フィッシング対策協議会

2013 年 7 月 16 日

The Counter eCrime Operations Summit VII

出張報告書

執筆：トレンドマイクロ株式会社

フォワードルッキングスレットリサーチ

林　憲明

目次

はじめに

Anti-Phishing Working Group (以下 APWG)は、2013 年 4 月 23 日から 25 日の 3 日間、7 回目を迎える"The Counter eCrime Operations Summit VII (以下 CeCOS VII)"と題する年次総会を開催しました。
今年は南米アルゼンチンの首都ブエノスアイレスに世界各地のサイバー犯罪対策の専門家 約 200 名が結集し、世界がサイバー犯罪に立ち向かうべき術について話し合いが行われました。

CeCOS VII 会場風景

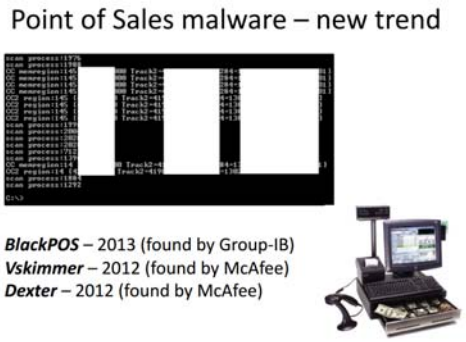
今回はスピーカーとして参加したこのカンファレンスについてレポートします。
今年はスペイン語圏での開催ということもあり、発表は英語とスペイン語の同時通訳で行われました。スピーカーはアルゼンチン、パラグアイ、ウルグアイ、ブラジル、アメリカ、ロシア、インドそして日本など色々な国から来ています。セッションは 2 つのパネルディスカッションを含む全部で 23 コマ、8 トラックに分かれていました。

参加者も地元アルゼンチンのみならず、欧米諸国からの参加者も多く見られました。また、日本からは 38 時間のフライトを要する地での開催でしたが、8 名が参加。この分野における関心の高さを知ることができました。
CeCOS では、警察・大学・産業界・法曹界などサイバー犯罪対策に関わる様々な分野の講演を聴くことができるのが特徴です。開会にあたって、APWG 事務局長の Peter Cassidy(ピーター・キャシディ氏)からも CeCOS が課題としているのは、コンピュータサイエンスやテクニカルではなく、「Management of Cyber Crime」であることを強調されていました。
Agenda は APWG のサイト[1]で確認することができます。私が特に注目したのは 2 つ。「ナショナルフィールドレポート」と「モバイル攻撃」セッションです。

1 http://apwg.org/apwg-events/cecos2013/agenda

National Field Reports

ナショナルフィールドレポートセッションは、各国の代表者によるサイバー犯罪の状況について報告が行われるセッションです。



ダン・クレメンツ氏 発表資料より抜粋

露：POS システムから情報を引き出す不正プログラム

セキュリティ企業、露 Group-IB[2]の Dan Clements（ダン・クレメンツ氏）が警告を鳴らしたのは POS System. 販売時点情報管理（Point Of Sale System）を狙った不正プログラムの増加傾向でした。

Group-IB の Dan Clements（ダン・クレメンツ氏）

彼はその脅威についてこれまでの変遷を示しながら発表しました。

Group-IB では過去 6 ヶ月間に 5 つの POS System を狙った不正プログラムを発見するに至っているとのことです。

このうち、「BlackPOS」(別名：TSPY_BANKER.HBE，Infostealer.Reedum)について詳細な発表がありました。彼らはその調査において、C&C（コマンド・アンド・コントロール）サーバの特定に成功し、解析を進めたそうです。

これにより、影響下にある組織を特定するに至ったとのことです。

BlackPOS は POS System 全体における一部分であるカードリーダーが接続された Windows ベースのコンピュータに感染します。そこでキャプチャした情報を FTP 経由でリモートサーバへアップロードすることにより、カード情報の収集を行っていたそうです。

濠：オンライン銀行を狙うカンガルー

引き続きダン氏が紹介したのは 2012 年以降に 15 万以上のマシンに対して感染を広げ、濠 / 独のオンライン銀行を標的とした「オンライン銀行詐欺

[2] http://www.group-ib.com/

ツール（Banking Trojan）」の「Kangoo（カンガルー）」と呼ばれる不正プログラムです。

Kangoo は元々ロシア圏で開発されたと言われている「Carberp」をオリジナルとする不正プログラムです。
Carberp のソースコードが流出[3]したことを受け作られた亜種の一つであると分析しているそうです。Kangoo という名前の由来は、C&C パネルのインターフェイスにカンガルーのロゴが使用されていたことを受け命名されたとのこと。その可愛らしいロゴとは裏腹に、多くのサイバー犯罪に荷担した不正プログラムであったといえます。

ブラジルにおけるハッカーコミュニティ

セキュリティ企業、ブラジル Apura Security[4] の Ronaldo Vasconcellos （ロナルド・バスコンセロス氏）が発表したのは、ブラジルにおけるホワイト/ブラックハットハッカーの現状でした。

Aqura Security の Ronaldo Vasconcellos （ロナルド･バスコンセロス氏）

ブラジルではホワイトハッカーによる文書化、情報の共有はまだ十分に進んでいないとのことです。そういった中ではありますが、「pr0j3kt m4yh3m br4z1l」によるソフトウェア Exploit の投稿を Full-disclosure / Bugtraq[5] / Exploits Database[6] などの国際的なコミュニティで確認することができ、こうした輪は今後更に広がりつつあるそうです。
南米地域のサイバー犯罪内容については類似性が見られるそうです。このため、南米の国同士での情報交換は有効な対策となることは多くのひとが感じていることですが、このとき問題となるのは、言語です。南米の言語圏はスペイン語とポルトガル語圏に分けることができます。 言語の壁は時には脅威の防御壁となることもありますが、対策の障壁となっていることを紹介していたのが印象的でした。
具体的な脅威として発表されていたのは、TAM 航空のマイレージサービスのポイントサービスを狙ったフィッシング詐欺でした。

3 http://threatpost.com/carberp-source-code-leaked
4 http://apura.com.br/
5 http://www.securityfocus.com/archive/1
6 http://www.exploit-db.com/

TAM 航空のマイレージサービス盗用を狙ったフィッシングサイト

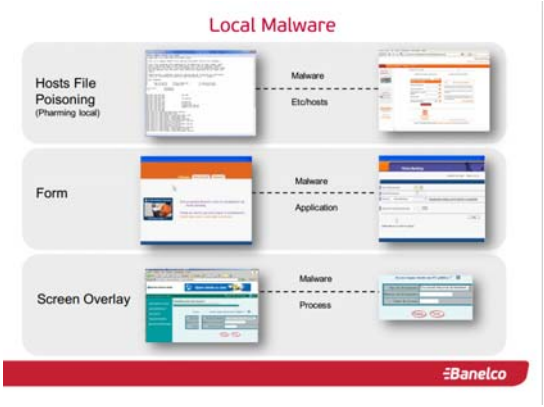
換金性の高いサービスを狙うという傾向はブラジルにおいても同様と言えそうです。
ブラジル国内における DDoS やサイト書き換えといったサイバー犯罪についてはハクティビズムやマネタイズといったものでは無く、ハッカー個人の知名度向上を目的とした攻撃も見られるそうです。
こうした現状を踏まえ、サイバー犯罪に取り組む意識を全体的に高めていく必要があるとのことです。また、そうした動きを後押しするように、サイバー犯罪やプライバシー保護に関する法律が相次いで成立しているとのことです。

アルゼンチンに見る脅威の Glocalization

アルゼンチンの ATM ネットワーク企業、Banelco[7] の Banelco CSIRT に所属する Lucas Coronel 氏と Lucas Paus 氏が発表したのは、アルゼンチン地域のみを標的とした地域限定の脅威「スクリーンオーバーレイマルウェア（Screen Overlay Malware）」と呼ばれるオンライン銀行を狙った不正プログラムでした。

Banelco CSIRT の *Lucas Coronel* 氏

アルゼンチン国内でのオンライン銀行詐欺ツールは、HOSTS ファイルの改ざん、フォーム注入、そしてスクリーンオーバーレイという攻撃の進化を辿っていったそうです。



Lucas Coronel 氏 発表資料より抜粋

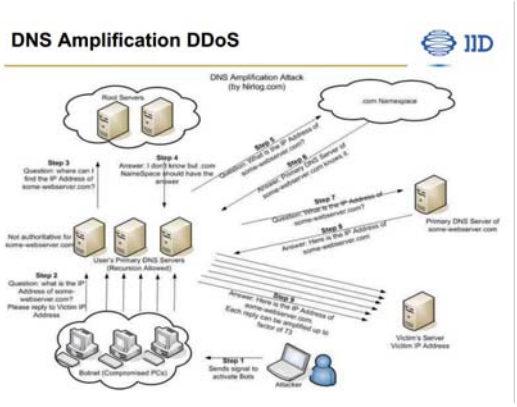
スクリーンオーバーレイマルウェアの詳細は二要素認証の乱数表を入力する画面を表示し、それらの情報を盗むという手口で有り、日本でも話題となった、HTML Inject、偽ポップアップの手口そのものでした。
脅威のグローカル（Globalization + Localization）化を感じさせる報告でした。

[7] http://www.banelco.com/

欧州：オープンリゾルバによる DNS リフレクション攻撃

セキュリティ企業、Internet Identity の Paul Ferguson （ポール・ファーガソン氏）が発表したのは、オープンリゾルバを介した DNS リフレクション攻撃に関する問題でした。

ポール氏は 2013 年 3 月に確認されたスパム対策組織 SpamHaus に対する大規模な DDoS 攻撃の事例を取り上げました。



ポール・ファーガソン氏 発表資料より抜粋

元々はSpamHausとその対応に反抗するISPとの小競り合いでしたが、インターネット全体の速度低下を引き起こすまでに大きく発展しました。その背景には、適切な対策が施されていないオープンリゾルバが数多く存在し、それらが踏み台となってDNSリフレクション攻撃を成立させたことに原因があるとのことです。
第三者が加害者に荷担することを防ぐためには、まずは自身の管理する DNS サーバについて、「OPEN RESOLVER TEST」[8]を使ったチェックを実施すべきとその方法を紹介してくれました。
その上で、根本的な対策としては「なりすまし」を防ぐことにあるとのことです。
現在、その方法として期待されているのが「BCP 38」（RFC 2827）[9]です。DNS リフレクション攻撃に限らず、多くのなりすまし攻撃においてその効果が期待できることを説明してくれました。
また、BCP 38 の利用促進にあたっては、ISP による協力も不可欠であるとのことです。ともに学び、対策を施していく時期であるとのことでした。

日本：オンライン銀行詐欺ツールはモバイルへ

日本から筆者がフィッシング対策協議会の代表として発表[10]させていただきました。発表テーマは「Finding the Banking Trojan in Eastern Asia（極東地域におけるオンライン銀行詐欺ツールに関する所見）」です。

Trend Micro の 林 憲明氏

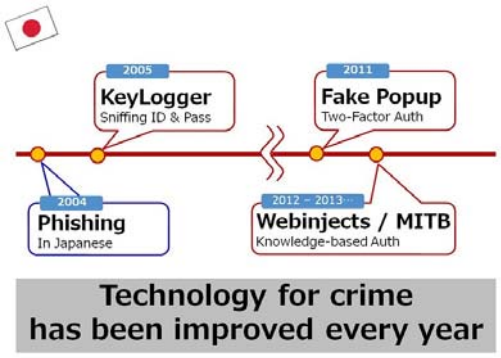
8 http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl

9 http://www.ietf.org/rfc/rfc2827.txt

10 http://blog.trendmicro.com/trendlabs-security-intelligence/finding-banking-trojans-in-eastern-asia-report-from-cecos-vii/

2004 年にはじめて日本語のフィッシングメールが確認されて以来、脅威は言語の壁を飛び越え、日本に続々と流入し、深刻な被害を与え続けています。

犯罪技術は年々進化し、その巧妙さも増しています。詐欺サイトへ誘導する手口のみならず、2013 年第 1 四半期にはマルウェアを組み合わせたオンライン銀行詐欺ツールの本格的な上陸が確認され、今後は国内での定番化が予想されます。



林　憲明氏 発表資料より抜粋

攻撃者の狙いは PC にとどまらずモバイルにも手を伸ばしています。その一例として昨年韓国のみで報告された「AndroidOS_CHEST」について紹介しました。

AndroidOS_CHEST の攻撃フロー

このマルウェアはスマートフォンをハイジャックします。これにより、攻撃者はすべてのテキストメッセージのモニタリングを行い、認証情報を通知するテキストメッセージのみを攻撃者に転送する攻撃手口がとられました。

これは、欧米の金融機関でも採用の進む二経路認証を攻略する攻撃手口として注目の事例でした。

こうした脅威から自己防衛するためのアドバイスをフィッシング対策協議会では「消費者向けフィッシング詐欺対策ガイドライン」[11]にまとめています。

林　憲明氏 発表資料より抜粋

このなかで特に重要なのが「パソコンを安全に保つ」ということです。
オンライン銀行詐欺ツールのほとんどは Exploit Kit によるドライブバイダウンロード攻撃によって拡散しています。この攻撃の連鎖を断ち切るには、コンピュータの脆弱性を排除することが重要です。
IPA：情報処理推進機構ではクライアントアプリケーションの脆弱性対策として「MyJVN バージョン

11 https://www.antiphishing.jp/report/guideline/consumer_guideline.html

チェッカ」[12]が無償公開されています。
このほか、パスワードの管理も重要です。あふれるパスワードをすべて記憶することは困難です。ソフトウェア[13]やガジェット[14]の力を借りることも有効といえます。

モバイル攻撃

続いて紹介するセッションは、APWG のワーキンググループによる成果発表です。今年度はモバイル WG よりブラックマーケットに関する動向が発表されました。この内容を中心に紹介します。

モバイルにも広がる闇市場

Edgardo Montes de Oca（エドガード・モンテ・デ・オカ氏）と Jart Armin（ジャート・アーミン氏）がモバイルによる金融詐欺と闇市場（アンダーグラウンドマーケット）の動向について報告しました。

その発表において強調されたのは、すでにモバイルマルウェアに関する市場が形成されているということでした。この実態を把握するうえで、どのような隠蔽工作が行われ、侵入やクライムウェアのサプライチェーンを形成しているのか明らかにする必要があると主張しています。

はじめに示されたのは、モバイルに対する合法的な侵入、国家による監視は日常的に行われているということでした[15]。

エドガード・モンテ・デ・オカ氏とジャート・アーミン氏 発表資料より抜粋

こうした国家レベルでの監視のみならず、犯罪者間の取引にも注目する必要があります。そうした取引の監視成果の一つとして示されたのが闇市場における価格表でした。

エドガード・モンテ・デ・オカ氏とジャート・アーミン氏 発表資料より抜粋

12 http://jvndb.jvn.jp/apis/myjvn/vccheck.html
13 http://safe.trendmicro.jp/products/pwmgr.aspx
14 http://safe.trendmicro.jp/products/pwmgr.aspx

15 著者注：元 CIA 職員のエドワード・スノーデン氏（29）が、2013 年 6 月、米国家安全保障局（NSA）が大手インターネット関連企業や通信会社から利用者のデータを収集していると暴露しました。この発表が行われたのはそれ以前の 4 月 24 日の事です。

モバイルに特化したボットネットは 4,000～3 万ドルで取引が行われているそうです。こうしたボットネットは闇のインフラを構築するために使われています。例えば、特定国家に対する妨害トラフィックを発生させる目的で使用することも可能とのことです。また、そうした攻撃を請け負うビジネスも闇市場には存在していることが報告されました。

また、サイバー犯罪者が利用者を騙し、クライムウェアを感染させる手口について紹介が行われました。

エドガード・モンテ・デ・オカ氏とジャート・アーミン氏 発表資料より抜粋

手口	事例
標的に偽アプリをインストールさせる	Opera Mini / ロシア SNS(vk.com)の偽アプリ / Skype
サブスクリプション型サービスに偽装しマルウェアをインストール	ZipWap.ru / Load-Wap.com / StimulPremium.com
携帯端末のテキストメッセージを悪用したフィッシング（スミッシング）	迷惑メッセージ：Skype / ICQ / SMS ツール：SMS Stealer/Authentication Tokens
バレットプルーフホスティング（防弾ホスティング）	犯罪者は犯罪を助長するバーチャルホスティングサービスを利用している。こうしたプロバイダーは法執行機関などによる捜査に対して非協力的で情報を出すことがない。

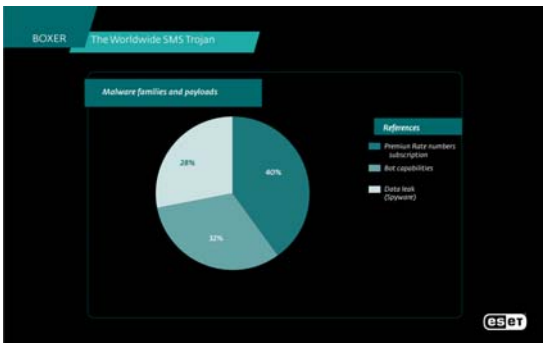
高収益な国を求め続けたモバイルマルウェア BOXER

セキュリティ企業、ESET の Andre Goujon （アンドレ・グージョン氏）と Pablo Ramos （パブロ・ラモス氏）が発表したのは、世界的に深刻な被害を与えている SMS トロイの木馬の一つである、BOXER に関する報告でした。

BOXER は欧米で利用されているプレミアム SMS サービス[16]を悪用することで対価を得ようとする不正アプリです。

SMS トロイの木馬に関する感染フロー
1. ユーザーが SMS トロイの木馬に感染
2. SMS トロイの木馬が密かにプレミアム番号を SMS 送信する
3. SMS の特別プロバイダーがユーザーに確認 SMS を送信
4. SMS トロイの木馬が確認 SMS をブロックし、ユーザーは悪さをされていることが分からないようになっている
5. ユーザーのお金が盗まれる
6. サイバー犯罪者がお金を確保する

こうしたプレミアム SMS を悪用するアプリは他にも多数存在します。確認されている不正アプリの約 40%がこのタイプに分類できるとのことです。



アンドレ・グージョン氏とパブロ・ラモス氏 発表資料より抜粋

これら SMS トロイの木馬の中で特に BOXER に注目する理由として影響下にある範囲の広さを主張しました。
プレミアム SMS サービスは、通信事業者や国によって実装方法が異なっています。このため、一般的な SMS トロイの木馬は影響下にある範囲が限定的であることがほとんどです。
これに対して、BOXER はアメリカ、ヨーロッパ、アフリカ、アジア、オセアニアなど、少なくとも 63 以上の国のユーザを対象とする能力を持っています。

アンドレ・グージョン氏とパブロ・ラモス氏 発表資料より抜粋

サイバー犯罪者が収益性の高い国を求め、脅威の範囲を世界に拡大し続けている可能性の一つとして BOXER は注目されます。

16 特定の番号宛てに SMS を送信することで、その返信としてコンテンツを提供し、コンテンツの利用料金は通話料金と一括で請求できる仕組み

脅威に対抗する手段

これまで見てきた脅威に対抗していくためにはどうすれば良いのでしょうか。その方向性を示したセッションを紹介します。

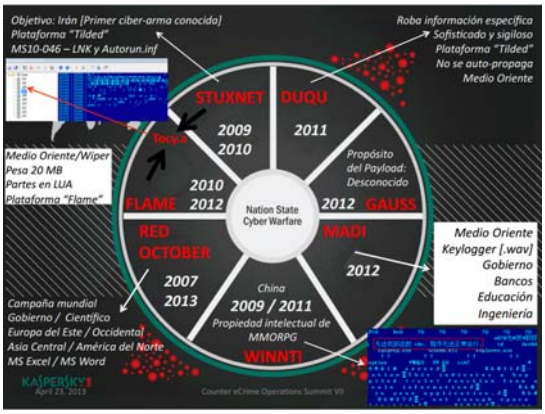
不正コード捜査にインテリジェンスを

セキュリティ企業、Kaspersky Lab[17] の Global Research and Analysis Team に所属する Jorge Mieres （ジョージ・マイヤーズ氏）が発表したのは、不正コード捜査にサイバーインテリジェンスを取り入れていこうという内容でした。

Kaspersky Lab の Jorge Mieres （ジョージ・マイヤーズ氏）

日本では「インテリジェンス」に関する定義すら曖昧と思われます。今回の発表は「諜報」と翻訳するのが適切かもしれません。

「Nation State Cyber Warfare」や「Cyber Espionage」とされる事件が 2007 年以降、相次いで報告されています。



ジョージ・マイヤーズ氏 発表資料より抜粋

こうした巨大な組織による犯罪に対抗していくための術となりうるものが「インテリジェンス」であると発表していました。

ジョージ氏はインテリジェンスに関する 3 つのプラットフォームを示してくれました。

ジョージ・マイヤーズ氏 発表資料より抜粋

公開情報を収集・分析することで知見を見いだす「**OSINT** (オシント：**O**pen **S**ource **INT**elligence)」、通信を収集・分析する「**COMINT** (コミント：**COM**munication **INT**elligence)」、そして人、ソーシャルエンジニアリングな観点から情報を収

17 http://www.securelist.com/en/blog/208194246/CeCOS_VII

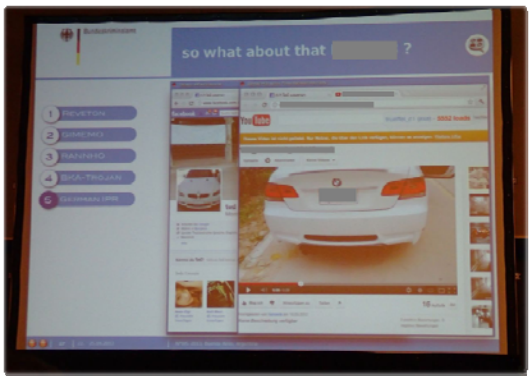
集・分析する「**HUMINT** (ヒューミット : **HUM**an **INT**elligence)」です。
こうした分析技法は暗黙知として既に取り入れているリサーチャーも数多く存在すると思われます。それを更に発展させるには、体系化が必要で有り技法の共有が必要と感じさせられました。

SNS でサイバー犯罪者のプロフィールを暴く

ドイツ連邦刑事局の Mirko Manske （ミルコ・マンスキー氏）が発表したのは、ランサムウェア（身代金要求型マルウェア、警察を装うものを特に Police Trojan[18]とも呼ばれている）を配布する犯人を facebook や Twitter などを使って追い詰めた事例を紹介してくれました。これは、OSINT の実践編です。

ドイツ連邦刑事局 の *Mirko Manske* （ミルコ・マンスキー氏）

刑事局では A という人物が容疑者であることを突き止めましたが、居場所の特定までには至りませんでした。そこで注目したのが A の妻が使っている facebook アカウントでした。このアカウントで「**公開されている情報**」、画像や動画サイトに投稿された動画などを調べる事で愛車を特定し、ナンバーを紹介することで容疑者 A のものに間違いないことを特定したそうです。



ミルコ・マンスキー氏 発表資料より抜粋（発表資料の一部分について筆者にてマスク処理を施しています）

居場所の特定にあたっては、facebook に投稿された写真が使われたそうです。写真に写りこんだ背景から、特徴的な箇所を抽出し、それを元に Google Earth で居場所がバンコク近郊であることを突き止めたそうです。
しかし、実際の検挙においては居場所の特定はスタート台にたったにすぎないとのことでした。
国際的な犯罪の場合、各国の警察組織との連携が必要となります。2～3 年前と比較すると状況はかなり改善しているそうですが、それでも数々の障壁が存在しているとのことです。
今回のケースでは、容疑者のビザ有効期間が切れていたため、ドイツのみに渡航可能な特殊な派スポとを発行することでドイツに連れ戻す取り組みが行われたそうです。

18 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-police-ransomware-update.pdf

犯罪者天国になっている onion ドメイン

アルゼンチン ブエノスアイレス警察の Ezequiel Sallis （エゼキエル・サリス氏）が発表したのは、Tor ネットワーク上で違法サイトを運営しているサイバー犯罪者を追い詰めた際の事例を紹介してくれました。

ブエノスアイレス警察 の *Ezequiel Sallis* （エゼキエル・サリス氏）

TorではHidden Service(秘匿サービス) という機能を使うことで、身元を明かさずに各種のサーバ（Web サーバ、メールサーバ、IRC サーバなど）を運用することが可能です。このとき「.onion」ドメインという特殊なドメインを割り当てて IP アドレスを結びつけることなく、Tor を実行させているノード同士が接続することができます。

エゼキエル・サリス氏 発表資料より抜粋

この onion ドメインの Web サイトには、児童ポルノ、薬物の密売、銃器売買、詐欺師、殺し屋、サイバー犯罪者などの違法サイトが多数存在しているそうです。しかし、これら Web サイトは匿名性が確保されている Tor ネットワーク上で運営されているため、サーバの IP アドレスなどを特定することが困難であり、実態の解明は簡単にはいかないようです。

エゼキエル・サリス氏 発表資料より抜粋

こうした違法サービスの通貨として使われているのは「Bitcoin」です。Bitcoin は銀行や政府が発行する通貨ではありません。匿名で使えるデジタル通貨のため追跡不能と言われています。こうした通貨を使った取引実態もまた、onion ドメインが犯罪者天国となっている一因といえそうです。

エゼキエル・サリス氏 発表資料より抜粋

こうした匿名づくしの犯罪者天国「Onionland」においても有効な捜査手法が OSINT でした。

onion ドメインの直接的な検索ができなくとも、通常のインターネット上に露出している情報、特にリンクをたどり得られる連絡先のメールアドレスなどは犯罪者に近づく有効な情報の一つとなるそうです。

また、onion ドメイン上の「メタデータ」には犯罪者特定につながるいくつかの痕跡が見られるそうです。例えば画像の EXIF データなどをあげていました。

また、捜査機関におけるより積極的な取り組みとして、自らが Tor のエンドポイントとなり、その出口で監視することで有効な情報を探す取り組みも行われているそうです。

エゼキエル・サリス氏は、Tor を一つの事例として取り上げていましたが、Tor に限らず、すべての国において、サイバー犯罪の新しい技術に関連する法整備は追いついていないことを指摘しました。

また、条約や協定など法執行機関による様々なサイバー犯罪捜査に関する提携契約があるが、これらが必ずしも現在のニーズを満たすのに十分ではないとのことです。

統括

CeCOS VII の統括として 2 つのキーワードを紹介します。「Glocalization」と「OSINT」です。

Glocalization とは、グローバリゼーション(地球一体化)とローカリゼーション(地域化)からの造語です。一見すると地域限定と思われるような事象であったとしても、さまざまな形でそれは文化として広がりを見せることがあります。

そこに事象の良悪は問われません。インターネットの世界はやはりどこかでつながりがあり、普遍化が進んでいるということを考えさせられました。

日本国内においては、昨年からオンライン銀行詐欺ツールの問題が大きく取り上げられています。

幸いなことにまだモバイルまでその問題は波及していません。しかし、世界の状況から推測すると近いうちにこの波がおそってくる可能性を考慮する必要があるのかもしれません。これもまた、Glocalization の一つと言えるかもしれません。

こうした Glocalization の波に対して、単一民族である我々日本人は「言語の壁」とどのように向き合っていくべきなのか考えさせられました。

言語は時には脅威に対する防御壁となりますが、一方でコミュニケーションにおける障壁ともなり得ます。

隣国で発生したサイバー攻撃、そしてそこから得られた知見について、必ずしも国内で生かすような取り組みが行われているとは言えません。

こうした地域特有の脅威情報を収集するための「場」は今後も重要性を増すものと考えられます。

今回、複数のスピーカーがサイバーインテリジェンス、特に「OSINT (オシント：Open Source INTelligence)」の重要性について訴えていました。

好む好まざるに関わらず、ソーシャルネットワークサービスは世界中で流行しています。

この流行は捜査関係者に対し、強力なツールを提供することになったようです。

それと同時にセキュリティやプライバシーにかかわる新たな問題も表面化していることを忘れてはならないといえます。

最後に、APWG CeCOS の次年度開催予定地はアジアとのことです。サイバー犯罪に対しては地球規模で考え、活動していく必要があると言えます。しかし、国内に留まってはうかがい知ることのできない情報もあります。是非次年度もサイバー犯罪対策に関わる多くの方に参加いただき、情報交換の機会を活用していただきたいです。