サイバーセキュリティ通信 Vol.4

令和４年6月

サイバァちゃん

Emotet（エモテット）に クレジットカード情報を盗み取る機能が追加

国内外で感染が拡大しているEmotet（エモテット）に

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」「名義人氏名」「カード有効期限」を盗み、外部に送信する機能

が追加されたことが確認されました。

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、使用している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。

Emotetとは？

○ 主にメールの添付ファイルを感染経路とした不正プログラムです。
過去にやり取りしたメールへの返信を装ったメールを返信し、添付ファイルの開封を促します。

○ Emotetに感染したパソコンからメールアカウント、パスワード、メール本文等を盗み出し、それらの情報を悪用して、感染拡大を目的としたメールを送信します。

感染対策

従来のEmotetと同様に、不用意に添付ファイルを開かない対策や送信者に電話などメール以外の手段で確認する対策が有効です。

Emotetに感染していても、パソコンに特に変化がない場合もあります。

Emotetに関する詳しい情報や感染確認ツール（Emocheck）、感染時の対応についてJPCERT／CCから公開されていますので、こちらも併せてご確認ください。

◎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

今回の詳しい内容については、下記ウェブサイトを確認してください。
警視庁ウェブサイト「@police」　Emotetの解析結果について
（https://www.npa.go.jp/cyberpolice/important/2020/202012111.html）

長崎県警察本部生活安全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　@387ojopi
公式LINEアカウントで
情報配信中！