サイバーセキュリティ通信 Vol.1

令和４年４月

サイバァちゃん

ショートカット、どちらが本物？！

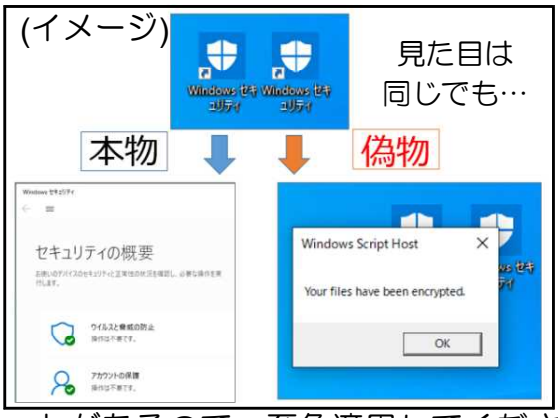
本年２月以降、マルウェアEmotetの感染が再拡大しています。

従来のＯｆｆｉｃｅファイルのマクロを使った手口だけでなく、ショートカットを利用した新しい手口も確認されています。引き続き、知人から送信されたと思われるメールであっても、添付されたファイルを不用意に開かないようにしてください。

１　Emotet（エモテット）とは？

- 感染したパソコンからメールアドレスやログイン情報などを盗み出すマルウェアです。
- メールの添付ファイルから感染させる手法が主流です。
- 感染した端末がマルウェアの配布に利用されることで、感染が広がっています。

２　Emotet感染の新しい手口



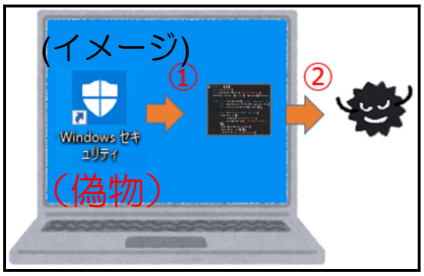
①　添付ファイル付きのメールを受信。

②　ショートカット（ＬＮＫ）又はパスワード付きＺＩＰファイル（ＺＩＰファイル中身は、ショートカット）が添付されている。

③　（ＺＩＰファイルを展開して）ショートカットを開くと、Ｅｍｏｔｅｔに感染する。

・　ショートカットのアイコンはＯｆｆｉｃｅファイルのものが確認されていますが、今後、新しいアイコンが利用される可能性があります。（例：「【重要】ウイルス対策ソフトのアップデートがあるので、至急適用してください」といったメール本文が記載され、ウイルス対策ソフトの見た目をした有害なショートカットが添付される。）

３　新しい手口の仕組み



①　ショートカットを開くと、マルウェアをダウンロードするためのプログラムが作成・実行されます。

②　実行されたプログラムがＥｍｏｔｅｔなどのマルウェアをダウンロードして感染します。

４　Ｅｍｏｔｅｔの対策や感染確認について

従来のＥｍｏｔｅｔと同様に、不用意に添付ファイルを開かない対策や送信者に電話などメール以外の手段で確認する対策が有効です。

Ｅｍｏｔｅｔに感染していても、パソコンに特に変化がない場合もあります。Ｅｍｏｔｅｔに関する詳しい情報や感染確認ツール（Ｅｍｏｃｈｅｃｋ）、感染時の対応についてＪＰＣＥＲＴ／ＣＣから公開されていますので、こちらも併せてご確認ください。

◎　マルウェアＥｍｏｔｅｔの感染再拡大に関する注意喚起（ＪＰＣＥＲＴ／ＣＣ）
https://www.jpcert.or.jp/at/2022/at220006.html

長崎県警察本部サイバー犯罪対策課
095-820-0110（3451・3452）
ﾒｰﾙｱﾄﾞﾚｽ e103107@police.pref.nagasaki.jp

サイバー犯罪対策課
公式LINEアカウントで
情報配信中！

@387ojopi