The Anti-Phishing Working Group

2007 APWG General Members Meeting

eCrime Researchers Summit

報告書

於;米国　ペンシルバニア州　ピッツバーグ

2007/10/2 – 2007/10/3: APWG General Members Meeting

2007/10/4 – 2007/10/5: eCrime Researchers Summit

フィッシング対策協議会

情報収集･提供ワーキンググループ　主査

中田　太(株式会社セキュアブレイン)

1．概要

APWG General Members Meeting

APWG は、フィッシング詐欺対策に取り組む世界最大の業界団体である。その APWG が主催する General Members Meeting は、APWG 参加企業・団体のみを参加者とするカンファレンスで、主にフィッシング詐欺に関する最新動向や事例紹介、パネルディスカッションからなる。本年は、FBI やカーネギーメロン大学などからなるアメリカのサイバー犯罪対策団体である NCFTA や、CERT、カーネギーメロン大学情報大学院(CyLab)が後援している。

APWG の 2007 年の成果としては、IODEF[1]へのフィッシング情報項目追加や、ICANN および FIRST[2]との連携を行っている。現在のフィッシング詐欺の状況としては、詐欺を行う側である犯罪組織の高度化があげられ、例として ROCK Phish（ロックフィッシュ）という世界的な犯罪組織について様々な調査レポートが発表された。FBI でさえも未だ全容がつかめていない組織であるが、欧米で発生するフィッシング詐欺の 8 割が ROCK Phish によるものであるという説もあるほど、強大なフィッシング詐欺の集団である。フィッシングに利用されるマルウェア技術も高度になっており、様々な組織・企業による対策検討がなされているが、有効な手段が無いためエンドユーザへの啓発・トレーニングの重要性が再度認識されつつある。

また、オーストラリア、ブラジル、オランダなど世界各国の状況紹介も行われ、フィッシング対策協議会も日本国内のフィッシング発生状況等の報告を行った。アメリカの事例と比較し、発生件数が非常に少ないという日本の特徴について複数の質問が寄せられた。

APWG General Members Meeting 会場の様子

[1] Incident Object Description and Exchange Format
[2] the Forum of Incident Response and Security Teams, http://www.first.org/about/

APWG eCrime Researchers Summit

カーネギーメロン大学情報大学院(CyLab)および PGP 社が後援し、より学術的なカンファレンスとして開催された。

主にパネルディスカッションにより活発な意見交換が行われている。内容は、技術的な問題からセキュリティ対策にかかるコストの問題まで幅広いが、残念なことにどの議論も結論が出るまでには至っていない。

学術的な成果のなかで注目すべきものとして、CANTINA というフィッシング対策技術の研究成果、および Anti-Phishing Phill というエンドユーザ向けの教育ツールの2点が挙げられる。CANTINA は、ブラウザのツールバーとして提供されるフィッシングサイト検知ツールとなっており、google の検索結果順位や参照するドメイン名がレジストラへ登録された時期等指標として、その Web サイトの安全性を判断する。また、Anti-Phishing Phill は、flash を用いて作成されたゲームとなっており、参照した web サイトが正しいドメインなのかどうかをエンドユーザが見分けるための知識が得られるようなシステムとなっている。

今後のフィッシングを含めたオンライン詐欺の動向として、すでに大きなビジネスとなっているオンラインゲームでの詐欺行為やハッキング、RTM(Real Money Trade)に関するトピックや、2008 年に控えているアメリカ大統領選挙において政治活動の妨害や誤認識につながるポリティカルフィッシングに関する議題もあがった。

国内からは、産総研が APWG 会員としてポスタープレゼンテーションに参加しており、PAKE という安全な認証基盤についての説明を行った。

APWG General Members Meeting 第 1 日目 (2007 年 10 月 2 日)

Opening Remarks and Conference Overview

APWG の現在の運営状態と今後の計画について簡単に説明。フィッシング詐欺の発生件数は増えているが特に新しい手口が出ていない。

Global Statistical Overview of Phishing and Crimware: Bassam Khan, Cloudmark

主に米国におけるフィッシング詐欺の状況について調査結果も含めて報告。フィッシング詐欺と迷惑メール、ウイルスの相関性に以前よりも重複が見られるようになっている。

International Field Report

- Australia: Steve Martin, Australian High Tech Crime Center (AHTCC)

AHTCC は組織としてはオーストラリア連邦警察の下部組織。活動内容としては IPA に通じるものがある。

オーストラリアにおけるフィッシング詐欺の状況を紹介。傾向としては増加傾向にある。なかでも職業斡旋サイトをかたって個人情報を詐取するタイプのフィッシングが多い。

- Japan: Futoshi Nakada, The Council of Ahti-Phishing Japan

  日本のフィッシング詐欺の状況についての質問内容は以下の通り。

  1. フィッシングメールについては日本語と英語どちらが多い？
  2. なぜ日本語のフィッシングメールは少ないのか？
  3. 日本語のフィッシングメールの送信元は？
  4. インターナショナルドメインを使ったフィッシング詐欺についての危険性は？

- Brasil: Cristine Hoepers, CERT.br

  ブラジルの CERT からの報告。ブラジルは、ほぼ毎回報告を行っている。フィッシング詐欺の発生件数もさることながら、ブラジルにあるサーバにフィッシングサイトがホスティングされていることも以前から問題視されている。数値的なものについては目新しい報告は無い。

- Netherland: Dave Woutersen, GOVCERT, NL

  オランダの CERT からの報告。自国が管理するべき Web サイトにフィッシングサイトができていないかどうかを検知するプロジェクトの紹介。また、二要素認証技術の紹介も行われた。

Potent & Emergent Technical Vulnerabilities Report Siege at the Desktop; Insurgency in Web Sapce

- Web Applications Vulnerabilities Survey and Review: Robert Hansen, CISSP

  Web アプリケーションに脆弱性があった場合に発生の可能性のあるリスクについての調査結果を発表。脆弱性のような内的な脅威の分析・対処はどうしても後手に回っている傾向がある。しかし、その状況が Web アプリケーションを利用するユーザにとってのリスクを高めていることを開発者はもっと認識するべきという提言。

- Web Applications Vulnerabilities Survey and Review Weakest Link on the Desktop: Still the User: CERT の発表者によるパネルディスカッション

  脆弱性の議論と同時にクライムウェアについての議論も交わされていた。クライムウェアについての新しい技術は発見されていない。

Technical, Tactical and Operations Report

- eCrime Network for Hire: Yinon Glasner, RSA Security
- Of BIND and Cache: Potent Technical Vulnerabilities Within BIND 9 Transaction IDs: Amit Klein, Trusteer
- The ROCK Targets Domain Name Management Systems: Implications for eCommerce Security: Rod Rasmussen, Internet Identity
- Phiriendly Phishing Landing Page Strategies: Leveraging the Phishing Victim Experience for Customer Education: Todd Inskeep, CISSP
- Building the Global Crimeware Radar Array: Jacomo Piccolini, Brazilian Academic Research Network CSIRT

フィッシングに関連する手法･ツールについての研究･調査の報告が行われた。特に「Fast Flux」等のドメイン乗っ取りの手法についての研究は盛んに行われている。

APWG Operational Resource Seesion

APWG の運営、特に DB の運用についての議論が行われた。

Working with Law Enforcement Session

- Enterprise Forensics and the Private Sector/Law Enforcement Interface: Joel Yusim, Cisco

官民の共同の取組みについての報告。米国では啓発･教育に関するプログラムの作成、対策ガイドラインの作成等において官民共同で積極的な取組みが行われている。また、法整備も進めており、フィッシングを禁止するための法律についても（国家レベルでは）まだ施行はされていないが議論は進んでいる。

The Cyberpol Proposal

- An eScotland Yard for Cybercrime: Cst. Kathy Macdonald, Crime Prevention Unit Calgary Police Service

カナダではサイバークライムの件数が全犯罪数の半数を超えている。注意喚起を行うポイントとして①教育面、②オンライン詐欺の防止、③重要インフラの防御、④人材登用の 4 つの面を上げている。「Cross Boarder Communication」というテーマも掲げており、他国の捜査機関との積極的な情報交換も行っていく意向。

Industry Collaborations at the Speed of eCrime

- A Colloquy and Call to Action by the National Cyber-Forensics & Training Alliance: Ron Plesco, CEO NCFTA 他 3 名

NCFTA は NPO で官民学をひとつに繋ぐ役割を持った組織。FBI とも共同で活動しており、オンライン犯罪防止における組織として重要な位置づけにある。今後の効果的な活動についてパネルディスカッ

ション形式で意見を集めていた。

Stalking the ROCK

- The NCFTA Shares Its Insights Into the Enigmatic ROCK Phishing Group: David Bonasso, NCFTA

ROCK Phish の追跡レポートの紹介 ROCKPhish が乗っ取ったドメインの調査、フィッシングサイト・メールの解析をはじめとした技術面と捜査機関と協力しての情報収集を行っているが、まだ全容解明には至っていない。

APWG General Members Meeting 第 2 日目 (2007 年 10 月 3 日)

Behavioral Vulnerabilities Session (Research Review: CyLab のメンバーからの報告)

- Supporting Trust Decisions Research at Carnegie Mellon
- You've been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings
- Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish

CyLab の人たちによる研究発表とパネルディスカッション。ソリューション・ツールの開発から教育プログラムの開発まで様々な活動を行っている。ソリューション・ツールの開発に関しては、フィッシングサイトを識別する技術、ユーザが正しいサイトを認識するための認証技術などが報告されていた。また、既存のソリューション・ツールについての調査も実施しており、その有効性についての報告もあった。

教育プログラムについてもゲームを活用したものロールプレイング形式等の手法が紹介され、それぞれの効果 (長所・短所) についても報告された。

Domain Name System policy Working Group Presentation and Panel

APWG で行われている DNS のワーキンググループの活動報告。

APWG Roundtable: Botnets, Network Forensics and the Diplomatic Aspects of the Private Sector/Law Enforcement Interface in eCrime Supression

- Following Botnet Controllers Home: Infiltrating and Monitoring eCrime Communications : Lawrence Baldwin, My|Netwatchman
- The Black Art of Mapping Criminal Actors to Correlative eCrime Events: Andre DiMino, Shadow Server
- Fraud 2.0 – How Botnet proxies defeat current credit-card and banking fraud protection: Alisdair Faulkner, Threat METRIX

- Geopolitical and Diplomatic Aspects of eCrime Networks: Sidney Faber, CERT
- Panel Discussion: Ethical, Legal and Techo-diplomatic Challenges to Botnet Mapping and Remedation

ボットに関連する研究報告が行われた。ボットの研究は米国でもかなり盛んに行われており、ハニーポッドをはじめとした「捕獲する技術」についての報告があった。

APWG Roundtable: Plotting Priorities 2008 and Beyond

今回の General Meeting のまとめ的なパネルディスカッション。今後どのようなオンライン犯罪が行われていくかについて議論が行われた。個人の資産のみならず、外交や政治にまで影響を与えることが予想されるが、オンライン犯罪はソリューション・ツールだけで解決できるものではないため官に求められる法の整備や安全なシステム構築のためのガイドライン作成等が議論された。

APWG General Members Meeting のまとめ

今回は CyLab、NCFTA のような教育・研究機関がスポンサーだったこともあり、教育プログラムに関連したプレゼンテーションも数多く行われた。依然としてフィッシング詐欺や、それに関連するクライムウェアの被害は後を絶たず、APWGもその守備範囲が広がりを見せている。ソリューション・ツールで防御しきれないという課題は以前より認識されているため、官民学で協調した取組みを行い、様々な側面から対策を講じるための枠組みができている。

日本国内においては、フィッシング詐欺・オンライン犯罪に関する状況は欧米とは異なるものの、フィッシング対策協議会がリーダーシップをとって、同様の活動を行うことでその存在意義を高めていけるのではないかと思われる。

APWG eCrime Researchers Summit 第 1 日目 (2007 年 10 月 4 日)

Keynote Speech: Gary McGrow 氏「Exploiting Online game」

- トラブルの原因となるインターネットの特性として「Connectivity」「Complexity」「Extensibility」があげられる。
- インターネットという仮想世界で「簡単に」行われている「Real Money Trade」
- 優秀なエンジニアの興味本位によるハッキング・クラッキング
- 進化の早いテクノロジー

これらの要素を満遍なく含んでいるのが現在のオンラインゲームの世界であるとして、そこに存在する危険性や実際の事例を紹介した。その上で「ソフトウェアセキュリティ」として「Risk Management」「Touch Points」「Knowledge」を軸としてその考え方を紹介した。

Examining the Impact of Website: Take-Down on Phishing

フィッシングのメカニズム (攻撃手法、対策手法) を実験・分析を行った。Rock Phish に向けたハニーポッドを用意して、そのフィッシング手法の調査や Fast-Flux Netowrk の研究を行っている。またフィッシングサイトがレポートされてから。ユーザがそこにアクセスする数の推移を調査した。

フィッシングを行った場合のコストと収入 (ROI) の試算なども行っており、非常に詳細な調査を行っていた。

Fishing for Phishers: Apply Capture-Recapture Phishing

NetCraft 社のデータベースを活用して、フィッシングサイトの正確な数を計測する実験を紹介していた。

Behavior Response to Phishing Risk

Phishing のリスクを低減していくためのトレーニングについて研究をしている CyLab の研究の発表。同じ内容であってもトレーニングの手法によって理解度が異なり、それに起因して受講者がフィッシングサイトに遭遇した際の振る舞いも変わってくる。その内容を数値化してどのようなグループにどのようなトレーニングを行っていけばいいかということをまとめあげている。

APWG eCrime Researchers Summit 第 2 日目 (2007 年 10 月 5 日)

Fighting Unicode-Obfascated SPAM

Unicode を表題や本文に活用したスパムメールの研究についての発表。Unicode を使用したスパムメールは現在既に 3 百万種類発見されている。検知技術についての紹介。

Comparison of Machine Learning Technique for Phishing Detection

フィッシングサイトの検知技術の紹介。一般的に URL のブラックリストやホワイトリストで対応するのではなく、フィッシングサイトの傾向を分析して検知能力を高めていく手法の紹介。

eCrime Researchers Summit のまとめ

研究発表の中で教育面についてのディスカッションが多かったことが印象に残った。

以上