2023 年 3 月 8 日

Venture Solution

コラム記事

昨年、全世界で急速に被害が拡大した「Emotet」
メディアで報道されている間は、各社で対策や対応をされていましたが、報道が下火になることに比例して
Emotet に対する危機意識も低下してきているように感じております。
そんな中で Emotet が手口を変え、再拡散の兆しがあるとの記事が掲載されておりしましたので、ご紹介いたします。

Emotet 再拡散か　アンチウイルスソフトの回避狙う新手口も　JPCERT/CC が注意喚起

（ITmedia NEWS 2023/3/8(水) 18:53 配信　より引用）

（ITmedia NEWS より引用）

JPCERT/CC は 3 月 8 日、マルウェア「Emotet」の感染を広げるメールが再度見つかったとして注意喚起した。添付の ZIP ファイルを開くと、500MB を超える文書ファイル（doc）が展開されるなど手口の変化が見られるという。「サイズを大きくすることでアンチウイルス製品などでの検知回避を図っていると考えられる」（JPCERT/CC）

Emotet はメールを媒介に感染を広げるマルウェア。攻撃の手口は従来のままで、メールに添付されたマクロ付 Office ファイルや ZIP ファイルなどを開くと Emotet に感染する。2022 年 11 月を最後に観測されていなかったが、JPCERT/CC が 23 年 3 月 7 日に再確認した。

感染チェックツール「EmoCheck」で検知できない例もあったという。JPCERT/CC は「EmoCheck による検知手法の更新の可否も含めて調査を行い、ツールのアップデートなどの進捗があれば適宜情報を更新する」としている。

一度拡大が下火になっていたとしても、その間に手口を変え再度拡散させる。
これはサイバー犯罪の大きな特徴の 1 つであると考えております。手口が変わるたびに対策を考える「いたちごっこ」では終わりはなく、セキュリティ対策が後手に回ってしまいます。
まずは個人でできる対策（添付ファイルを開かない、各ツールを最新バージョンへ更新する等）を行い、企業としてもセキュリティ対策を見直すなど、先手を取れるような対応が必要であると感じております。