JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

スパイウェア啓発WG活動報告

野々下幸治

ウェブルート･ソフトウェア(株)

2007 年 6 月6日

2006年度の主な活動

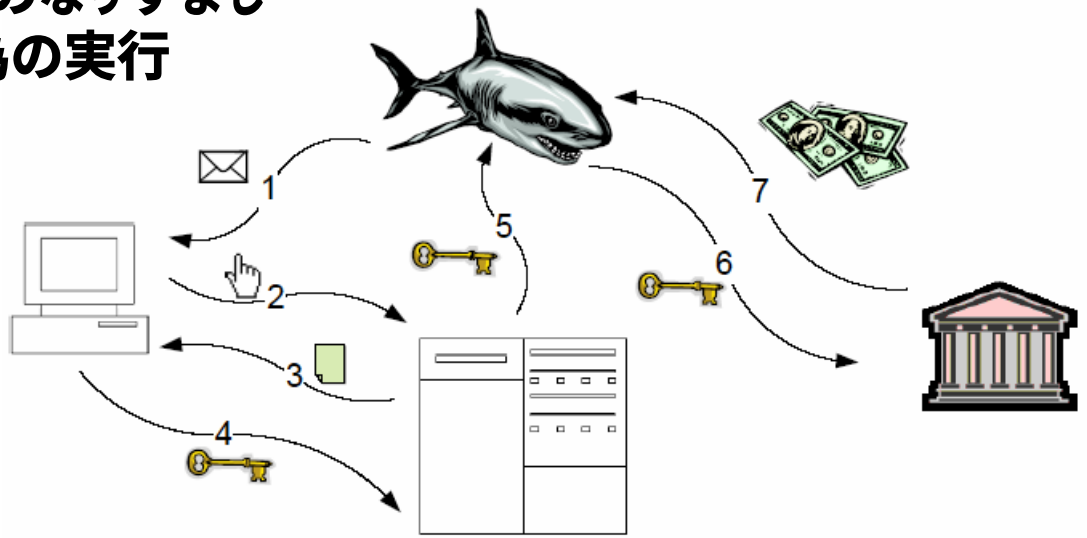
- ECOM(次世代電子商取引推進協議会) の情報セキュリティ懇話会への参加
  - 第3回懇話会での講演
    - スパイウェアのビジネスモデルの紹介
    - 偽セキュリティソフトの実態の報告
    - オンラインゲームを狙ったトロイの木馬の実態の紹介
  - CDTの副局長およびASCの設立者であるAri Schwarz氏の講演と自由討論
    - 主にUSのプライバシー保護法に関して講演

ﾌｨｯｼﾝｸﾞ対策協議会

- ﾌｨｯｼﾝｸﾞ対策協議会の技術･制度検討WGの主査をJNSAとして務める
  - 技術･制度検討WGを5回開催
  - 技術･制度検討ワーキンググループの報告書の作成

ﾌｨｯｼﾝｸﾞを攻撃段階に沿って整理

0. **準備段階**
- **トリガの実行**
- **トリガにユーザが反応**
- **ﾌｨｯｼﾝｸﾞ攻撃の実行**
- **機密情報の送信**
- **機密情報をフィッシャーに送信**
- **機密情報を利用してのなりすまし**
- **最終目的の不正行為の実行**



技術的対策と法･制度面での対策のまとめ

ステップ	内容	技術的対策方法	法･制度面での対策
0：フィッシングの準備	攻撃ターゲットの選別や電子メール送信のためのアドレス収集。類似ドメインの取得	類似ドメイン取得の監視	類似ドメイン取得の禁止 JPRSによる類似ドメイン取得に関する注意喚起の提供
1：メールの送信	フィッシングサイトに誘導するために詐欺メールの送信	ISPによるメールフィルタリング技術 送信者認証、メールの電子署名 *課題：迷惑メール用フィルタのため、フィッシングの場合フィルタの誤検知のとの見分けが付かない*	迷惑メール法、偽装メールに対する著作権法の適用 *課題：迷惑メール法はフィッシングに対しては有効な歯止めとならない。* *送信者認証や電子署名の技術を推進する制度が必要とされる。*
2：ユーザがメールに反応	届いたメールを開封し、URLをユーザが実行	証明書付き電子メール	教育・啓発活動によるユーザの教育 フィッシング対策協議会のWebによるフィッシングの啓発活動
3：フィッシング攻撃の実行	偽装サイトにユーザが訪れる	クロスサイトスクリプティングの脆弱性の除去	偽装Webに対する著作権法の適用
4：機密情報の送信	偽装サイトにユーザが個人識別情報を入力する	ユーザが容易にフィッシングサイトを見分けられるようにするための技術 フィッシング対策ツールバー 実在性も保証する厳密な証明書(EV SSL) サイト画像認証 画像を利用したユーザ認証	*課題：制度面での技術の普及の後押しが必要*
5：機密情報の入手	偽装サイト上の収集された個人識別情報をフィッシャーが取得	マルウェアによる識別情報の盗み取りを防止するための技術 ソフトキーボード、キーロガー検知	*課題：個人識別情報の入手を罰する手段がない*
6：機密情報の利用	個人識別情報を利用してユーザになりすましてサービスを利用	盗み出した個人識別情報を利用してもなりすましを出来ないようにするための技術 二要素認証 帯域外認証 *課題：コスト*	不正アクセス禁止法 *課題：制度面での技術の普及の後押しが必要*
7：不正行為の実行	クレジットカードの利用や預金の引き落としなど不正行為の実行	トランザクションの不正検知	現行の刑法に順ずる *課題：国際的な犯罪に対する国内法の限界*

2007年の活動

- スパイウェア対策がほとんどのアンチウイルス対策にも組み込まれ、用語の認知度もかなり高くなったことにより、啓発活動は終了。
- よってスパイウェア対策啓発WGは2006年で活動終了