CeCOS 2007

APWG Counter-eCrime Operation Summit

報告

於;米国　カリフォルニア州　サンフランシスコ

2007/5/30 - 2007/5/31

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）

開催概要とその趣旨

米国 Anti-Phishing Working Group が年に 2 度開催するカンファレンス。主に会員企業からの参加者と官公庁関連、(フィッシング詐欺の攻撃対象とされるような)民間企業の講演者(APWG のメンバー企業であることも多い)などの参加者で構成される。

講演内容はその講演者の立場により異なるが、主に自分、または自分が属する組織におけるフィッシング詐欺への取組みについて、中立的な立場(ベンダー色を出さない)で発表を行う。

また媒体関係者は参加不可となっているため、その言動や情報は外部へ漏洩することは基本的には無い。そのため、既に記事になっていたり、発表がなされているものではなく、最新情報を入手する場としても期待のできる場所である

第 1 日目(2007 年 5 月 30 日)

1. Take Down Tall tale-Battle Royale

各パネリストが「Funniest Story」としてフィッシングサイトの閉鎖について、自身、または自社の経験を紹介した。言語や習慣の違う文化圏に作られているフィッシングサイトの閉鎖には非常に苦慮しており、特に諸外国に対してのサイト閉鎖業務(交渉)は難航しているため、関係各所との連携が不可欠である。

ISP が自社サーバ内にある契約者のサイトの内容はまったく把握していないケースなどもあり。フィッシングサイト閉鎖への道のりは非常に険しい。最近では Vishing(Voice Phishing)の報告も増えてきている。

2. Colloquy on 'state of the art' eCrime Technology

(ア) Mapping the Mal Web, by McAfee

McAfee 社のフィッシングサイト検出技術「SiteAdvisor」のテクノロージーについて紹介したが、技術的に具体的・詳細な情報の紹介は無かった。

(イ) Predictions of Phuture Phishing

Speaker:Dan Habbard(WebSense)

自社の研究結果をもとに様々なフィッシング手法について紹介された。

- Wishing(Whale Phishing の略称。比較的著名な人物や、政治家などの富裕層を攻撃対象として行われるフィッシングのこと。手法としては「スピア型」に似ている)
- Blow Phish(暗号化されたプログラム(マルウェア)を悪用して情報搾取を行う手法)
- Sishing(検索エンジン(Search Engine)を活用したフィッシング手法)
- Hishing(Hardware Phishing の略称。Hardware 内に情報取得用のソフトウェアを忍ばせる手法)

(ウ) CERT/CC

Speaker: Ross Kinder of CERT/CC

フィッシングマルウェアへの対処を中心として、その効果的な対策方法について紹介された。

3. Taming the Toxic DeskTop

Speaker:Dave Culliance CISO eBay

世界で最も多くのフィッシングサイトを作られている会社として、その現状と今後の展望について考察を述べた。

これは以前から言われていることだが、犯罪が行われる場所（Threats Space）がリアルな世界からインターネットというバーチャルな世界に変わりつつある。実社会と同じように組織的犯罪が行われその被害範囲の拡大は非常に深刻。クライムウェアの増大は実社会に置き換えると犯罪を行うための道具（拳銃等の武器）としてその拡大が危ぶまれている。多くのユーザはフィッシング詐欺に対しての知識は驚くほど希薄である。教育（啓発）の重要性を考えつつも広範囲にその危険性と対策の必要性を広めていくことは困難である。

このような状況におけるソリューションとして考えられるものとして次が挙げららる。

- ユーザの環境をセキュアに保つ努力（教育やツールの導入）
- 安全度の高いブラウザーやツールバーの開発
- その他セキュリティツール（ソリューション）
- Web の認証技術
- 生態認証などの新しい技術

（参考資料：CeCOS_Cullinane.pdf）

4. Counter eCrime Data Handling Best Practice

Speaker:Lance James（SecureScience Corporation）

フィッシングマルウェアに関連した調査を行っていくと、その機能などから推察するに非常に大量の情報が盗まれていると思われる。フィッシングマルウェアはスパイウェア同様その存在自体を隠す傾向にあるためアンチウィルス・アンチスパイウェアソフトでは検知が困難。そのため情報が盗まれてもわからず、その存在自体が明るみに出ない。

5. Nation Report of UUAM-CERT

Speaker: Juan Carlos Guel Lopez

メキシコの CERT のレポート。メキシコでは自国の企業のフィッシングサイトはそれほど多くないが、フィッシング詐欺を行う犯罪組織の存在が深刻になっている。

6. Bridging Low Enforcement with Critical Infrastracture Experts（Round Table Session）

Speaker: Michael Levin(US Secret Service)、Erin Kenneally（CEO, Elchemy,Inc.）、Jon Praed（Infragard member）

SecretService、Infragard（電気、ガス、水道、国の機関等のいわゆる重要インフラの安全性を追及する組織体）のメンバーをパネリストに招き、国の重要インフラが攻撃された場合の脆弱性や起こりうる問題、また考えうる対策について論議を行った。

米国内においても、インフラのセキュリティの未整備は深刻な問題である。現時点では起こっていないだけで様々な攻撃が想定されている。もちろんそれに対しての対策は行っているが、それが十分機能するものかどうかについては議論が分かれるところである。

個人の情報管理という面においては、法整備が遅れている。特に個人情報詐取を規制するための法制度は未整備。そのための国家的プロジェクト（Project WHO）もある。

また、ここでもユーザに対しての教育の問題については語られていた。

また法執行機関（Law Enforcement）インターネット犯罪に対する法規制の整備は行うものの、インターネットやセキュリティ技術にいては理解不足の面がある。その部分を補うための連携を民間の祖引きと取っていく必要がある。

（参考資料：ProjectWHO_Kenneally.pdf）

第 2 日目（2007 年 5 月 31 日）

1. LA eCrime Stoey

Los Angels の FBI 捜査官によるフィッシング 検挙（捜査）の実例紹介

FBI へのフィッシング詐欺の報告は 2005 年で 18,000 件/月という実績があり、現在の数値は更に増大している。

実例紹介では同一の盗難カードを二人の女性が使って検挙されたものを紹介。電話を盗聴しておりフィッシャー（Jeffery Brett Goodin）が詐欺カードをその女性に販売するやりとりが聞けた。

個人情報のやり取りの部分は「ピー音」で消されていたが、臨場感のあるやりとり。

フィッシャーの傾向とまでは行かないが、このフィッシャーが準備段階から実行段階におけるまでどのように作業してきたかの説明なども行われた。

2. Nation Report:USA：Challenges of coordinating and conducting incident response on a national level

Speaker:US-CERT

US-CERT における業務紹介。やっていることは基本的に JPCERT/CC と同様と思われる。

2006 は 23,978 件のインシデントレポートがあったが 2007 年は現時点で既に 23,000 件を超えている。2006Q3 から急激に増えているのはボットの増加が関係している。

US-CERT では EINSTEIN Program を米国国土安全保障省の管轄下で行っている。これは国内のサイバーネットワークの監視と情報共有するためのシステム構築と運用を行うための取組み。

（参考資料：APWG_US-CERT_FINAL_MarkHenderson.pdf）

3. Better Collaboration Tools for Fighting Fraud

Speaker: John Frike CSO of FSTC、Jason Rafail CERT/CC、Romulo Dantas Organization of American States（米州機構）、

フィッシング体策に向けて協調していろいろな提言をしていこうというパネル CERT/CC 関連の方が主にプレゼンテーションを行った。

米国はフィッシング詐欺のような犯罪においては、日本同様さまざまな組織が関連してしまうこともあり、ソリューションの提言についてもまとめていくのが難しい。

（参考資料：BetterCollaborationToolsforFightingFraudv3Fricke.pdf）

4. APWG Electronic Crime Database Reporting Update

Speaker: Pat Cain APWG Resident Research Fellow

APWG のサーバで収集しているフィッシングメールのデータベースについて、その説明と今後の改良予定。現在毎 5 分ごとにフィッシングの URL リストのデータベースが刷新されている。

今後はユーザインターフェース、バックエンドシステム含めて改良は行いたいが、時期は未定。クライアントにエージェントをばら撒いて自動でフィッシングメールやフィッシングサイトの報告が行えるようなツールについても考えている。

5. Toward a World Health Organization Model for Managing eCrime Network Events

Speaker: Paul Ferguson(CTO, TrendMicro)、Richard Perlotto（Shadow Server）、Mark Henderson（US CERT）、Nick Bilogorskiy（Sonicwall）、Joe St Sauver（University of Oregon）、Minaxi Gupta（Indiana University）

これは対ボットに向けた RoundTable ディスカッションである。

ネットワーク上を流れるボットのパケットは米国においても深刻な問題となっている。国とセキュリティベンダーが協力してその対処に取り組んでいるが、効果的なソリューションはまだ存在していない。そういった背景があるためか、セッションの中では「このような問題点がある」という議論のほうが積極的に行われていた。

しかしボット撲滅へ向けたアプローチについては、Step1[責任の所在]→Step2[相関関係]を明確にさせることが必要である。

ボットの実態について「もっとユーザ向けの啓発を」という意見もあったがフィッシングやマルウェアに比べてその実態の理解がしづらい。どこまで効果が上がるかなど、疑問視する声も上がっていた。

6. DNS Security

Speaker: Paul Vixie、 John Frickle (Chief of Staff FSTC)

APWG が分科会を作って取り組んでいるテーマである。非常に長い間議論が行われている。DNSSEC（DNS Security Extentions）（http://www.dnssec-deployment.org/）の考え方を中心にディスカッションが行われた。しかしながら、DNSSEC 自体も既にその考え方が始まってから 5 年以上経過しているため議論されている情報そのものも最新のものではなかった。

プレゼンテーションの内容としては金融業界にとっての DNSSEC の必要性が中心だった。DNSAttack や CachePoisoning などの攻撃に対しての DNSSEC がどのように有効であるかの説明が行われた。（参考資料：DNSSEC.pdf）

APWG Counter-eCrime Operation Summit 総括

従来からの情報のアップデートが中心であったが、フィッシング詐欺やそれにまつわる事象が米国内では引き続き問題視されていることに変わりは無い。しかしながら対策ソリューションという意味では革新的なものが現れていないために、問題点を注視する傾向にありその対策についての議論があまりなされていないことが残念であった。

しかし、参加人数も 200 人を超えており、その顔ぶれもベンダー、政府関係者、金融機関、その他民間企業等多岐にわたっており、講演と講演の合間のブレーク時に積極的な意見交換も為されていた。

今後はフィッシング対策協議会でも、発表枠を獲得し、日本の状況を伝えることによって、その存在感を示していけるよう考えていくべきである。

第 3 日目（2007 年 6 月 1 日）

マイクロソフト社とのミーティング

日時：2007年6月1日（金） 午前9時～10時
場所：米国サンフランシスコ マイクロソフト社にて

アジェンダ

1. フィッシング犯罪の最新動向
2. フィッシング対策に関するマイクロソフトの取り組み
   - ✧ 技術的対策（IE7）
   - ✧ 政府及び業界との連携
   - ✧ 消費者への教育啓発活動

3. 今後、日本におけるフィッシング対策との連携

意見交換内容

1. フィッシング犯罪の最新動向

（スライド資料に基づき説明（フィッシングに関する WW 及び US のデータを提供））

- URL 偽造による詐欺や迷惑行為から発展して、悪意のあるソフトと連動した挙動へ
- フィッシングサイトとマルウェアサイトとボットが連携して、個人情報、政府・企業の機密情報を盗む傾向
- フィッシング対策としては、SPAM（迷惑メール）対策が”1st line defense”として最も重要
- フィッシング対策の範囲としては PC メールのみならず、Instant Messaging（メッセンジャ）、VoIP、Smart Phone、ゲーム機等の経路を視野にいれる必要がある
- 米国では、迷惑メール対策として、Sender ID の普及が進んでいる。SPAM の増加率よりも Sender ID の導入による SPAM 削除率が上回る。

2. フィッシング対策に関するマイクロソフトの取り組み

- 技術的対策（IE7）
  - IE7では、日々相当数の online reporting を受け、human grading 作業を経て、real-time にフィッシングサイトをブロックしている（数値については非公開だが会議で提示）
  - False Positive についても、件数が減少し精度が上がっている。
  - 日本を含む非英語圏のフィッシングサイトのブロックに関しては、今後日本側関係機関等との協力体制も検討したい。
- 政府及び業界との連携
  - MS としては、米国のみならず世界中の法執行機関と緊密に連携(Digital Phishnet)

補足：Digital Phishnet は世界の法執行機関を対象に提供しているフィッシングに関するポータルサイト。登録制でリアルタイムに脅威の情報共有等を行う。アジアにおいても、今後連携を拡大する予定

- 競合を含め、50 社以上を超える企業・業界団体と緊密に連携(MOG)。内容はキャンペーンの実施、オンラインガイダンス、印刷物の作成・配布など。（米国ではボーイスカウト、家電量販店の Best Buy 等と連携）金融関連機関との連携が重要であるが、米国ではバンクオブ・アメリカ、e-Bay 等と連携
- 連携作業においては、政策的課題、ビジネスベストプラクティス、データの共有を総合的に推進する必要がある
- フィッシングを取り締まる場合に適応される法律は、通常通信詐欺、著作権、商標などである

- 消費者への教育啓発活動
  - 日本特有の現象として、「ワンクリック詐欺」について解説。米国においても、social engineering タイプの詐欺は横行しており今後、フィッシングの定義を超える詐欺の技術的対応が課題(IE 7 でどのように対応できるか)

ベリサイン社とのミーティング

日時:2007年6月1日(金) 午後 3 時～4 時
場所:マウンテンビュー ベリサイン社にて

Anti-Phishing Solutions Vision Statement と題して、ベリサイン社の位置づけるフィッシングの脅威とそのソリューションについて。まず説明があった。(前段でフィッシングのフレームワークに関する説明があるが、その点については既に機知の知識ということで、ミーティング時間の有効活用のため省略)

■ベリサインの取組みについて
フィッシングに対してのエンドユーザ側の理解は深まってきている。企業に向けての教育は行っており、その危険性や対策の必要性については理解されている。個人への教育はまだまだ十分とはいえない。企業が個人に対して教育を行っているのでそこへの情報提供といった形での取り組みは行っている。

■今後のフィッシングの動向について
ボットの脅威に関係してくる。世界規模なボットネットワークはフィッシングメールの配信にも利用されており、今後もこの傾向は変わらないだろう。APWG のレポートにもあるとおり、スパイウェアと組合わせた攻撃手法も数多く報告されており、フィッシング手法も多様化している。

■法整備について
銀行業界におけるガイドライン(二要素認証の推奨など)、その他法整備は進んでいる。また、個人向けのサービスとして米国には Fair Credit Reporting Act(FCRA)というクレジットの履歴を管理するような仕組みがある(米国ではクレジットのサマリーがない人はクレジットカードが新たに作れない)それを利用することにより、消費者は自分のカードが不正利用していないかを確認することができる。

■EV SSL について
今後 Mobile の世界にどう展開していくかが重要。

マイクロソフト社、ベリサイン社訪問に関する総括

マイクロソフト社としては、OS 供給ベンダーという枠組みにとらわれずにさまざま機関と連携して情報収集・提供に努めている。特にエンドユーザに向けた教育にも力を入れて取り組んでいる姿勢は、コ

ンシューマビジネスのインフラを効果的に活用しつつ行われており、自社の強みを生かした取組みを展開している。

同時に企業のトップに向けた「ハイレベルエデュケーション」も展開しており、全包囲網的な啓発活動が米国では行われている印象を受けた。また、その活動を各拠点でどのように展開しようとするかはこれからの議論になっているようで、それに関連して協議会とマイクロソフト社日本法人との連携も議論を深めていく必要がある。

ベリサイン社に関してはエンタープライズへ絶大なる存在感のあるセキュリティベンダーとして企業との協調関係を生かした取組みが目立つ。個人ユーザに対しての啓発を行うには、企業側がその必要性を認識しメッセージを出していくことで、初めてユーザの理解を促進させることができ、この考え方に基づく活動が実を結びつつある。

同時に今後のフィッシング詐欺の動向についても、ワールドワイドの顧客ネットワークを生かした情報収集と高い技術力により、現状への対策にとどまらず、将来を見据えた上でのソリューションの開発・提供を目指しているその姿勢は、今後のフィッシング対策協議会の活動においても提言をいただき、連携を深めていけるよう協力体制の構築についても考えていきたい。

以上