サイバーセキュリティ通信 Vol.18

令和４年３月

サイバァちゃん

【注意】 Emotetによる感染が急拡大！

JPCERT/CCによると、3月２日、Emotetに感染しメール送信に悪用される可能性のある、JPメールアドレス（●●@●●.jp）の新規観測数が過去最大（これまでの最高値の約５倍）になっています。

新しい感染手法が取られている訳ではありませんが、長崎県内においても、警察への相談が増加しているので十分に警戒をしてください。

１　Emotet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。
- Emotetに感染後、さらにランサムウェアに感染する事例もあります。
  ランサムウェアに感染した端末は、データが暗号化されてしまいます。

２　Emotetの感染経路と特徴

- 現在主流となっている感染経路は以下のとおりです。
  ①パスワード付ZIPファイルが添付されているメールを受信
  ②ZIPファイルを展開するとExcelファイルなどのOfficeファイルが保存されている
  ③Officeファイルを開き、「マクロを有効化する」とEmotetに感染する
- 日本語による本文、返信メールを装った件名、文字化けした引用文などの特徴があります。

※類似の手口、特徴のものが複数あります。

３　Emotetによる悪影響は？

- Emotetに感染することで、自組織のなりすましメールが配信される
- さらに、自組織の端末に記録しているメーリングリストをもとに、関係者なりすましたメールが配信される

※自組織の端末が感染していなくても、他社からメール情報等が流出していることもありまえます。

【 注　意　事　項 】

- 関係者からのメールであっても、不用意にファイルを開き、マクロを有効化しないで下さい。
- 従業員に対し、添付ファイル付きのメールには特に注意するよう、繰り返し注意喚起をお願いします。
- 感染が判明した際は、端末をネットワークから切り離して下さい。
- 自組織がなりすまされてしまった場合に対する備えも必要です。関係者への注意喚起のほか、プレスへのお知らせについても日頃から検討しておく必要があります。

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！
友だち登録お願いします！

@387ojopi