



令和4年4月28日
警察庁

マルウェアEmotetの新たな手口に係る注意喚起について

警察庁では、国内においてEmotetの攻撃によるものとみられる被害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。

これまでは、添付ファイルのマクロを有効化した場合にEmotetに感染させる手口等が確認されてきました。これに加えて本年4月下旬以降、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新たに確認されています。

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。

【関連サイト】

- 春の大型連休に向けて実施いただきたい対策について（注意喚起）

<https://www.npa.go.jp/cybersecurity/pdf/20220425press.pdf>

- 警察庁（@police）Emotetの解析結果について

<https://www.npa.go.jp/cyberpolice/important/2020/202012111.html>

- マルウェアEmotetに係る注意喚起について

https://www.npa.go.jp/cyber/pdf/R040204_emotet.pdf