APWG 2006 eCrime Researchers Summit

Radisson University Hotel　米国フロリダ州オーランド
2006 年 11 月 16 日～17 日

主査代理参加・報告
坏　毅（株式会社　日立製作所）

Ⅰ．ミーティング趣旨

eCrime Researchers Summit 2006 は、APWG、フロリダ法執行機関（Florida Department of Law Enforcement）、フロリダ州立大学、セントラルフロリダ大学 4 者による共同主催のカンファレンスで、今回はじめての開催となる。カンファレンスの目的は、過去公開されていなかったフィッシングやファーミング、クライムウェア等を利用したオンライン詐欺に関連する調査結果やこれらに対抗するベストプラクティスを発表し、eCrime を抑制するための対策のアイデアを議論すること、さらには学術、法律、IT 技術分野における関係者の協力を強化し、eCrime の対策技術の開発を促進することである。Anti-Phishing Working Group General Meeting が AWPG member だけのクローズドなミーティングであるのに対して、eCrime Researchers Summit は、大学研究者、学生、フロリダ州の行政関係者等、フィッシング詐欺、オンライン詐欺に取り組む幅広いメンバが 100 名程度参加していた。

本カンファレンスでは、フィッシングやクライムウェアに関連する新しい攻撃手法や対策・対応技術に関する研究結果、また政府・フロリダ州の法執行機関の関係者により連邦政府、州としての取り組みが紹介された。特に 1 日目は、前日までの Anti-Phishing Working Group General Meeting よりさらに技術的に踏み込んでフィッシングに関する取り組みが紹介、議論された。

Ⅱ．セッション概要

第 1 日目（11 月 15 日）

1 日目は、フィッシングやクライムウェアに関する新しい攻撃手法や対策手法など、技術的な研究結果や現在の取り組みが紹介された。以下に各セッションの概要を纏める。

<Phishing and Crimeware>

① <u>The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond</u>

講演者：Aaron Emigh（Radix Labs）

オンライン ID の窃取事案は年々急速に増加してきており、フィッシング詐欺による直接の金融損失だけでも年 10 億を超えている。特に最近増加しているのがクライムウェアを使った個人情報や機密情報の盗難であり、フィッシング詐欺でもクライウェアによる被害が急速に増えてきている（2006 年 5 月に報告された、キーロガー種類=215、キーロガーの配布サイト=2100）。このセッションではクライムウェアを定義し、その攻撃手法／配布方法／使用方法の観点から分類を行い、対策について解説した。

<クライムウェアの定義>

ここでの「クライムウェア」の定義は、ユーザの予期しない不法な（非合法）動きをするソフトウェアで、特にその配布により利益をうむことを意図したソフトウェアを指す。オンライン詐欺組織の増加に伴い、クライムウェアも急速に増加しており、ID やその他センシティブな情報の摂取に利用されている。下記にクライムウェアと定義されるソフトウ

ェアと、そうでないものの例を示す。

【クライムウェアの範囲】

クライムウェア	クライムウェアでないもの
- キーロガー・スクリーンロガー - 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 - トランザクションジェネレータ - Rootkit - データ盗難	- 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 - データコレクタ・フォワーダ -

クライムウェアの分類方法としては、増殖方法、利用目的、活用技術などによる分類等が考えられる。例えば、利用目的による分類では、ID 摂取を目的としたクライムウェアとそれ以外の収入を目的としたクライムェアに分けることができる。前者の例としては、キーロガー・スクリーンロガーやセッションハイジャックなどがあり、後者の例としてはスパム転送、DoS 攻撃、クリック詐欺等が挙げられる。また、下記に増殖方法による分類を示す。

【クライムウェアの増殖方法】

(a) ソーシャルエンジニアリング	- メールへの添付 - ピギィバッキング（例：ZCODEC、ErrorSafe）
(b) セキュリティエクスプロイット	- インターネットワーム - ブラウザの脆弱性 - ハッキング - アフィリエイト広告（例：IFRAME CASH）

クライムウェア対策としては、クライムウェアの配布／感染／実行それぞれのタイミングにおける対策の実施が必要である。例えば、配布のタイミングでは適切なメール、その他フィルタリングが有効であり、またクライムウェアの感染や実行を防止するためには、アンチウイルスやコードサイニングが必要となってくる。

② PhishFeeding: *An Active Response to Phishing Campaign*

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

このセッションではフィッシング詐欺による被害を減少させるための技術（ツール）として PhishFeeding が紹介された。PhishFeeding の仕組みの他、典型的なフィッシングの被害パターンに対する PhishFeeding の有効性が解説された。

PhishFeeding とは、フィッシングサイトに擬似データを提出するプロセス／ツールである。通常は擬似データの生成やサイトへのアクセスのモニタリング等がシステムにより自動化されている。PhishFeeding のプログラムは、通常、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し、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する（＝罠を仕掛ける)。また、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・追跡する機能を有する。

【通常のフィッシング被害者のレスポンスレベル】

- レベル 0：何もしない、または気付かない
- レベル 1：通知する
- レベル 2：フィッシングサイトを停止させる
- レベル 3：法執行機関と連携する
- レベル 4：フォレンジック／フィッシング分析
- レベル 5：積極的なレスポンス

通常は上記レベルの 2 程度までしか対応しない事業者がほとんどである。一方、PhishFeeding を利用することにより下記のような効果が得られる。

【PhishFeeding による効果（被害の低減)】

- フィッシャー（攻撃者）が売買目的で情報を収集している場合、データ自体の価値を低下させることができる
- 利用者がフィッシングの被害に気付き、金融機関に連絡するための時間的猶予を提供する
- 金融機関は擬似データを監視し、それを利用した不正なアクセスを特定し、そのソース（アクセス元）を追跡することができる
- 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

一方、PhishFeedingの罠を回避する、Turning Numberを実装したフィッシングサイト（例：ebay（2006年9月））やman-in-the-middleとして動作し、都度アカウントの有効性をチェックするようなサイト（例：paypal（2006年9月））も出現している。今後は、パーソナライズされたフィッシングメールやサイト停止を難しくする対応が取られたフィッシングサイトが増えていくものと予想される。

<Online Fraud>

③ Consumer Perspective

講演者：Susan Grant（National Consumer League） susang@nclnet.org

National Consumer League （NCL）は、消費者へ様々な情報やアドバイスを提供する組

織であり、1996 年よりインターネット詐欺、2003 年にはフィッシング詐欺に関する情報の提供を開始している（www.phishinginfo.org）。本セッションでは、NCL の組織の成り立ち、フィッシング詐欺に関連する NCL の活動が紹介された。

【NCL が実施した調査の抜粋】
- 2004 年 5%（450 万人）の消費者がフィッシングメールを受け取り、その内半分は ID 盗難の犠牲者となった。
- ID 盗難の犠牲者は、30%の人がその後インターネットの利用を減らし、29%の人がオンラインショッピングの利用を減らし、25%の人が完全にオンラインショッピングの利用をやめている。

【NCL が推奨するフィッシング対策】
- 更なる消費者教育のサポート
- デザイン向上によるユーザ・エクスペリエンスの強化
- ユーザ認証、Web サイト認証の強化
- ISP、ドメイン所有者の協力（ホワイトリスト、ブラックリストの管理）

消費者のオンラインバンキング、E コマースに対する信頼を失わないようにするためにも、今後も政府、関連団体、個々の事業者の協力による、さらなる努力が必要であることが強調された。
- 公の教育機会
- 商用 Email への認証、証明書の適用
- ユーザ認証、Web サイト認証の強化
- 企業経営者への意識付け
- 民間、公共事業者におけるリソース、戦略の共有

④ Badvertisements: Stealthy Click-fraud

講演者：Mona Gandhi、Markus Jakobsson、Jacob Ratkiewicz（Indiana University）

本セッションではインターネット広告を利用した新しいクリック詐欺の概要、その対策が説明された。「Badvertisement」と呼ばれる詐欺手法は、効率的、かつ非常に精巧に偽装されたインターネット広告におけるクリック詐欺の手法であり、スパムの凶悪化した変形やフィッシング攻撃と位置付けることができる。実際にいくつかの広告スキームにおいてその存在が検証されている。

＜Reporting Infrastructure Development＞

⑤ *Using XML to Support Robust Information Sharing*: IODEF Automation Approach

講演者：Pat Cain（APWG）

本セッションでは、IODEF に準拠したフィッシング情報の報告・転送のフォーマットに関する取り組みが紹介された。Anti-Phishing Working Group General Meeting 報告書「Counter-e.Crime Data Resources, Tools, Techniques and Schema」を参照。

⑥ ***The Phisherman Project*: Using Comprehensive Data Collection to Combat Phishing**

講演者：Greg Tally（Malicious Code Defense SPARTA, Inc）

Phisherman Project は、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プロジェクトであり、現在 SPARTA、Southern Methodist University、Internet Compliance Systems、APWG 等のメンバで推進されている。本セッションでは、現在のフィッシング対策の限界、またこれら課題を解決する対策として Phisherman Project の有効性が解説された。

一日に1000近い新たなフィッシングメールが出現しており(ユニークなものだけでも)、インシデント情報の収集機関には大量のレポートが集まってくる。また通常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も多く、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、かつ効率的なレスポンスのためには攻撃の検知からレスポンスまでの時間短縮が不可欠であり、そのためにはシステムの自動化が必要となる。ただ、誤検出（false positive）は利用者の信頼を大きく損ない兼ねないため、収集されたレポートの信憑性のチェックも非常に重要となる。

Phisherman では、レポジトリの信頼性を高めるため、e-mail、フィッシングサイト、マルウェア等の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、レポジトリに登録される。また、さらに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仕組みも実装されている。

【Phisherman の効果】

- フィッシング事案に関する適切な計測・観測が可能となる。
- 防御メカニズム（e-mail フィルタ、ツールバーにおける警告）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）を提供することが可能となる（被害の最小化)。
- ブランド所有者に対して速やかに情報を提供することにより、より迅速な対応が可能となる。
- ISP は攻撃のトレンドを特定し、必要な箇所にリソースを集中することが可能となる。
- 法執行機関は、関連する攻撃を特定し、また効率的、かつ的確な訴訟が可能となる。

⑦ ***PhishScope*: Tracking Phish Server Clusters**

講演者：John Quarterman （InternetPerils）

「PhishScope」は、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 InternetPerils 社の技術（サービス）である。本セッションでは、PhishScope のシステムの概要、その有効性が紹介された。

PhishScope では、Phishing Cluster の情報がインターネットトポロジにグラフィカルにマッピングされ、かつ時間経過に従った変動を表示することができる。そのフィッシングデータとしては APWG のデータベースを活用している。

フィッシングのターゲットとなる組織は、この情報を利用して、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となる。また、ISP や法執行機関もこれら 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となる。ちなみに、例えば 2006 年 5 月 8 日に APWG に報告されたレポートを分析すると、フィッシングメッセージ（2174 件）、IP address（395 件）、Cluster（27 件）となっている。

＜Forensic Tools and Techniques＞

⑧ Exploring Investigative Methods for Identifying and Profiling Serial Bots

講演者：Robert Lyda（Sparta Labs）、James Hamrock（McDonaldBradley, Inc）

本セッションでは、ボットおよびボットネットの分析・追跡する手法として、シリアル・ボットに関する研究開発が紹介された。ボットは、ここ数年爆発的に増大しており、様々な攻撃や詐欺のツールとして活用されることから非常に大きな問題となっている（現在、10 万種類ものボットが存在する）。

シリアル・ボットとは、同じ作成者により繰り返し作成、または再配布されている一連のボットのことを指す。この研究では「ボットは同じ作成者により繰り返し作成・再配布されるケースが多い」という前提のもと、ボットの特性を分析することにより、一連のシリアル・ボットを特定し、ボットの増殖パターンを分析・追跡している。

【シリアルボットの特定方法の例】

- バイナリデータの中に残骸データが残っている（例：コンパイラのデータ）
- 作成者を特定するストリング（例：名前やハンドル）
- 特殊な圧縮、暗号アルゴリズムを使用している
- バイナリファイルにおける作者特有の構造

例えば、下記 pdb（プログラムデータベース）ファイルの特性を分析することにより、同じ作成者により作成されているボットであることを特定することが可能である。

- Microsoft Visual Studio でコンパイルされたバリナリに残っているデータ
- 作成者の開発マシンにある symbol file のフルパスやファイル名

- リファレンスに含まれている情報（ディスクドライブの文字、プラットフォーム名等）

実際に発見されたボットを対象に分析した結果では、シリアル・ボットは同じ特徴を有する傾向にあった。ただ、ボットの特性を特定するためにはさらなる研究が必要であることも判明。これら技術の研究は、他のフォレンジックでも活用できるものと考えられる。

⑨ ***REGAP*: A Unicode Attack Detection Tool**

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

本セッションでは、Unicode を利用した Web アイデンティティ（Web のリソースを特定するための情報）を利用したフィッシング詐称を検知するツールとして、City University of Hong Kong が開発した REGAP（Regular Expression Generator for Anti-Phishing）が紹介された。

今後、Webアイデンティティとして、ACSIIを利用する従来のURIに変わり、Unicodeを利用したInternationalized Resource Identifier（IRI）やInternationalized Domain Name（IDN）の利用が広がっていくことが予想される。しかし、Unicodeの文字セットUniversal Character Set（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（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）、潜在的にドメイン名を悪用したフィッシング詐欺に利用される危険性が非常に高い。

このような脅威に対抗するツールとして、IRI/IDN SecuCheckerというツールが存在する。このツールでは文字レベルのUnicodeアタックを回避することが可能である（REGAPはセマンティックレベルの攻撃にも対応可能）。REGAPでは、URIに利用される可能性の高いワードごとのリスト（Regular Expression）を構築し、潜在的にフィッシングに利用されるIRI/IDNパターンを特定する。これにより高速化も可能となり、実験ではこのRegular Expressionで構成される 7000 万のドメイン名を 87 秒で検証することできた（通常のパソコン（Pentium1.3GHz）を使用）。同ツールの評価版は、左記ホームページより入手可能である。（http://antiphishing.cs.cityu.edu.hk）

⑩ Forensics Analysis of Phishing Cases Using Free and Open Source Tools

講演者：Phillip Craiger（University of Central Florida）

本セッションでは、フィッシング詐欺に関連するフォレンジック手法として、オープンソースソフトウェアの利用方法、およびその有効性が紹介された。ここでは、具体的なツールとして、5 つのツールが紹介された。

① md5deep

ハッシュ値はファイルのフィンガープリント（Unique Identifier）と解釈することも可能であり、マルウェア等によるファイルの改ざんを検知するのに利用することが可能。

② foremost

fomremost は、ファイルのヘッダー・フッターファイル構造の特徴を利用してデータを復元するツール（例えば、JPEG イメージの OxEF で始まる）。うまく活用すれば拡張子の変更を検知することができる。

その他、sleuthkit（データの復元ツール）、pasco（Internet Explore history の展開など、事後的にどこにアクセスしたかを解析できるツール）、Autopsy（ファイルシステム等を分析する GUI ツール）などが紹介されたが、オープンソースは無料であるため商用ソフトの代替としてコスト低減には有効である一方で、必ずしも万能薬となるものではないことも指摘された。

第 2 日目（11 月 17 日）

2 日目は、主に政府やフロリダ州の法執行機関により、連邦政府・州としての取り組みが紹介された。以下に各セッションの概要を纏める。

＜Investigating Phishing＞

⑪ Government/Banking and Finance

講演者：Stanley W. Crowder（Banking and Finance Sector Detailee, Department of Homeland Security） stanley.crowder@dhs.gov

本セッションでは、国土安全保障省（Department of Homeland Security）の銀行金融部門に属する Stanley W. Crowder 氏により、米国におけるフィッシング攻撃の被害状況、また対策指針が説明された。

フィッシング詐欺はより組織化・専門化が進んでおり、昨年からだけでも新たな 100 以上の犯罪組織が増えている状況にある。そのフィッシングサイト数も継続して増えており、オックスフォード英辞書にも「フィッシング」という言葉が追加された。

【現在のフィッシング攻撃・被害の状況】

- 先週だけで 22,288 サイトのユニークなフィッシングサイトが出現している
- 米国の消費者は 2006 年フィッシング攻撃により、28 億円の損失を被る見込み
- 2006 年、350 万人の消費者がフィッシングにより窃取された金融情報を諦めている
- 被害件数が減る一方で、平均の被害金額が増加している（一件あたり 256 ドルから 1,244 ドルに増えている）

【フィッシングの最近の技術的な特徴】

- プロキシの利用が増えている
- プロキシボットの利用（アイデンティティとロケーションを隠すため）
- サイトを頻繁に変えている

このような状況の中、いくつかの企業は ID 盗難に関する保険サービスの提供をはじめており、またマイクロソフトも Internet Explore 7 にアンチフィッシング機能を実装した。法執行機関としては、海外の法執行機関とのさらに強いパートナーシップを確立し、インターネット犯罪に対するペナルティの強化を図っていきたいとのこと。

⑫ Government/Law Enforcement

講演者：Michael Levin（Department of Homeland Security National Cyber Security Division） Michael.Levin@usss.dhs.gov

本セッションでは、国土安全保障省（DHS）の国家サイバセキュリティ部門（National Cyber Security Division：NCSD）によるサイバセキュリティに関する取り組みが紹介された。

NCSD は連邦政府におけるサイバセキュリティの専門組織として設立されており、公的／私的な国際機関と協力し、米国内のサイバー空間、サイバー資産の安全性を維持することをミッションとしている。NSCD は、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）を作成し、業界／政府／学界の間で効果的なパートナーシップの育成を目指している。また、NCSD が運営する組織の中には US–CERT や Law Enforcement & Intelligence Branch があり、後者はサーバセキュリティ犯罪の防止、調査、告訴を実施することをミッションとしている。

下記は、サイバ警察（Cybercop）と USSS（United States Secret Service）が組織するサイバセキュリティに関する委員会とワーキンググループである。

① International Association of Chiefs of Police（IACP）
② Internet Disruption WG
③ Joint Task Force Global Network operation
④ Technical support WG

US-CERT Operation Branch は、24 時間体制でサイバー上の脅威の監視、警告、対応に取り組むUS-CERT の運営部門として組織されており、インシデントハンドリングや分析、マルウェアの研究などを行っている。

⑬ The Phlorida Autopsy Report

講演者：Mike Cantey（Florida Department of Law Enforcement, Florida Computer Crime Center（FC3））

本セッションでは、フィッシングに関連する Florida Computer Crime Center（FC3）の活動が紹介された。

FC3 では、フロリダ州立大学コンピュータ科学課及び National White Collar Crime Center と協力し、サイバ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）を組織している。また、フロリダを拠点とする 3 つの金融機関及び法執行機関（FBI、地元警察や州裁判所）と協力し、Phishing Post Mortem（PPM）を組織しており、フィッシングに関連する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を行っている。

企業が取るべきフィッシング対策としては、「顧客や従業員に対する教育」、「セキュリティポリシーや実践の改定」「レスポンスチームの組織化」、「ブランドやドメイン名の保護（早期取得）」、「地域の法執行機関とのコンタクトの確立」等の事前対策も重要である。

Ⅲ．所感

本カンファレンスでは、「PhishFeeding」、「Phisherman Project」、「PhishScope」、「Serial bot」、「REGAP」など、企業や研究者によるアンチフィッシングに関する取り組みが技術的にさらに踏み込んで紹介され、技術的な視点でフィッシング詐欺の現状や現在の対策が抱える課題を理解することができた。欧米諸国においてフィッシングメール／サイト数が急増し、さらにクライムウェア等の活用によりさらに対策が困難となっている現状をうかがうことができた。

政府・州関係者の報告からも、スパイウェアやボットなどのクライムウェアによる詐欺が組織化され非常に深刻化していること、またフィッシングの攻撃形態の変化・進化に伴い、様々な対応・対策が要求されている状況も実感させられた。

なお、本カンファレンスは今後も定期的に開催されるとのことであり、APWG の枠を越えた産学官の連携より、より現実的なソリューションが開発されていくことに期待したい。

以上