



バンキングマルウェア「Zloader」にご注意を！

「Zloader」と呼ばれるマルウェアの日本国内における感染が確認されています。このマルウェアに感染すると、インターネットバンキング利用中に、偽の入力フォームが表示され、アカウントやパスワードを窃取されたり、パソコンをリモート操作されるおそれがあります。このマルウェアは、先にお知らせしたマルウェア「Emotet」がダウンロードしたり、メールの添付ファイルのマクロ機能を有効化することで感染することが多いようです。

「Zloader」は、コンピュータウイルスだよ！
感染したパソコンに勝手にインターネットバンキングのログイン画面を表示させたいのさ！！
そこで入力したIDやパスワードは僕に筒抜けなんだよ！

犯人



「emotet」に感染したら「Zloader」も一緒に感染している可能性大！
添付ファイルにくっついていて、ファイルを開くと感染してしまう！

- ・ 知らないメールなどが来ても開封しない
- ・ 添付ファイルを開くときはよく確認してから！不用意に開かないで！
- ・ こまめにパソコンのアップデートをして最新の状態にする
- ・ ウイルス対策ソフトを導入する



こまめにアップデートせんばよ！



「Zloader」に感染しないためには、左図の対策のほか、

- 「Emotet」に感染しないように注意する
 - インターネットバンキングを利用時に、通常と異なるタイミングでIDやパスワードの入力を求められたら、入力せずに銀行に問い合わせる
 - オフィスソフトのマクロ機能を無効にするか、有効にする際に、確認のメッセージを表示するような設定にする
- などの対策が有効です。

長崎県警察本部サイバー犯罪対策課
095-820-0110 (3451・3452)
メールアドレス e103108@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！

LINE ID : @387ojopi

