

令和4年5月1日

サイバーセキュリティ関連情報（5月号）

鳥取県警察本部サイバー犯罪対策課

○ ウクライナ情勢を悪用した詐欺の手口に注意！！

独立行政法人国民生活センターは、ウクライナ情勢を悪用した詐欺の相談事例を公開し、注意を呼びかけています。

この度公開された相談は、今年3月、30歳代の男性から寄せられたもので、その男性によると、『ウクライナでロシアの軍事侵攻が激しさを増してきたため、何か自分にもできないかと思っていたところ、SNSで義援金を募集していたので、クレジットカード決済で1,000円を募金した。ところが数日後、SNSに、募金した義援金サイトは偽物の可能性がある则表示された。』とのことでした。

今後も、ウクライナ情勢に関連した様々な手口の詐欺の発生が予想されます。

インターネットで義援金を振り込む場合は、真正な団体かどうか、新聞やテレビ等で公表されている口座番号や名義情報と一致しているか確認するとともに、不審なSNSやメールは開かないよう基本的な対策を心掛けましょう。



引用：【国民生活センター】 https://www.kokusen.go.jp/news/data/n-20220325_1.html

○ 「Emotet」の新たな手口を確認！！

独立行政法人情報処理推進機構（IPA）や一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は、マルウェア「Emotet」に関して、「ショートカットファイル（.lnkファイル）」を悪用する新たな攻撃手法を確認しているとして注意を呼びかけています。

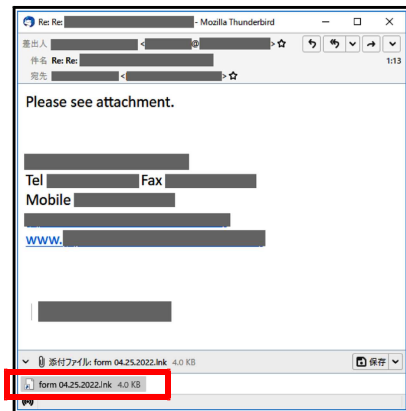
確認された手口には、

- ・ショートカットファイルがメールに直接添付されている場合（図1）
- ・ショートカットファイルがパスワード付きZIPファイルとして添付されている場合（図2）

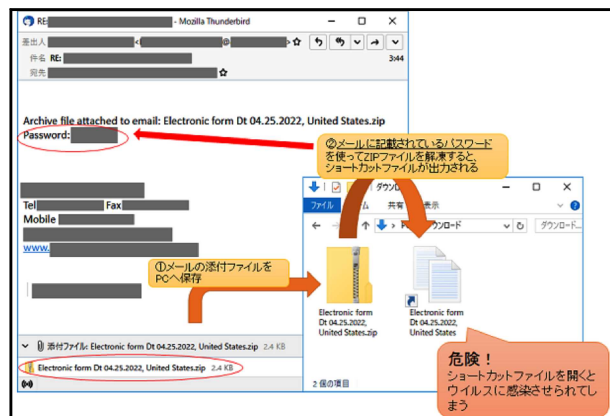
があり、ショートカットファイルをダブルクリックなどで開くとEmotetに感染します。

これらは、これまで確認されていた「Emotet」のように、WordやExcelのマクロやコンテンツの有効化を必要としないため、誤ってファイルを開いただけで感染するおそれがあります。

また、ショートカットファイルは、アイコンが文書ファイルのように偽装されていることや、Windowsの標準設定では拡張子が表示されないといった特徴から、見分けが付きにくい点に注意が必要です。



【図1】ショートカットファイルを悪用する攻撃メールの例



【図2】ショートカットファイルが格納されたパスワード付きZIPファイルからEmotet感染までの流れ

不審なメールだけでなく、自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない、メール本文中のURLリンクはクリックしないなど警戒をお願いします。

引用：【情報処理推進機構（IPA）】

<https://www.ipa.go.jp/security/announce/20191202.html>

【JPCERTコーディネーションセンター】

<https://www.jpccert.or.jp/at/2022/at220006.html>