ANTIPHISHING JAPAN フィッシング対策協議会 ▶ NEWS LETTER

APWG CeCOS Ⅱ 特集（2）

APWG（Anti Phishing Working Group）主催「ネット犯罪対策運用サミット（CeCOS Ⅱ ：The second annual Counter-eCrime Operations Summit)」報告

１．はじめに

NEWS LETTER NO.1 に引き続き、米国 Anti Phishing Working Group(APWG)が主催し、東京で開催された「CeCOSⅡ：Counter eCrime Operation Summit」の第２日目（５月２７日）の内容について紹介します。当日の概観を示し、特に選択した２つの発表についてより詳しく「３．」及び「４．」にて報告します。

２．第２日目概要

第２日目の冒頭、APWG 事務局からの挨拶において、前日午後３時の NHK TV ニュースで放映された CeCOSⅡ第１日目の模様が披露された。

２．１「パネルディスカッション」セッション

第２日目の最初セッションは、技術、運用そして教育という３つの領域についてパネルディスカッションが行われた。モデレータ、パネリストは次の通り。

＜モデレータ＞
佐々木良一（東京電機大学工学部 教授）
＜パネリスト＞
Alexander Seger（欧州評議会 経済犯罪部 部長)、Bonnie Chun（HKDNR / HKIRC/香港)、星澤裕二（(株)セキュアブレイン)、片山昌徳（ビットキャッシュ(株))、Steve Sheng（カーネギーメロン大学)

技術面では、星澤裕二氏より、フィッシングのようなソーシャルエンジニアリングが絡む（すなわち人間の判断行動がからむ）犯罪対策には技術だけの対応では不足であり、教育と組合わせることが必要であることが示された。運用面では、Bonnie Chun 氏より、不正使用されたドメインを停止させるためには、法律による規制だけではなく法律以外での

サポートが必要であることが述べられ、その運用内容が紹介された。教育の議論では Steve Sheng 氏より、啓発の浸透には政府の援助が必要であり、産業界での教育、例えば社員教育を実施する等も重要であることが指摘された。最後に佐々木教授により推奨されるべき事項が次のようにまとめられた。

① 教育コンテンツのアーカイブ（蓄積）が有用である
② 国家間の協力あるいは国の枠を越えた市民同士の協力が不可欠である
③ 技術は常に良いものを目指し関係者が努力する必要がある

２．２「ネット犯罪対策の当局機関のオペレーション」セッション

(1) サイバー犯罪の効果的な国際捜査（Alexander Seger、欧州評議会／欧州）

Alexander Seger 氏は、欧州評議会の人権及び法務関連の事務局長として経済犯罪部門を率いており、サイバー犯罪の国際的プロジェクトと同様に、組織犯罪、マネーロンダリング、汚職他に対抗する技術協力プログラムの責任者である。本セッションでは、サイバー犯罪条約に批准している全世界の国々をサポートプロジェクトが紹介された。

(2) データシェアリングと国際協力における成功事例（Jason Milletary、CERT/アメリカ合衆国）

米国とルーマニアの捜査機関が協力し、フィッシング詐欺を行なっていた 38 人を起訴した事例からも、犯罪を未然に防ぐという観点でも、組織間の情報共有が重要であるといえる。フィッシング詐欺などの場合、サイトをホスティングしている業者、銀行・カード会社、捜査機関などが情報を共有して連携することで、被害を最小限に抑えることが可能になり、その後の犯罪捜査も迅速に行なえることが示された。

(3) お金の痕跡と運び屋～Of Money trails and Mules～（Yinon Glasner、RSA/アメリカ合衆国）

犯罪組織がフィッシング詐欺などによって不正に得た金銭を、マネーロンダリング（資金洗浄）して海外に送金する新たな手法として、一般人をリクルートして金銭の「運び屋」として利用する実態、一例として Mule Network と呼ばれる、ネット上で集めた運び屋のネットワークにより金銭を小分けにして海外に送金が行われていることが紹介された

(4) 京都府警ハイテク犯罪対策室の事例（小山 雅子、京都府警/日本）

京都府警が検挙したサイバー犯罪の事例として、ネットオークションの ID やパスワードを盗んで架空出品等を行った詐欺団を検挙した事例など 2 件のフィッシング詐欺事件が紹介された。さらに、Winny ネットワークを通じてウイルスを作成・配布していた男性を著作権法違反・名誉毀損で検挙した事例が紹介された。

２．３「現実のネット犯罪対策運用ポリシー」セッション

(1) 数千の Rockphish と.hk ドメインの登録抹消に成功したリアルケースの共有（Bonnie Chun、HKDNR / HKIRC/中国香港）

2007 年に何千もの.hk ドメインがフィッシングに悪用された時に、影響を最小限にするためにとった対策事例が紹介された。また、外部機関（CERT[1]、及びフィッシングやspamvertizing[2]ドメインの検証や特定を行うためのガイドライン策定を支援した法執行機関）からの支援の重要性が強調された。

(2) ccTLD レジストリから見たフィッシング対策（堀田 博文、日本レジストリサービス（JPRS）/日本）

レジストリがフィッシングに使われているドメイン名の削除要請にたいして取る対応が説明され、またレジストリがフィッシングの対策をとることの問題点も提示された。加えて、JP ドメイン名諮問委員会による次の勧告が紹介された。

(1) ドメイン名無効化の決定および提言を行なう権限を持った団体の設置に関し関係機関間で議論すること

(2) その団体の決定に従ったドメイン名の緊急無効化の正式なルールやプロセスを整備すること

(3) レスポンスハンドリング：ネット犯罪に対するレスポンスのための統一アーキテクチャの提案（Paul Ferguson、トレンドマイクロ/アメリカ合衆国）

レスポンスハンドリングの際 WHOIS[3]データベースのドメイン名に関する情報は信頼性が落ちているが、IP 割当てに関する情報は当該組織の責任者を探し出す信頼性の高い方法であることが紹介された。また、法執行機関と NGO（CERT など）が双方向コミュニケーションをとり連携する体制が提案された。

(4) マルウェア分析：自動化と監視（Chris Horsley、JPCERT/CC/日本）

マルウェア分析を自動化するアプローチが紹介された。隔離されたサンドボックス環境の中で検体を解析しようとすると、マルウェアは本来の動きを止めてしまうため、マルウェアから見てサンドボックスでは無い通常の環境に見せかけた仮想環境を構築し、システム・ログの中でマルウェアがどんな動きをするのかを細かく解析・対策する手法を実装した自動マルウェア分析システムが紹介された。

２．４「ネット犯罪とグローバルコミュニケーションのインフラストラクチャ」セッション

(1) ネット犯罪とグローバルコミュニケーションのインフラストラクチャ- ISP・LE のケーススタディ(高橋郁夫、IT 弁護士 及び小山覚、Telecom-ISAC_Japan/日本)

Winny 作成者検挙や原田ウイルス事件などを通じた裁判事例や、フィッシング等の対策

---

[1] コンピュータセキュリティに関する情報収集･提供やインターネット上の不正アクセス報告の受付などを行う非営利団体。

[2] Spam(スパム)と Advertising(広告)との造語で、e-mail 中のリンクからポルノサイト等に誘う手口

[3] IP アドレスやドメイン名の登録者などに関する情報をインターネットユーザが誰でも参照できるサービス

で議論される ISP での対策案と通信の秘密との関係などについて法律面から論じられた。

(2) ボットネット-感染の放置：頑丈でかつ暴走するボットネットの急増に対して不可欠かつ重要な変更（Randy Vaughn、ベイラー大学/アメリカ合衆国）

ボットネットは、数多くのインターネットの諸問題・障害の背後にある基盤的なメカニズムだといわれており、法執行機関やインターネットセキュリティのコミュニティでは、ボットネット問題を制御する努力を強化している。一方でボットネットは周辺環境、対応技術の変化といった状況に巧妙に対処し、勢力を拡大し続けている。このようなボットネットに対しては、ボットネット対策担当者のコミュニティで継続的にプロセスを改善することで対抗することが可能となる。本講演では、そうした変化を促進する必要があるリソースやプロシージャの特定の試みが紹介された。

２．５「ドメインネームシステムポリシーワーキンググループからの報告」セッション

(1) 国家的ドメイン管理（CDG：Country Domain Governance）プロジェクト：ccTLD[4]悪用に関する ccTLD オペレータポリシーの影響(上村 圭介、国際大学グローバル・コミュニケーション・センター/日本)

国際大学グローバル・コミュニケーション・センターが担当している Country Domain Governance (CDG) project という研究の内容が紹介された。このプロジェクトは実施の途中であるが、研究課題の例として、ccTLD が不正使用されやすい国との相関関係を調査、インターネットの世界で誰がどのような責任と役割を持つべきかの検討等について紹介が行われた。

(2) レジストラ、レジストリ、ユーザに関する進歩（Rod Rasmussen、Internet Identity/アメリカ合衆国）

.asia ドメインで試みようとしている、ドメイン無効化の迅速化計画が紹介された。この計画は、APWG が Takedown 対象と認定した.asia のフィッシングドメインに対しレジストリやISPにコンタクトし、2時間経過して当該ドメイン登録者より応答がないときには、レジストリへの要請により、保有者の了解が無くともドメインのサスペンドを行うことが出来るようにするというものである。

３．マルウェア分析：自動化と監視

Chris Horsley, JPCERT/CC

マルウェア分析のプロセスはソーセージ作りに似ているところがある。つまり、色々な材料をインプットして、混ぜ合わせて最後に結果としてのレポートを出力することになる。通常、その過程は自動的には行われず、ソフト・ベンダが人海戦術によりマルウェアの検体を入手し、解析して定義ファイルを作成しており、更新定義ファイルの配布までには早

[4] 国や地域ごとに割り当てられた最上位のドメイン。例えば「.jp」が日本を表すトップレベルドメインに相当する。

くても数時間から数日間かかっている。

更新定義ファイルが配布されるまでの間、脅威となるのがゼロデイアタックである。悪意のハッカーが未知の脆弱性の利用や、既知の脆弱性のパッチ配布までの時間を狙ってアタックを行うと大変な被害が発生する危険性が高い。自動分析システムを使うと、一つの検体を 5 分から 10 分という短時間で解析し、その結果を基に駆除ツール（あるいは更新定義ファイル）を生成することが可能になる。

しかし、最近の傾向として、隔離されたサンドボックス環境の中で検体を解析しようとすると動きを止めてしまうため、マルウェアから見てサンドボックスでは無い通常の環境に見せかけた仮想環境を構築し、システム・ログの中でマルウェアがどんな動きをするのかを細かく解析・対策するのが、最新の自動マルウェア分析システムである。

もちろん、すべての検体が自動分析のみで対応できるとは限らないので、実際には約半数のケースが手動で分析することになる。

また、この自動化システム構築・運用実現のためには、準備として、システムの目的範囲の明確化、システム設計とその十分な考察、使用ツールとインフラの検討、能動的解析等次のステップのための協力先との連携、等が必要である。

そして最終目的実現のための機能分析の検討として、マルウェアそのものへの理解・周知、アンチウイルスソフト以外の検出方法の理解と実践、インシデントからの復旧策の立案が必須であり、続く、トレンド分析手法の導入目的として、新しい手法の理解、マルウェア作成者の意図確認やプロファイルが前提となる。

次に、当該マルウェア解析システムの設計原則としては、緩い結びつきである疎結合アーキテクチャの発想、柔軟なデータストレージの導入、さまざまな入力に対応できる設計構造、確固たるセキュリティシステムがあげられる。

当然ながら、制限事項の考察も必要である。特定のマルウェア（世の中に蔓延する以前の状態で、特定の企業やアプリをターゲット）については、当然ながら小規模チームで対応しなければならずどうしても当該の小人数メンバー（少ない開発者）での取り組み内容が基本となる。次に、これもよくあることで、限られた時間内で低予算、たとえば数百万円程度の金額で、やり遂げねばならないため、チーム編成も重要な要素である。

当該マルウェア解析システムの構成コンポーネント（Tracking ステップ）については次の通りである。

①Collection（検体の収集）
②Storage（検体格納）
③Automatic analysis（自動解析）
④Feedback（中間レポート）
⑤Manual analysis（手動分析）
⑥Reporting（トラッキング結果報告）
⑦Monitoring（監視続行）

以上のように、トラッキングシステムを使って収集したデータをベースにして、いくつかの他の専門システムも共用しながら、オープンデータも利用してまとめて行く、つまり

データの組み合わせが大切である。

続いて、自動化の手法であるが、そのマルウェア解析のための手段として既存のものと新規のものをどのように組合せるかが課題である。もちろん、既存の解析ツールは、マルウェア作成者も手に入れることができるわけで、当然、それを意識した回避方法や潜伏策はマルウェアに織込み済みと考えたほうがよい。前述のように実際に、監視環境においたりすると動きを停止するマルウェアが報告されていることが、その証拠といえる。

最後に今後の課題として次の三つを挙げる。

①結果の可視化、分析結果のテキスト情報だけでなく、何が起きているのかをビジュアル化することが大切である。つまり、その事象がどんな種類のものなのかを一目で判断できるようなグラフ化の検討などがその例である。

②“面白い”検体を見つけること、これは、大量の砂の中から、ある特定のひとつの砂粒を見つけるようなもので大変な労力が必要な面がある。但し、この検体（砂粒）が猛威を振るわないうちに、確実にこれを捕捉した上で分析して対策することが重要である。

③マルウェア分析作業の効率化、これについては自動分析システム自身がまだまだ発展段階であり、これからかなり改善の余地があるものと思われる。ゼロデイアタックを見てもわかるように、この分析作業の効率化は被害を最小限に食い止めるためには最大のポイントであり、手動分析との併用を含めて今後の検討課題である。

４．データシェアリングと国際協力における成功事例

Jascon Milletary, CERT

Software Engineering Institute（CMU/SEI）はマルウェア（Malware）を分析するチームである。これまでに、特に金融機関を狙ったサイバー犯罪は様々な言語圏や経済圏が対象となっている。今後は、情報を地域、国家間で共有していくことにより犯罪を食い止めていく事が出来ると思う。

犯罪を食い止めるための対策には、特定サイトをオフラインにすること、ISP に対してそのサイトを停止させていく要求をすること、どういうツールを使ってマルウェアをどうやって突き止めてくのかといったものがあり、特定の個人やグループである犯人を突き止めていき将来の損出を食い止めて損出の軽減を図る必要がある。

また、グローバルな視点で見ていくことも大切だが、ドメスティックな視点で見ていくことも必要である。被害報告について最初に応答する組織は所轄の警察になるが、個々の警察署では対応するリソースがないという場合もある。また、個人の損失が小額の場合、警察は対応に対してあまり力を入れないという現状もある。更に、情報を共有することに抵抗を示す人もいるので、情報を共有することによりメリットもあるということを説得する必要がある。

場合によっては、法律や規制により情報を共有できるが、逆に混乱をもたらす場合もある。何か法的な阻害があるのであれば、どのようにして阻害を取り除く事が出来るかを検討する必要がある。

アメリカでの情報共有の成功事例として、CERT があり、金融機関と協力して何が起き

ているのかという情報を共有する会議を行っている。

その中で、CERT はマルウェアの動向情報を持っているので、被害を最小限に食い止めるためマルウェアに関する特定の情報を金融機関と共有している。それにより、銀行が自分たちでルールを作り、将来の顧客が感染する可能性があるマルウェアを見極められるようになり、事前に被害を食い止めることができている。

法律や言語の壁により、情報共有が阻害される可能性があるが、地域で協力することにより、やがて来る犯罪の対策ができる。

場合によっては、同じグループが攻撃している場合もあるため、情報共有が更に重要になってくる。情報共有のグループとして、アジアの地域については APCERT や APEC でのワーキンググループがある。また、情報共有については、欧州やアメリカ、ラテンアメリカの協力が進んでいる。

グローバルな協力として、特に重要なのは信用できる知識を共有することである（たとえば、メーリングリスト、カンファレンスなど)。

また、何の情報が共有できて、今後共有できるのかを明確にすることが重要である。たとえば、一般のトレンドに関する情報を共有していくこと（諸外国での解釈など）や業界、警察、対応者から構成されるアドホックグループを作ることにより、直面している問題を解決していくなど、グローバルで対応することにより、時差を活用して常に犯人を追いかける事が出来る。

グローバルでのコラボレーションによる成功事例では、APWG やメーリングリスト（技術情報の共有)、グローバル CSIRT のコミュニティがある。

結論として、コンピュータ犯罪に対応していくには色々な人や国の協力が必要で、そこに信頼できる関係を構築する必要がある（金融機関、警察、対応者など)。また、新しいスキル（運用上の専門性など)、具体的な機能別のワーキンググループを作ることによりコンピュータ犯罪を防止していき、国を越えて信頼の輪を増やすようにして欲しい。

５．（参考）CeCOSII のホームページ

次のホームページに CeCOSII に関するプログラムやスピーカ紹介などが掲載されていますので、ご参照ください。

http://www.antiphishing.org/events/2008_operationsSummit_jp.html