IT時事ネタキーワード「これが気になる！」（第112回）

エモテット3か月ぶりに活動開始、その新たな手口

2022.12.14

Emotet（エモテット）と呼ばれるウイルスへの感染を狙う攻撃メールについて、本連載でも継続的に注意を呼び掛けてきた（「エモテット、ここへきて大流行。対策してみた」他）。このエモテット、今年7月13日頃より攻撃メールの配信が観測されない状態が続いていたが、11月2日から再開という情報がIPAからリリース、JPCERT/CCも同様の情報を11月4日にリリース、復活したエモテットの新たなる手口を紹介している。

トレンドマイクロも「攻撃手法から考える防御策 2022年11月に活動再開したEMOTET（エモテット）を既存環境で防ぐ考え方」という記事を出し、復活したエモテットに対して注意喚起と対応を呼び掛けている。

Excelファイルの偽の指示に注意。特定のフォルダにコピーして開かせる

エモテットの新たなる手口については、IPAの「Excelファイル内に書かれている偽の指示の変更について（2022年11月4日追記）」が参考になる。

ここには、「2022年11月2日から、メールに添付されたExcelファイル内に書かれた偽の指示が、コンテンツの有効化を促す内容から、記載されたフォルダにファイルをコピーして開くよう、変化しました」と書かれている。この変化は主に、マイクロソフトが、最新Officeでのマクロ機能無効の標準化を発表したことで、攻撃の有効性が落ちることを予期して攻撃者側が講じた新たな対策と推測される。

指示は、具体的には、添付されたExcelファイルを指定の「Templates」フォルダにコピーして開く、という内容。指示に従うと、マクロを無効にする設定がされていても、ファイルを開く際にマクロが実行されてしまう。なぜなら、コピー先の「Templates」フォルダは、Windowsのデフォルトで“信頼できる場所”として設定されているからだ。

マクロを無効化していてもマクロが強制的に実行。対処方法は？… 続きを読む