TLP:WHITE【全分野】

別紙

2022 年 4 月 27 日

内閣サイバーセキュリティセンター
重要インフラグループ

Emotet の新たな感染手口に関する注意喚起

マルウエア Emotet について、2021 年 11 月中旬から活動再開がみられたことから、注意喚起を行いました（別添 1 及び別添 2 参照）。

2021 年 11 月の活動再開以降、多数の国内組織で感染被害が報告されており、ショートカットファイルを使った、新たな感染手口が確認されたことから、注意喚起します。

これまで、マクロ付きの Office ファイル(Word や Excel 等)を使った攻撃手法が多数確認されており、マクロの無効化や Office ファイルの実行制限等の対策が考えられていました。

これらに加え、2022 年 4 月 25 日頃からショートカットファイル（lnk ファイル）単体又はショートカットファイルを含むパスワード付 ZIP ファイルが添付されたメールを着信するケースが観測されています。このショートカットファイルを実行した場合、Emotet に感染する恐れがあるため、マクロ付き Office ファイルに加え、ショートカットファイルに対しても注意してください。

Emotet の感染により、ランサムウエアを始めとした他のマルウエアの被害につながる可能性があります。今後も攻撃手法が変化する可能性があるため、定期的に Emotet の動向や対策の有効性等、被害拡大防止に万全を期してください。

参考 URL
- マルウェア Emotet の感染再拡大に関する注意喚起(JPCERT/CC)
  https://www.jpcert.or.jp/at/2022/at220006.html

TLP:WHITE【全分野】

別添 1

2021 年 11 月 19 日

内閣サイバーセキュリティセンター
重要インフラグループ

Emotet の活動再開に関する注意喚起

過去の注意喚起の中で触れてきておりますが、2019 年頃から国内で感染拡大したマルウエア Emotet について、2021 年 1 月末以降活動がみられていませんでしたが、11 月中旬から活動再開し、国内でも不審メールの受信が確認されたことから、注意喚起します。

Emotet の感染により、ランサムウエアをはじめとしたマルウエアの被害に繋がる可能性があります。また、新たに Emotet に感染していない場合も、過去に窃取されたメールを悪用されるケースが発生しています。今後、攻撃手法が変化する可能性があるため、定期的に Emotet の動向や対策を確認してください。

参考 URL
- Emotet botnet returns after law enforcement mass-uninstall operation (Recorded Future)
  https://therecord.media/emotet-botnet-returns-after-law-enforcement-mass-uninstall-operation/
- 【注意喚起】マルウェア Emotet が 10 カ月ぶりに活動再開、日本も攻撃対象に（LAC）
  https://www.lac.co.jp/lacwatch/alert/20211119_002801.html
- 更新:「Emotet(エモテット)」と呼ばれるウイルスへの感染を狙うメールについて（IPA）
  https://www.ipa.go.jp/security/announce/20191202.html
- ランサムウエアによるサイバー攻撃に関する注意喚起について（NISC）
  https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf

TLP:WHITE【全分野】

別添 2

2022 年 2 月 4 日

内閣サイバーセキュリティセンター
重要インフラグループ

Emotet の活動急増に関する注意喚起

マルウエア Emotet について、2021 年 11 月中旬から活動再開がみられたことから、2021 年 11 月 19 日に注意喚起を行いました（別添参照）。

2022 年 1 月末以降、我が国において、Emotet に感染させるメールが急増し、被害を受けた組織で公表する事例が多数みられています。

参考 URL などを参照し、定期的に Emotet の動向や対策の有効性を確認する等、被害拡大防止に万全を期してください。

参考 URL
- 更新:「Emotet(エモテット)」と呼ばれるウイルスへの感染を狙うメールについて(IPA)
  https://www.ipa.go.jp/security/announce/20191202.html
- マルウエア Emotet への対応 FAQ （JPCERT/CC)
  https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html