サイバーニュース

2022年11月
第 15 号

Emotetの活動再開について

今年に入ってから活発に活動していた「Emotet」というマルウェアですが、７月中旬から突然観測されなくなっていました。しかし、11月２日から、**再び「Emotet」の感染に至るメールの配布が観測**され始めました。

今回、**少し変わった手口**のものが確認されているので、その点も解説します！

Emotetの特徴

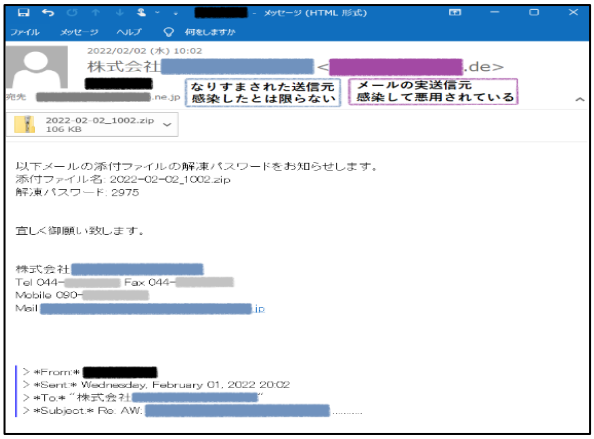
Emotetは、情報の窃取に加えて、他のマルウェアへの感染に悪用されるマルウェアで、攻撃メールにより感染が拡大します。従来のEmotetは、メール添付されているExcelファイル等やパスワード付きのzipファイル内の、Excelファイル等を開いて、**マクロを有効にする**ことで感染していました。

しかし、今回の手口では、**添付ファイルを指定のフォルダにコピーするよう指示**されます。

指示されるフォルダは、Excel等に元々指定されている「信頼できるフォルダ」であり、**全てのマクロが自動的に有効になるフォルダ**です。そのフォルダに保存されたExcelファイル等を開くと、自動でマクロが有効化され感染します。

Emotetの攻撃メールは、過去にやり取りをしたことがある実在の相手の氏名や会社名、メールアドレス、メールの内容等の一部が流用され、**正規のメールを装う**場合や、採用情報などの業務上添付ファイルを開く必要があるような**巧妙な文面になっている**場合があります。（右図・Emotetメールサンプル）

出典：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



出典：JPCERT/CC　マルウェアEmotetの感染拡大に関する注意喚起
https://www.jpcert.jp/at/2022/at220006.html

Emotet対策

☆　ＯＳやウイルス対策ソフトなどを**常に最新の状態**にしておきましょう

☆　ExcelやWordなどのマクロの自動実行機能を備えたソフトウェアは、**自動実行機能を無効化**しましょう

☆　保存フォルダを指定された場合など、少しでも不審に感じた場合は、メールの相手方に**電話などのメール以外の方法で確認**しましょう

☆　メールセキュリティ製品や不正通信ブロックサービスの導入を検討しましょう

☆　**組織内への注意喚起**を実施しましょう

被害にあった場合はすぐに警察に通報を！

Twitter
@IP_cybertaisaku

石川県警察本部生活安全部サイバー犯罪対策課
076－225－0110　cyber@police.pref.ishikawa.lg.jp

Instagram
IP_cybertaisaku