回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security Newsletter Vol.90

あさまセキュリティニュースレター

Emotet（エモテット）再び　（2022年11月11日）

9月、10月数件検知していたEmotetと思われるウイルスが、11月はすでに数十件検知。増加傾向です。
一度、Emotetのメールが来たことあるアドレス宛が目立っておりますが、社内全体でご注意ください！

11月にEmotetと思われる不審なExcelファイルを検知ブロックした履歴からみると、
ファイル名は**年月日、〇〇report、数字の羅列**など、従来同様のファイル名が見受けられます（セキュリティ機器のアラートより）

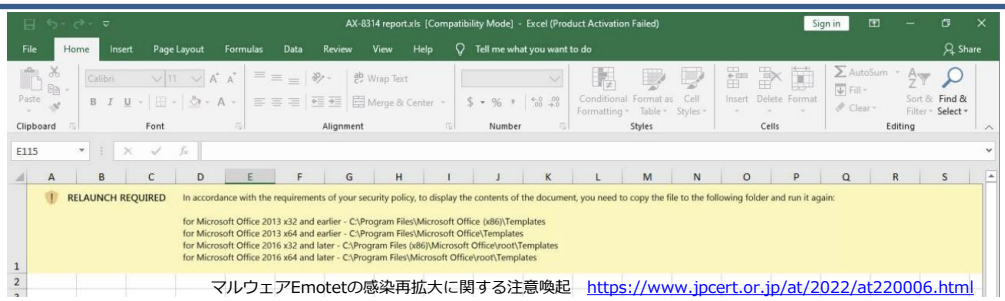
[redacted] filename: report 11 03 2022.xls
virus: XLM.Trojan.Abracadabra.8.Gen

[redacted]@[redacted]
filename: 2022-11-04_1036.xls virus:
XLM.Trojan.Abracadabra.8.Gen

user[redacted]@[redacted].jp
filename: attachments_311490.xls virus:
XLM.Trojan.Abracadabra.8.Gen

11月のEmotet感染させるxlsファイルの特徴

JPCERTの情報によるとxlsファイルを特定のフォルダにコピーして実行するよう促すものが観測されています。Officeの設定で「信頼できる場所」に登録されているようなフォルダパスにxlsファイルをコピーさせた後に実行させることで、警告を表示させずに悪性なマクロを実行することを試みていると考えられます。



マルウェアEmotetの感染再拡大に関する注意喚起　https://www.jpcert.or.jp/at/2022/at220006.html
[図3-1：特定の場所にコピーして実行することを求めるxlsファイル（2022年11月4日追記）]

Emotetメールが届くケース

Emotetの感染によってメールが送信されるケースは、感染者とその関係者を巻き込む形で複数のパターンに分かれます。

1）自組織がEmotetに感染し、なりすましメールが配信されるケース
2）取引先がEmotetに感染し、なりすましメールが配信されるケース

また、自組織で管理するメールサーバーなどが悪用されているケース
（直接メールサーバに不正アクセスされ、情報搾取、大量メール発信など悪用されるケース）
Emotetは様々なパターンで配信されますので、メールが届いた場合の報告、確認、対策をまとめておきましょう

今回も実在する企業名、取引先名をファイル名に入れているケースを確認してます。
filename: Fuji[redacted]_2022-03-11_0819.xls virus:

被害

- **メールソフトやウェブブラウザーに記録したパスワードなどが窃取**される
- **過去にやり取りしたメールの本文、メールアドレスなどが窃取**される
- **窃取されたメール関連の情報が悪用され、感染拡大を目的としたメールが送信**される
- **ネットワーク内のほかのPCに感染が拡大**する
- **ほかのマルウェアに感染（ランサムウェア、インターネットバンキングの情報の窃取を目的としたものなど）**

対策

- **不審なメールだけではなく、自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。メール本文中のURLリンクはクリックしない　相手に確認する**
- **メールに添付されたファイルを開き、マクロやセキュリティに関する警告が表示された場合、安易に開かない**
- **ソフトウェアアップデート、ウイルス対策ソフトの導入、インターネット出入り口のセキュリティ対策の確認・更新**

情報源
JPCERT　https://www.jpcert.or.jp/at/2022/at220006.html　**IPA**　https://www.ipa.go.jp/security/announce/20191202.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414