回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security Newsletter Vol.85

あさまセキュリティニュースレター

Emotet（エモテット）に新機能　クレジットカード情報を窃取　（2022年6月14日）

Emotetの解析結果について

2022年6月9日
警察庁

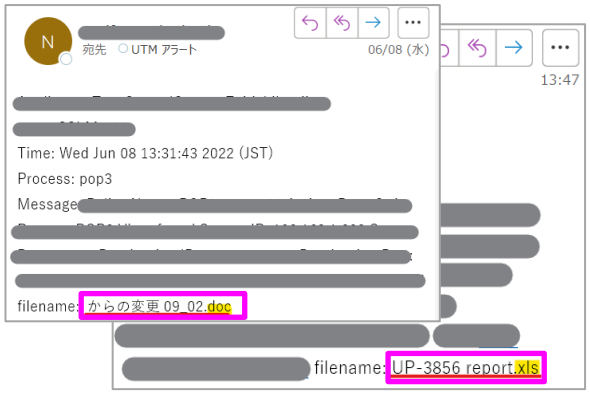
新機能の確認（2022年6月9日）

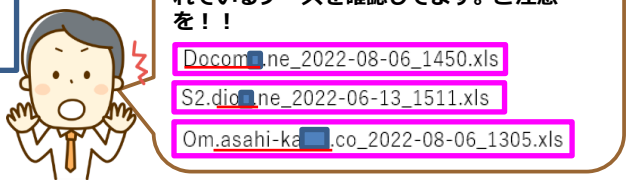
ウェブブラウザ「Google Chrome」に保存されたクレジットカード番号や名義人氏名、カード有効期限を盗み、外部に送信する機能が追加されたことを確認しました。Google Chromeでは個人情報を暗号化して安全に保存していますが、Emotetの新機能は暗号データを元に戻すための鍵も同時に盗み出すため、Emotetに感染すると、お使いのクレジットカード情報が第三者に知られるおそれがあります。

出典:Emotetの解析結果について | 警察庁 @police (npa.go.jp)
https://www.npa.go.jp/cyberpolice/important/2020/202012111.html

警察庁のEmotetの解析結果によると、
ブラウザに保存されたクレジットカード情報（カード番号や名義人氏名、カードの有効期限）を盗み、外部に送信する機能が追加されたことを確認

6月のEmotetと思われる検知履歴
相変わらずXX-数字4桁report.xlsのファイルを多く検知
Word（.doc）形式、も検知し始めました





Emotetメールが届くケース

こちらを参考　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

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

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　**警察庁**　https://www.npa.go.jp/cyberpolice/important/2020/202012111.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