CyberCrime Control Project

平成 25 年 10 月

広島県警察本部
サイバー犯罪対策課
082-228-0110

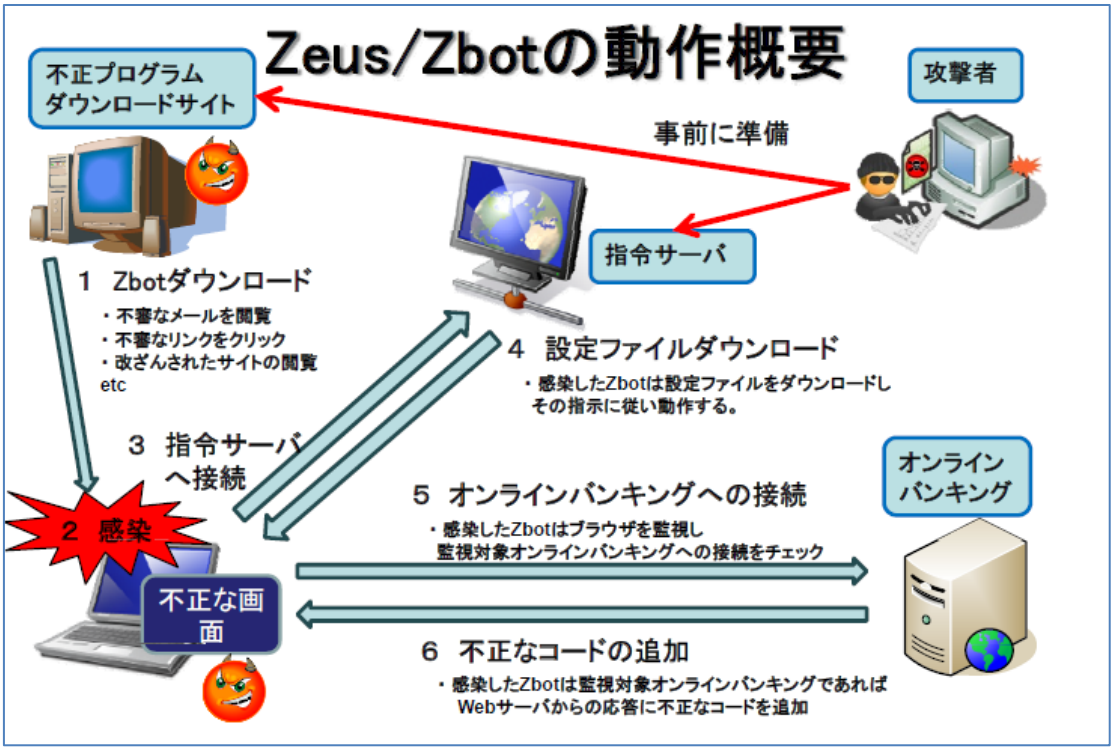
～インターネットバンキング不正送金事案への対策～

■　インターネットバンキングによる不正送金被害の実態

平成 23 年には約 3 億円，平成 24 年には約 4,800 万円の被害が発生したインターネットバンキング不正送金事案が，今年に入って急増し，9 月 20 日現在，全国で 615 件が認知され，被害金融機関は 18 金融機関，被害総額は約５億 5，000 万円（広島県内では 10 月 7 日現在で９件認知，被害総額約 500 万円）にも上っており，現在も被害は増え続けています。

また，狙われる金融機関が都市銀行等の大手金融から地方の金融機関に確実に拡大しつつあるとともに，ワンタイムパスワード認証も破られるなど，その手口も日々進化しており，被害拡大を防ぐために，金融機関と利用者それぞれに一層の対策が求められています。

■　インターネットバンキングによる不正送金の代表的な仕組



1　攻撃者が，対象とする金融機関ごとに構成したウイルス(ZeuS/Zbot/Citadel 等)を作成します。
　特化された内容になるため，ウイルス対策ソフトで検出することが困難です。

2　ウイルスを，スパムメールに添付・送信して感染，サイトに仕掛けて感染，フェイスブックやツイッターに掲載した URL から感染させるなど，あらゆる方法でパソコンに侵入させます。

3　感染したウイルスは，指令サーバと通信し活動の指令を受け取ります。

4　感染パソコンのシステムを解析し，独自の構成に自分自身を変化させて潜伏します。
　そのため，更にウイルス対策ソフトに検知される可能性が低くなります。

５　潜伏したウイルスは，通信を傍受し特定の金融機関との通信が始まったことを検知します。
６　金融機関と通信中のキーボード入力を盗み取ったり，送られて来たサイトの内容を改変し，本来は無いはずの入力画面を表示するなどして，利用者が入力した ID/パスワードを窃取し，攻撃者に送信します。
７　窃取した ID/パスワードを使って，攻撃者が，被害者の口座からの他人の口座へ送金します。

※ 攻撃する目標の金融機関の情報(URL)は，攻撃者がその情報リストをウイルスに書き込みますが，最近，警察において，このウイルスに感染した被害関係者のパソコンを解析した結果，リストに広島県内の金融機関が書き込まれていたとの情報があります。

■　被害防止の方策

被害を防止するには，金融機関，利用者それぞれの対策が必要です。

１　金融システムでの対策

一部の金融機関では被害を防ぐために大幅なシステムの改修を行っています。次の例を参考に，検討をお願いします。

- 利用者から送金要求があった場合に，要求があった通信回線**以外**の回線を使って，**送金前の確認メールとワンタイムパスワード**を送ることで，安全性を高める。例えば，パソコンからの要求だった場合は，**携帯電話にメール送信**するなどの方法が考えられます。
- **利用者が通常使っているパソコンや利用回線と異なった環境から送金要求**を行った場合や，ブラックリストに掲載されている口座や IP アドレスが関係していた時に，**当該要求が高リスクであることを総合的に判断**するシステムを導入する。(別紙「リスク検証システム」参照)
- 高リスク要求であった場合，利用者のみが知る通常使用していない「第二のパスワード」を入力させるなどして，再度，本人確認を行うシステムを導入する。
- 専用の**パスワード生成器**や乱数表による「ワンタイムパスワード認証システム」を導入する。
- 家族の写真など利用者が選んだ画像を，パスワードを入力させる画面に常時表示させることで，ウイルスが作ったポップアップ画面であることを利用者に気づかせるシステムを導入する。
- キーボードを画面上に表示し，毎回入力位置を変更することで入力パスワードを盗み取れなくする技術を導入する。
- 暗号化通信技術の導入，アクセス先が正規の金融機関サイトであることを証明する技術を導入する。(別紙「暗号通信・サイト認証」参照)
- フィッシング・サイトを発見した際に，速やかに閲覧防止措置をとれる連絡体制を確立する。
- 被害発生時に，直ちに口座凍結や送金停止措置をとれる体制を確立する。
- 個別の対応だけでは，すべてのウイルスに対応することはできません。**総合的な対策を講じて初めて抑止効果が期待できます。**

２　ネットバンキング利用者に対する広報・啓発

次の対策をとるよう，具体的な注意喚起をお願いします。

- ログイン時やパスワード等入力時に，通常と違う画面が出た場合には，操作を中止し，金融機関に確認の連絡を取る
- **ワンタイムパスワード認証システム**などの，より安全なシステムに移行する
- 取引先が限定できる場合は，相手口座を限定する設定を行う

・　１回の利用金額上限値を設定する
・　**OS やアプリケーションを最新**状態に保つ
・　インターネットブラウザのセキュリティレベルを高めに設定する
・　**ウイルス対策ソフトを最新**に保つ
・　パソコン内部のウイルスが勝手に外部と通信できない設定にする
・　不用意に**不審なサイトにアクセス**したり，発元不明のメールを開かない
・　ID/パスワードの管理を徹底する
・　ウイルス対策ソフトの導入を行う
　意外に多くの人が非導入/有効期限切れの状態なので，無料のウイルス対策ソフトが提供されていることを紹介する(Microsoft Security Essentials 等，個人利用の場合は無料なものもあります)。

３　不正送金先口座に対する対策

不正送金先に利用された口座の約 69%が「中国人名義の口座」です。

広島県内でも検挙者が出ており，多くの外国人研修生や留学生が，安易な気持ちで犯行に加担していることがうかがえます。

このことを踏まえ，特に外国人口座開設者に対しては，身分確認を徹底するほか，在留期限と開設目的をよく確認の上で

○　日本では，売買目的で口座を開設することはもちろんのこと，口座を売買する行為も犯罪となる

○　不審な口座は，警察に通報する

旨の確実な周知徹底をお願いします。