Anti-phishing Working Group General Meeting APWG 2006 eCrime Researchers Summit 報告

主査代理参加・報告
坏　毅(株式会社　日立製作所)

1 APWG General Meeting 概要

- 開催場所: Radisson University Hotel 米国フロリダ州オーランド
- 日程: 2006年11月14日～15日（2日間）
- 参加者: 200名程度（APWG会員企業・団体のみ）
  - 米国／ヨーロッパ諸国(イギリス・ドイツ・スペイン等)／アジア諸国（韓国・日本）／その他ブラジルなどの企業・政府・業界団体の関係者

＜講演内容＞

- 一日目

① フィールドレポート：各国におけるフィッシング詐欺の状況と取り組み状況（1−1）
② クライムウェア・ラウンドテーブル：クライムウェアによるインシデント被害の現状（1−2）
③ 法執行機関、業界団体における取り組み状況（1−3）
④ 新しい情報共有やフィッシングメールフィルタリングに関する取り組み（1−4）

- 二日目

① ポリシー・ラウンドテーブル：ドメイン名登録を悪用したフィッシング被害への対応（1−5）
② テクニカル・ラウンドテーブル：ボットによる被害の現状と対策
③ サーチ・ラウンドテーブル：一般利用者のフィッシングの判断基準と教育の効果（1−6）

1-1 各国の被害状況と取り組み①

- 米国の状況　講演者：Bassam Khan（Cloudmark）
  - フィッシングの発生件数：劇的には増えていないが、少しづつ増加傾向
  - フィッシング手口の変化
    - ターゲットの変化：大規模の金融機関から中小の金融機関がターゲットに
    - Vishing等新しい攻撃手法の出現
  - ボットネット対策が重要に
    - ボットの利用拡大：90%のスパムメールがボットネットから送信されている
- スペインの状況　講演者：Enrique Gonzalez Ochoa(PandaLabs)
  - フィッシングの発生件数：フィッシング詐欺以外の詐欺事件が多い
  - 宝くじ（lottery）を利用した詐欺
    - 宝くじが非常に庶民的で海外でも人気（フランス、ドイツ、米国、韓国等）
    - 「おめでとうございます、当選しました」というフィッシングメール
    - 2006年7月に300人が逮捕、50カ国で2万人の被害

1-1 各国の被害状況と取り組み②

- イギリスの状況　講演者：Colin Whittaker（APACS）
  - フィッシングの発生件数：増加傾向（9月に1400件超）
  - オンライン詐欺による被害額：2005年上期£1450→2006年上期£2250
  - 攻撃手法：メールやWebサイトの詐称が多く、次にキーロガーが多い
  - フィッシング手口の変化
    - マルウェアの進化、ボットネットやルートキットの利用が拡大
    - パーソナライズされたフィッシングメール（成功率大）、Vishing、SMiShing等
    - 犯罪組織のほとんどが東欧（ロシア、ルーマニア等）、最近は西アフリカから
  - その他の取り組み： e-Banking Fraud Liaison Groupの立ち上げ

- 日本の状況　講演者：Yurie Ito(JPCERT/CC)
  - フィッシングの発生件数：金融機関をターゲットしたものも少ない
    - 理由：言語の壁等
  - その他の詐欺
    - ワンクリック詐欺、またはツークリック詐欺
    - 偽セキュリティソフトウェア（フェイクソフトウェア）の押し売り

1-1 各国の被害状況と取り組み③

- ドイツの状況　講演者：Waldemar Grudzien（Bundesverband Deutscher Banken）
  - 攻撃手法の変化
    - 伝統的なフィッシング詐欺（10%）からマルウェアを利用した攻撃（90%）に移行
  - オンラインサービスバンキングにおける対策
    - ほとんどの金融機関がPIN/TAN(取引番号）による認証サービスを提供済み
    - フィッシング詐欺対策としてiTANに移行、一部携帯電話を利用したmTANも導入
    - 2ファクタ認証（ひとつは動的な要素による認証）が必須

- 韓国の状況　講演者：Terrence Park（KrCERT/CC）
  - フィッシングの発生件数：少ない
  - オンラインサービスバンキングにおける対策
    - PKIの利用：Financial Supervisory Service（FSS）がセキュリティ規則を定めている
  - その他の取り組み
    - 普及啓発ツール（パンフレット・教材、相談窓口の提供）
    - 中小企業支援策として、脆弱性検査サービス、Webアプリサンプルコードの提供

1-2 クライムウェア・ラウンドテーブル①
（クライムウェアの現状と対策）

- クライムウェアによる被害の現状 （SymantecのISTRの調査）
  - マルウェアの目的
    - トップ50のうち、30は個人情報の窃取を目的としたもの
  - ボットの現状
    - 一日平均5万7千台のボットPCが活動、6ヶ月間で5百万台のボットPCを発見
    - ボットPCの所在地：中国が最多（20%）、米国（19%）、日本は10位で2%
  - スパムの現状
    - ネットワーク上を流れる電子メールの54%はスパム、発信国は米国が50%以上
    - スパムの122通に1通はマルウェアを含んでいる
  - DoS攻撃の現状
    - 毎日6000程度のDoS攻撃が検知されており、増加傾向
    - ターゲット国：米国が最も多く（54%）、中国の12%、攻撃元も米国が最も多い
  - クライムウェアの技術的な進化
    - 存在（プロセスやファイル）を隠すルートキット（haxdooor etc.）、アンチウイルスやパーソナルFWをバイパスするトロイの木馬など

1-2 クライムウェア・ラウンドテーブル②
（クライムウェアの現状と対策）

- 対応状況
  - 非常に厳しい状況（パネリスト全員の見解）
  - 犯罪者が新しいタイプのクライムウェアを次々と生み出す一方で、、、
    ユーザの理解不足及び対策不足、かつ効果的な抑制手段がないのが現状

- 今後の対策の方向性（案）
  - マルウェアの作成が割に合わない（ビジネスにならない）ようにすること
  - 罰則を厳しく、かつ判決の迅速化を図る
    （裁判に何ヶ月も何年も掛かるようでは駄目）
  - 国際的な司法・警察の管轄権の明確化
  - ユーザ意識を変える啓蒙：セキュリティ意識の自覚（awareness）

1-3 法執行機関、業界団体の取り組み①

講演者：Jonathan Rusch（US Department of Justice）

- 米国の取り組み
  - フィッシング詐欺、オンライン詐欺犯罪者の逮捕実績
    - 州・国を超えた司法、警察の協力により、2006年だけでも多数の犯罪者を逮捕
  - 大統領令（EO）によりIdentity Theft Task Forceを設立（2006年5月）
    - 目的：ID窃取防止に関わる米政府の取り組み強化、戦略計画の立案
- イギリスの取り組み
  - 「Fraud Act of 2006」法の制定
    - 複数法でバラバラに取り扱われていたID窃盗を一つの法律で包括的に規定
      - ID窃盗を目的とするツールの所有：最高5年の禁固刑
      - ID窃盗を目的とするツールの作成：最高10年の禁固刑
- 国連「UNCCIEGFCMFI」の取り組み
  - United Nations Crime Commission Intergovernmental Expert Group on Fraud and the Criminal Misuse and Falsification of Identityの略
    - 国連加盟国の政府、警察・司執行機関による国際的な協力体制の確立
    - ID窃盗事件の扱いに関するガイドラインやベストプラクティスを策定

1-3 法執行機関、業界団体の取り組み②

講演者：Donald Saxinger（Federal Deposit Insurance Corporation）

- 連邦預金保険公社（FDIC）の取り組み
  - ID窃取に関する様々な調査の実施
    - FDIC Study: Putting an End to Account-Hijacking Identity Theft（2004年11月）
    - Identity Theft Study Supplement on Account-Hijacking Identity Theft（2005年6月）
  - インターネットバンキングのガイドライン策定
    - FFIEC Authentication Guidance（2005年10月）
      （Authentication in an Internet Banking Environment）
      - 複数ファクタによる認証、階層化されたセキュリティを要求
    - Authentication FAQs（2006年8月）
      - Authentication Guidanceのスコープの明確化
      - 中小の金融機関のほとんどがTSP（Technical Service Provider）を利用しており、TSPを利用する際の配慮事項等も記載

1-4 その他取り組み

- スパムデータベース(SpotSpam) 講演者： Thomas Rickert(ドイツISP協会)
  - EUを中心とした国際的なスパム事例のデータベース
  - 背景： 警察・司法機関による国際的な情報共有は遅れていること
    スパム被害者である個々のユーザが訴訟を起こすことが難しいこと
  - 狙い： 脅威分析での活用、ISPや執行機関における対策の支援
    スパマーに対して訴訟を起こす際の必要な証拠を提供
- メールフィルタリング(PILFER)　講演者：Ian Fette(Carnegie Mellon Univ)
  - フィッシングメールに特化したメールフィルタリングツール
    - フィッシングメールの特徴を抽出し、独自の分析アルゴリズムを実装
  - フィッシングメールの特徴
    - HTMLメール、javascriptの存在
    - URLドメインの登録期間
    - メール内のURLリンク数やドメイン数、ドット(.)数、またはIPベースURL
    - 表記されるURLと実際のURL(hrefタグ記載のURL)が不一致
  - テスト結果
    - フィッシングメール認識率(93%)、誤認率false positive(0.1%)、false negative(7%)

1-5 ポリシー・ラウンドテーブル
（ドメイン名登録を悪用したフィッシング詐欺の現状と対策）

- 現状
  - 2006年10月に確認されたフィッシングサイトの56%がドメイン名を悪用
- ドメイン名悪用の手口

  ・スペル違いを巧妙に隠す　例：vvellsfargo.com（正：wellsfargo.com）、citilbank.com
  ・信頼されそうなそれっぽいドメイン名　例：accountvalidator.com, onlineaccess.net
  ・ホスト名を加えて、本物らしく見せる
  ・正しいドメイン名のカントリーコードだけを変える
  ・スパムフィルタをすり抜けるためのワイルドカードDNS、rotating DNS、エイリアス等の利用
- 問題点
  - インシデント発生時、対応が遅いドメイン登録事業者の存在
    - フィッシャーはこうした事業者を選んでドメイン登録に利用
- 想定される対応策
  - 事業者ごとに異なるインシデント報告・対応に関する基準の改善が必要
    - ICANNのポリシー・基準に組み込む
    - APWGが登録事業者に対して認可を発行
    - PDRP（Phraud Dispute Resolution Policy）の策定
      - UDRP（統一ドメイン名紛争処理方針）同様のポリシーを作成

1-6 リサーチ・ラウンドテーブル
（一般利用者のフィッシングの判断基準と教育の効果）

- フィッシングメールの判断基準の調査 （インディアナ大学のMarkus Jacobsson氏）
  - 一般消費者へアンケート実施 「絶対フィッシングメール」～「絶対本物のメール」の5段階評価
    - 本物のメールと判断する基準

・パーソナライズされている（個人名明記で送付）
・Verisignロゴが貼付してある（他の証明書ベンダのロゴでは効果なし）
・クリック先のウェブサイトに著作権等、法的文言がきちんと掲載されている
・強制（「～してください。さもないと・・・」ではなく、任意（「確認してみてください」）

    - フィッシングメールと判断する基準

・スペルミスがある（ユーザは非常に敏感）
・URLが架空っぽい、またはIPアドレスである
・「このメールは本物です」と書かれている、または安全性を強調している
・クリック先のウェブサイトのデザインが素人っぽい

- 教育効果の調査 （カーネギーメロン大学Lorrie Cranor氏）

・金融関係の情報を開示するよう求められて、おかしいと感じる（55%）
・異なるタイプのフィッシング詐欺に対しては知識が活かされない
・メールの送信元が自分の取引企業（口座を持っている等）であれば怪しいとは思わない
・電子証明書の期限切れ等のポップアップは良くわからないから無視する
・ツールバーのフィッシングサイト監視ツールに頼る
・教育資料を読んだ直後であれば、フィッシングへの判断力が飛躍的に向上する

2 eCrime Researchers Summit概要

- 開催場所：Radisson University Hotel 米国フロリダ州オーランド
- 日程：2006年11月16日～17日（2日間）
- 主催：APWG、フロリダ法執行機関、フロリダ州立大学、セントラルフロリダ大学による共同開催（オープンなミーティング）
- 参加者：100名程度（APWGメンバ、大学研究者、学生、州・政府関係者）
- 目的：オンライン詐欺に関連する未公開の調査結果/ベストプラクティスの発表
  学術、法律、IT技術分野における関係者の協力強化

＜講演内容＞

- 一日目
  ① クライムウェアの定義と分類 (2-1)
  ② アンチ・フィッシング・クライムウェア技術：FhishFeeding (2-2)
  ③ インシデント・レポーティング・インフラ構築：Phisherman (2-3)、PhishScope (2-4)
  ④ フォレンジックツール・技術：シリアルボット、REGAP (2-5) 、オープンツールの有効性
- 二日目
  ① 政府関係機関（DHS、NCSD）によるフィッシングに関する調査と取り組み状況
  ② フロリダ州（Florida Computer Crime Center）の活動紹介 (2-6)

2-1 クライムウェアの定義と分類

講演者：Aaron Emigh（Radix Labs）

- 被害状況
  - オンラインIDの窃取事件が急増、フィッシングによる直接損失だけでも年10億超
  - 特にクライムウェアを使ったフィッシング詐欺が急速に拡大
- クライムウェアの定義
  - ユーザの予期しない非合法な動きをするソフトウェアで、かつその配布により利益を得ることを意図したもの

クライムウェア	クライムウェアでないもの
・キーロガー ・EメールとIM リダイレクタ ・セッションハイジャッカ ・トロイの木馬 、ルートキット	・アドウェア ・スパイウェア ・愉快犯による悪意のコード ・ボットネットコントローラ

- クライムウェアの分類
  - 攻撃手法、増殖方法、利用目的、活用技術などにより分類することが可能

例【増殖方法による分類 】

(a) ソーシャルエンジニアリング	(b) セキュリティエクスプロイット
・メールへの添付 ・ピギィバッキング	・ワーム ・ブラウザの脆弱性 ・ハッキング ・アフィリエイト広告

2-2 アンチフィッシング技術（FhishFeeding）

講演者：John Brozycki（Financial Services Network Security Consultant）

- 概要
  - フィッシングサイトに擬似データを提出するプロセス／ツール
    - ① フィッシングサイトのフォームに合わせて、一見有効な擬似データを生成
    - ② 現存のフィッシングサイトのフォームに擬似データを転送
    - ③ 擬似データを利用してサイトに接続してきた不正なアクセスを監視・追跡
- FhishFeedingによる効果
  - フィッシング詐欺による被害の減少
    - 売買目的のフィッシャーに対して、データ自体の価値を低下させる
    - 被害者に時間的猶予を与える（金融機関に連絡するための時間を提供）
    - 金融機関は擬似データを監視し、そのデータを利用したアクセスを特定し、そのソース（アクセス元）を追跡
    - フィッシャーにフラストレーションを与え、攻撃を諦めさせる

2-3 レポティング・インフラ（Fhisherman）

講演者：Greg Tally（SPARTA）

- 概要
  - リアルタイムでフィッシングデータの収集・検証・転送・アーカイブするシステムを構築することを目的としたプロジェクト
  - Sparta、南メソジスト大、Internet Compliance Systems、APWG等のメンバで推進
- 現在のレポーティングシステムの課題
  - 毎日大量のフィッシングメールが出現、情報収集機関には大量のレポートが、、
  - インシデントレポートには誤った情報や重複したレポートが多く、その対応が情報収集機関の大きな負荷となっている。
  - 迅速なレスポンスには攻撃の検知からレスポンスまでの時間の短縮が不可欠。
- Fhishermanの特徴
  - レポジトリの信頼性を高めるため、情報の収集フェーズにおいて2段階でその信頼性が自動検証される。
  - 既存のレポートの類似性を評価し、攻撃手法の特徴に基づき潜在的に関連しそうな攻撃とリンクが取られる。
  - ISP、ブランド所有者、防御ツール（フィルタツール等）にリアルタイム、かつ正確なフィッシングデータ（ブラックリスト等）を提供可能

2-4 レポティング・インフラ（FhishScope）

講演者：John Quarterman （InternetPerils）

- 概要
  - 特定のISPに存在するアクティブなフィッシングサーバ群（Phishing Cluster）を検知・追跡する技術
  - Phishing Clusterの情報をインターネットトポロジにグラフィカルにマッピングし、時間経過に従った変動を表示

    APWGに報告されたレポートの分析結果(2006/5/8)
    ：フィッシングメッセージ（2174件）、IP address（395件）、Cluster（27件）

- FhishScopeによる効果
  - 効率的なインシデント対応の実施
    - ターゲットとなった組織は、Phishing Clusterの情報を利用してISPに連絡し、効率的にフィッシングサイトを停止させることが可能
    - ISPや法執行機関は、Phishing Clusterの情報により、報告された個々のレポートごとに対応するのでなく、効率的な対応が可能

2-5 フォレンジック技術（REGAP）

講演者：Professor Xiaotie Deng（City University of Hong Kong）

- 背景
  - 今後、Webアイデンティティとして、従来のURIに変わり、Unicodeを利用したIRI/IDNの利用が広がっていくことが予想される。
    - IRI : Internationalized Resource Identifier
    - IDN : Internationalized Domain Name
  - Unicodeの文字セット(UCS)には視覚的、意味的にも非常に似ているコードが多数存在するため、潜在的にフィッシングに利用される危険性が非常に高い
    - 例えば、citibankという文字でも263,189,025,000ぐらいのパターンかある
- REGAPツールの概要（Regular Expression Generator for Anti-Phishing）
  - Unicodeによるドメイン名を悪用したフィッシング詐欺を回避
    - 視覚的、セマンティック的に似たUnicodeアタックを回避可能
    - URIに利用される可能性の高いワード毎のリストを構築、潜在的にフィッシングに利用される可能性の高いIRI/IDNパターンを特定（高速化対応）
      - このRegular Expressionで構成される7000万のドメイン名を87秒で検証
  - 類似したツールとして、IRI/IDN SecuChecker

2-6 NSCD、FC3の取り組みの紹介

講演者：Michael Levin（National Cyber Security Division）
Mike Cantey（Florida Computer Crime Center）

- National Cyber Security Division（NSCD）の取り組み
  - サイバー・セキュリティ・パートナーシップ・プログラム（Cyber Security Partnership Program）を作成
    - 業界／政府／学界の間で効果的なパートナーシップの育成
  - US –CERTやLaw Enforcement & Intelligence Branchの運営
    - サイバー脅威や脆弱性の分析や緩和、脅威に関する警告の発令、インシデント対応の調整、National Cyber Alert System の運用
- Florida Computer Crime Center（FC3）の取り組み
  - フロリダ州立大学、National White Collar Crime Centerと協力し、サイバーセキュリティ関する調査／教育／トレーニングを目的としたFlorida Cybersecurity Institute（FCI）を組織
  - フロリダを拠点とする3つの金融機関および法執行機関（FBI、地元警察や州裁判所）と協力し、Phishing Post Mortem（PPM）を組織
    - フィッシング攻撃のプロファイリング、組織的レスポンス手法に関する調査

3 所感

- アンチフィッシングに向けた様々な取り組みが紹介され、関係者による問題解決に向けた意欲が強く感じられた。一方で欧米諸国とアジア諸国の間での温度差が存在することも感じた。
- フィッシングがソーシャルエンジニアリング的な詐欺行為からクライムウェアを活用したより技術的な方向に進化しており、対策もより複雑化している。
- 欧米諸国の政府・業界団体では、フィッシング/ID窃盗に関する取り締まりを強化する法整備やガイドラインの策定が非常に積極的に進められている。
  - FDICの「FFIEC Authentication Guidance」、英国の「Fraud Act of 2006」、ドイツにおけるオンラインバンキング関連の規則など
- 従来同様の根気強い教育・啓蒙活動、またタイムリーな警告の発信が重要であり、日本でも「フィッシング対策協議会」のような活動を通して、さらなる情報連絡・連携体制の構築、人的資源の共有等が必要