1.pdf