インターネットバンキングを狙うマルウェアに注意!!

令和２年１０月３０日
奈良県警察本部
サイバー犯罪対策課

インターネットバンキングの情報を盗み出すマルウェア

Zloader

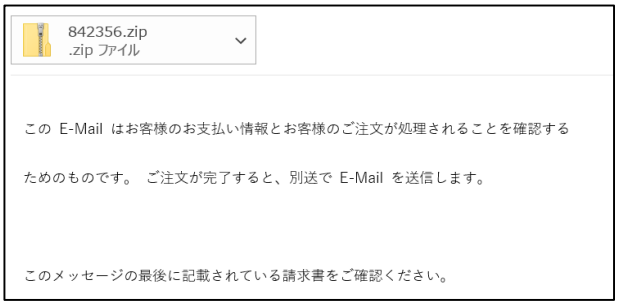
(別名：SILENTNIGHT，Terdot，DELoader，ZEUS Spinex)

の感染が日本国内でも確認されています。

「Zloader」に感染した端末からインターネットバンキングを利用すると、アカウント、パスワード、ワンタイムパスワードなどが窃取される可能性があります。

Zloaderの感染手口

日本国内における「Zloader」の感染手口は、
　〇メールの添付ファイルのマクロ等を有効にしたことによるもの
　〇Emotetに感染したことで、Zloaderにも感染したもの
が確認されています。



「Zloader」に感染させるメールの例

セキュリティ対策

〇 インターネットバンキングの利用者における対策
　ZloaderやEmotet等のマルウェアに感染しないようにする。
　・マルウェア感染に係る手口（返信型などのメールによる手口）等の周知
　・OSやブラウザ等、各種ソフトウェアを最新の状態に更新
　・ウイルス対策ソフトを導入し、最新の状態に更新

〇 インターネットバンキングの法人利用における対策
　・取引の申請者と承認者とで異なるパソコンを利用
　・金融機関が提供するセキュリティ対策や指定したソフトを導入、利用
　・取引明細の定期的な確認