AntiPhishing Working Gourp General Members Meeting & eCrime Researchers Summit 出張報告書

株式会社セキュアブレイン

中田 太

2010/12/03

会議の概要

「General Members Meeting & eCrime Researchers Summit」は年に一度、米国内で開催される。APWG のメンバーに参加資格があり、以下の様なプログラムから構成される。

1. APWG 活動報告
2. 各 Region からのトピック報告（今回は日本と中国）
3. APWG 内の各 WG の活動成果の報告
4. 論文の募集とその発表

今回日本からは JPCERT/CC 小宮山様、日立情報システムズ 丹京様、フィッシング対策協議会から中田が参加した。

セッションは 2 日半にわたって開催され、約 30 のセッションが行われた。「フィッシング詐欺」が組織的、かつ国際的な犯罪となってからは、その対策の傾向として「セキュリティシステム」で防ぐのではなく「法律」「教育」「機関連携」「啓発」等の「社会的仕組み」の中で防いでいくという考え方の傾向があり、その方向性は変わっていない。しかし、年々その機運はAPWGのメンバーの中でも高まりを見せており、対策する側も「組織的」「国際連携」の動きを見せており、なおかつ一定の効果をあげている。

今回は日本からの発表の枠もあり、日本のフィッシング詐欺の状況と事例として「警視庁」と「CarView 様」の事例を紹介した。特に「CarView 様」の事例については、米国内でも同様の事例があることが分かり、今後の犯罪防止ついても情報交換を行える関係構築するという効果をあげることができた。

2 日半のセッションの参加では、セッション時間以外でも情報交換を行う機会も多数あり、非常に有意義な時間を過ごすことができた。本報告書では、全体の中で特筆すべきトピックについて報告する。

目次

オンライン犯罪の傾向 － 米国では 1 千億円以上の被害が。手法も多様化

ソーシャルエンジニアリング手法、技術、両面で進歩している。また、「Mule（運び屋）」の存在が欧米における、オンライン犯罪において重要な役割を果たしている。

欧米においてはオンラインバンキングを狙った攻撃が依然として根強い。
特に米国では、インターネットバンキングでは、フィッシング詐欺により$1Billion 以上の金額が失われている。

「Man in the Middle、Man in the Browser」等、比較的高度な技術を使った手法が流行

金融系のオンライン犯罪では「Man in the Middle」「Man in Browser」「ScreenScrapping」「Key Logger」等、以前流行、または紹介された攻撃手法が流行っている。

特に「Man in the Middle」「Man in Browser」は実際に大量の被害が出ている。

PayPal の取り組み

フィッシャー（フィッシング詐欺を行っている犯罪者）追跡の為の PayPal の取り組み

フィッシング詐欺の一連の流れ「フィッシングキットの活用→フィッシングサイトの構築→個人情報の収集」の中で、利用される電子メール・IP アドレス・ドメイン名・クレジットカード番号等の、いわゆる不審な情報の保有者を追跡している。

例：不審なクレジットカードの番号を追跡して、相関図の作成を行うと、フィッシャーのアカウントは「孤立」している事が見えてくる。（実際の相関図は紹介されなかった）

FSISAC の主な活動内容

金融インフラ保護を活動目的としている「FSISAC（Financial Services Information Sharing and Analysis Center）」はオンラインバンキング保護の為、下記の様な様々な施策を行っている。

1. BlackList の作成
2. オンラインバンキングのアカウント閉鎖（各銀行の担当者から形成されるタスクフォースで運営）
3. 防御・検知・対応それぞれのフェーズにおいて WorkingGroup が存在している。

※銀行は国際企業である場合が多い。しかしこれらの組織の動きは米国内に限定した動きである為、国際連携の問題が残っている。

携帯電話・スマートフォンとオンライン犯罪の脅威 － 犯罪プラットフォームの多様化

オンライン犯罪のプラットフォームとしての携帯電話・スマートフォンの台頭が著しい。非常に危険性が高まっている。

携帯電話に格納されているほとんどの情報は、盗まれる可能性があることが指摘されている。

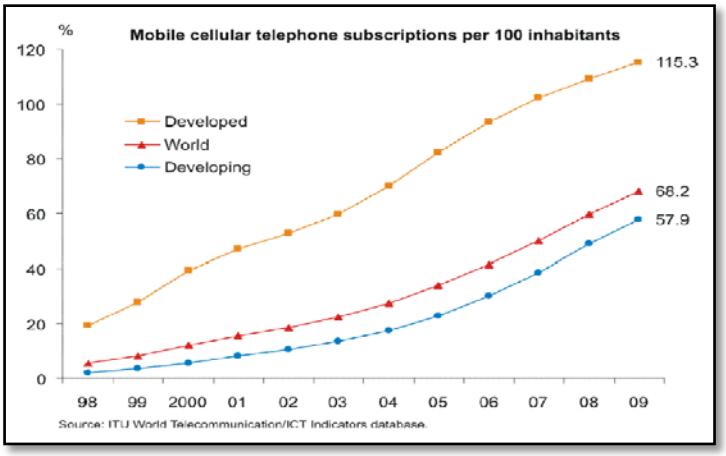
日本でも猛威をふるっている個人情報を盗むトロイの木馬「ZEUS」は、元々は PC 向けの不正プログラムだったが、最近では携帯電話への対応が行われていた。

今後、不正プログラムが携帯電話への対応が行われていくという見方がある。米国では、日本ほど携帯環境の整備が進んでいない。インフラの整備が進めば、それに応じて脅威が伝播する環境も整備される。

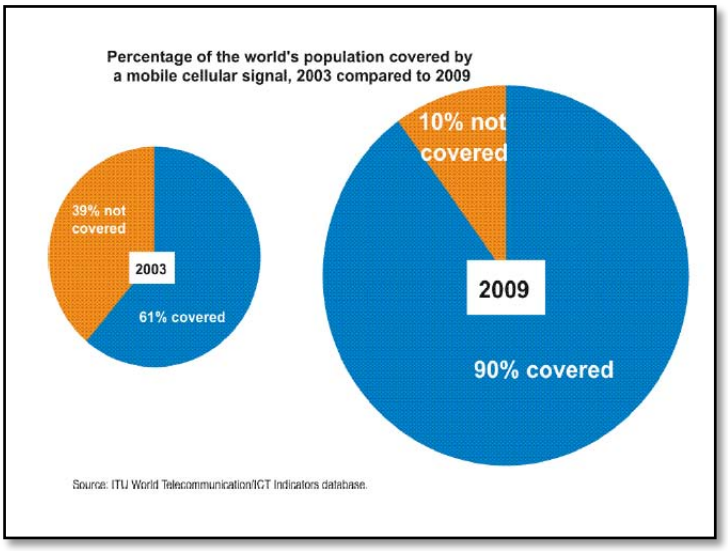
スマートフォンの急激な普及もあり、2-3 年以内に PC の脅威と携帯電話の脅威の数に逆転現象が発生するという予測もある。携帯電話。スマートフォン利用者は PC のユーザに比較するとセキュリティリテラシーが低い。その為。対策と同時にユーザへの教育も重要。

※米国内におけるオンラインの脅威の PC から携帯・スマートフォンへの移行が進めば、その脅威は当然ながら日本の携帯・スマートフォンユーザも対象としてくる。

【地域毎の携帯電話の普及率推移】



【世界人口における携帯電話保有率の推移】



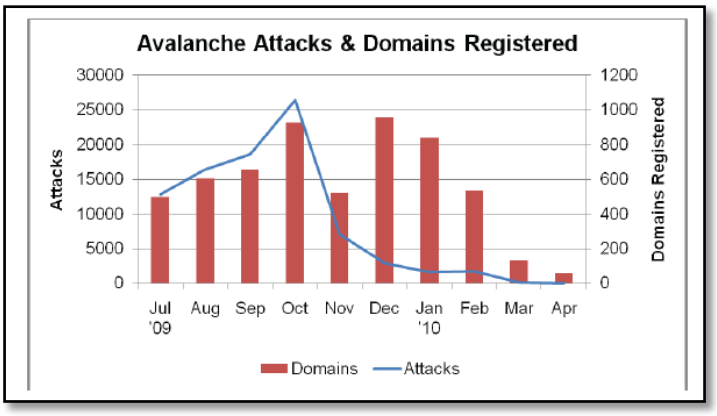
APWG vs 犯罪組織 －「Avalanche」の活動阻止に一定の効果

APWG の活動の一つとして、フィッシング詐欺を行う「犯罪組織」の活動を阻止するという取り組みがある。現在、世界的に有名な組織は「Avalanche（アバランチ）」。オンライン犯罪を行う組織の実態は正確には把握されていないが、全世界でおこなれているフィッシング詐欺の 80%は「Avalanche」によって行われていると言われている。

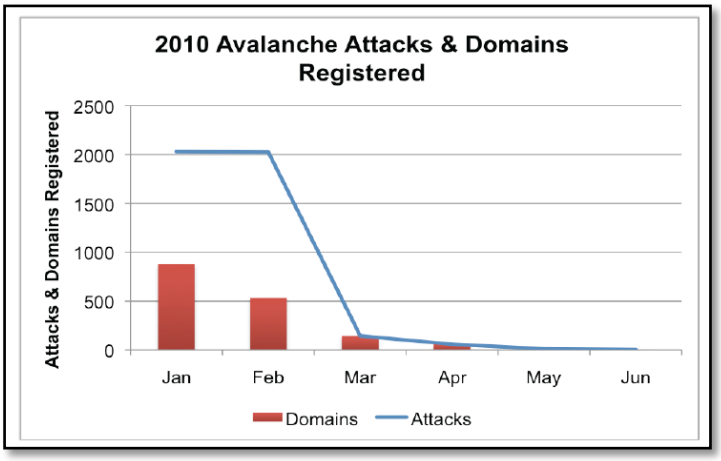
「Avalanche」の攻撃手法としては、「不正なドメインを取得後、そのドメインにフィッシングサイトを作成する」というものが代表的。APWG は、「Avalanche」が作成したドメインの「閉鎖」作業を各国の CERT や NIC と連携して行っている。2010 年に入ってから、「Avalanche」のドメイン登録が急激に減少している。

この活動では、APWG のような NPO 団体が、米国内だけでなく他国の CERT、捜査組織と連携して犯罪防止に対して一定の効果をあげている。組織的、かつ国際的なオンライン犯罪は今後増加の一途をたどることが予想される中、この活動は犯罪防止策の一つのモデルケースとなり得ると感じた。

【Avalanche 登録ドメインの推移-1】



【Avalanche 登録ドメインの推移-2】

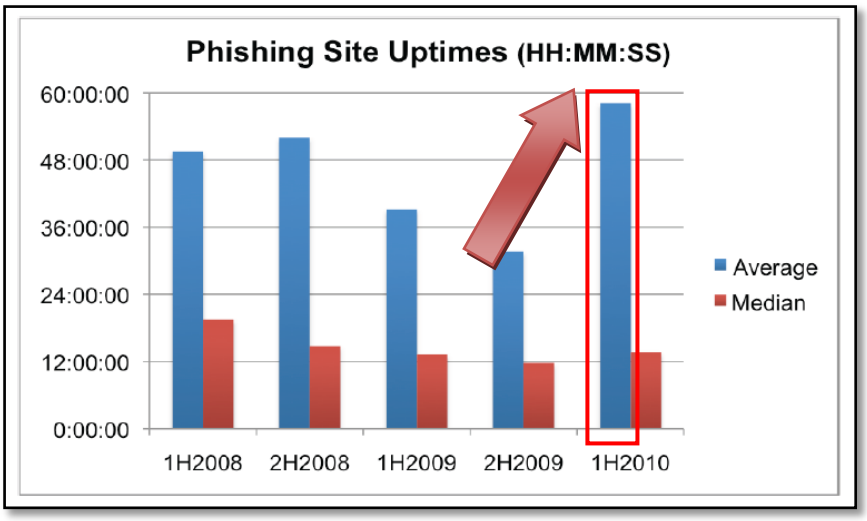


犯罪組織は別の手法を模索

「Avalanche」のドメイン登録は減少しているが、マルウェアを使用して一般のサーバに不正アクセスを行い、フィッシングサイトを設置するケースが急増している。APWG が調査した 28,646 個のフィッシングサイトのドメインの内、83%は一般のウェブサイトが不正に乗っ取られたものだった。

フィッシングサイトの残存時間について

2010 年に入ってフィッシングサイトの残存期間は伸びている。

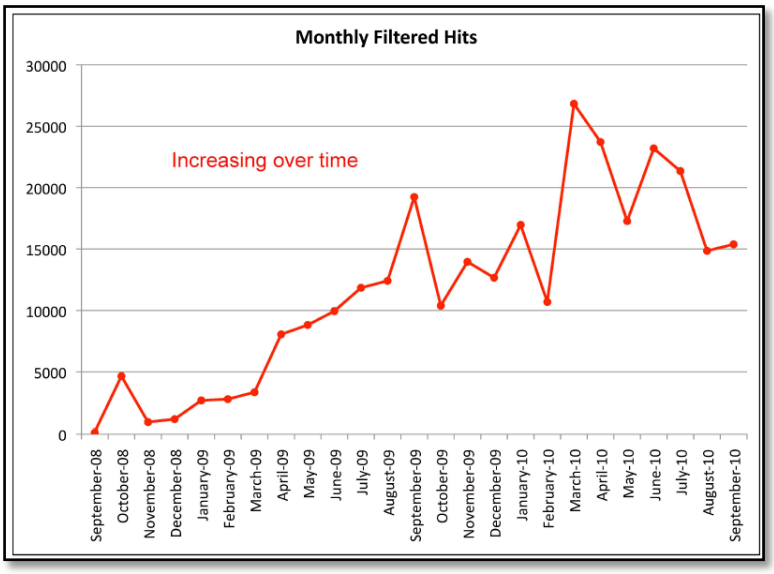


残存期間についても、「Avalanche」のドメインと「非 Avalanche」のドメインでは大きな違いがある。

	Average (HH:MM)	Median (HH:MM)
All Phish, All TLDs	58:10	13:42
Avalanche Phish Only	12:28	9:55
Non-Avalanche Phish	62:33	15:10

フィッシング対策を目的として e-Learning について

日本でもおなじみの「フィッシングフィル」。米国サイトの統計報告。2 年間（2008/9 月~2010/9 月）293,125 回利用されている。（2,379 の URL からアクセスされている）。利用頻度は上昇傾向。



日本の発表について – CarView 様の事例紹介。eBay でも同様の事例

「Japan Field Report and Case Study」と題して、以下の内容について、日立情報システムズ 丹京様と中田で発表を行った。

1. フィッシングメールと詐欺サイトについて、フィッシング対策協議会が発表している数値をベースに日本の状況を説明。
2. 全体的な数値としては月毎にばらつきがあり、定まった傾向は捉えずらいが、「偽装されるブランド」は以前より増加傾向にある。クレジットカードやオークションサイト等、従来からのものは引き続き存在しているが、CarView 様のケースの様に特殊な手法を取る事例が出てきた。
3. 警視庁が Winny ウイルスを悪用して詐欺を行ったグループ（2 名）を検挙した事例について紹介。
4. CarView 様の事例の紹介。CarView 様の事例においては、米国のオークションサイト「eBay」にて同様の事例が報告されている旨、出席者より情報提供があった。

中国の状況について － 犯罪の抑制に APAC（AntiPhishing Alliance of China）が活躍

日本の発表についで「AntiPhishing Alliance of China」より、中国のオンライン犯罪の状況について説明があった。

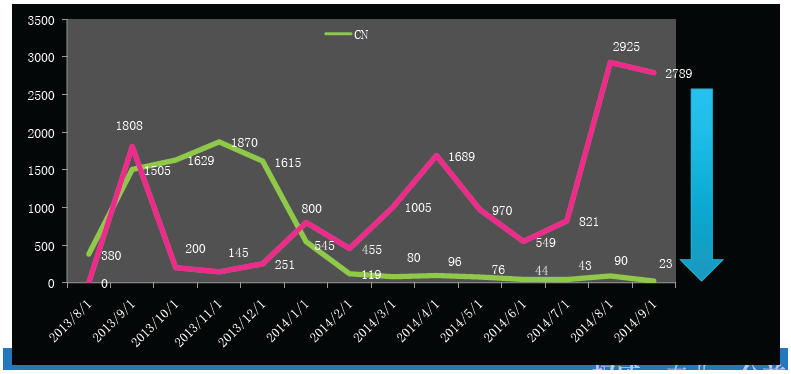
中国のフィッシング詐欺は EC サイトが主な攻撃対象となっている。中でも中国最大の EC サイト「TaoBao（淘宝網）」のフィッシングサイトは全体の 50%に上る。

北京オリンピックの際には、チケット販売サイトのフィッシングサイト、2008 年四川省、2010 年青海省の大地震では「義捐金サイト」を偽ったフィッシングサイトが出現した。

Official:www.tickets.beijing2008.cn

Phishing:www.beijing-tickets2008.com
Phishing:www.beijingticketing.com
More than 50 million USD.

インターネット黎明期の中国では、ドメインの登録状況も整備が進んでいない為、犯罪者が容易に「CN」ドメインを入手する状況が 2009 年まで続いていたが、2010 年に入ってから「CN」ドメインのフィッシングサイトは急激に減少している。



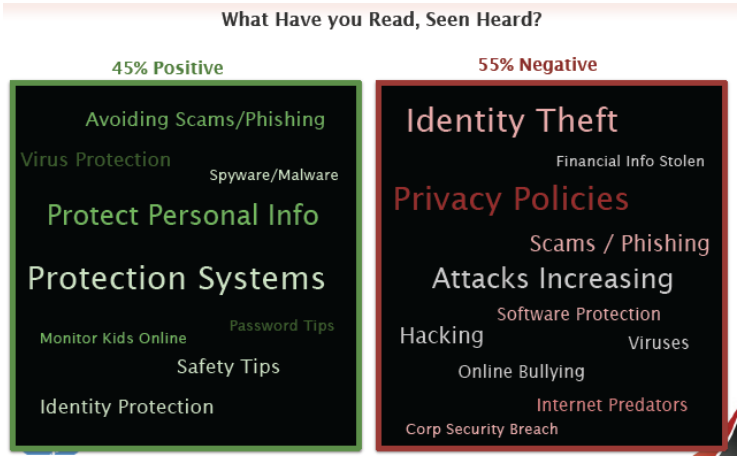
2008 年−2009 年の統計では「CN」ドメインが全体の 38%を占めていたが、2010 年では 4%まで減少した。

ユーザ意識調査の発表

- 調査の目的：インターネットの利用に際して、ユーザが感じている不安を分析（外部の調査会社を利用）
- 調査方法：インターネット調査
- 調査対象：無作為に抽出したインターネットユーザ（約 1,000 人）

「Security」という言葉に対しては 55%の人がネガティブなイメージを抱いている。

ポジティブに受け取られる言葉として、「Avoid（避ける・排除する）」「Protect（防ぐ）」という言葉に関連するキーワードが多く見受けられた。



自分自身が「『Safe』または『Secure』な状態にあるか」という設問に対して、比較的年齢の高い世代（50 代～60 代）においては、「自信を持てていない」側面が伺われる。逆に若い世代（10 代後半～30 代前半）においては、「十分に安全である」という意識が見られる。

「インターネットを利用する際に注意すべき事項」としては以下の様に日本と同様の傾向が見受けら

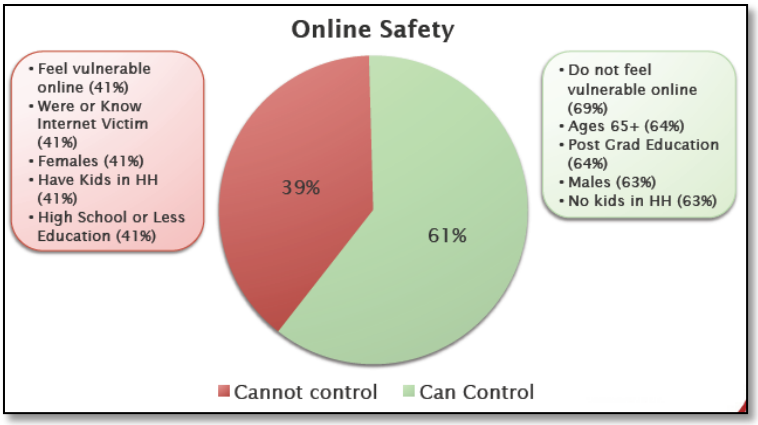
れた。

- 「クレジットカードの利用」
- 「パスワードの管理」
- 「アンチウイルスやセキュリティパッチの活用」
- 「電子メールの添付ファイルに対しての注意」
- 「個人情報の取り扱い」
- 「SNS 等の利用について」
- 「無線 LAN の活用について」

インターネットの安全管理について

自分自身の安全は「コントロール可能」と回答が全体の 61%。特に高齢者にこの傾向が強い。

逆に若い世代（高校生以下）においては「コントロールできない」という回答が 41%。自分自身のセキュリティの状態に対する「自信」の調査結果と逆の結果に繋がっている事が見受けられる。



新たな攻撃手法：「そのタブは本物？」Tabnabbing Attack

2010 年 5 月に発表された「ブラウザのタブ機能を悪用した」フィッシング詐欺の手法「Tabnabbing Attack」についての研究発表

「Tabnabbing Attack」の概要

1. タブブラウザ使用時に複数のタブを開く
2. 「Tabnabbing Attack」を行おうとしている「不正な Java スクリプト」が埋め込まれたページ（以下「Tabnabbign Attack」ページ）を別のタブで開く
3. 別のタブに遷移する
4. 「Tabanabbing Attack」ページが、自分のページが「アクティブではない」ことを検知すると、ページタイトルやコンテンツを変更する。
5. ユーザが「Tabnabbing Attack」ページに戻ると、フィッシング詐欺コンテンツが表示されている。


http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/
Tabnabbing: A New Type of ...
I'm Aza Raskin @azaaza. I make shiny things. I simplify.
Tabnabbing Attackを行おうとしているページ
http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/


http://jp.msn.com/
セキュアブレイントップページ
MSN Japan
Yahoo! JAPAN
Tabnabbing: A New Type of Phi...
別のページに遷移。「Tabnabbing Attack」のページが「非アクティブ」状態になると・・・


http://jp.msn.com/
セキュアブレイントップページ
MSN Japan
Yahoo! JAPAN
Gmail: Email from Google
ページのタイトル、アイコン、コンテンツを入れ替える！
Hotmail
Hotmailアカウントでサインインすると、新着メールをすぐに確認できて便利です。
2億8000万円でも完売間違いなし！12台限定のランボルギーニ

タブブラウザを利用するユーザは、複数のタブを開いてタブ間を遷移する。既に開いているタブの内容が変わっていても気付かない場合がある。「Tabnabbing Attack」ではこの点を悪用して「フィッシング詐欺」を行っている。

このスクリプトは複数のブラウザで動作することが確認されている。

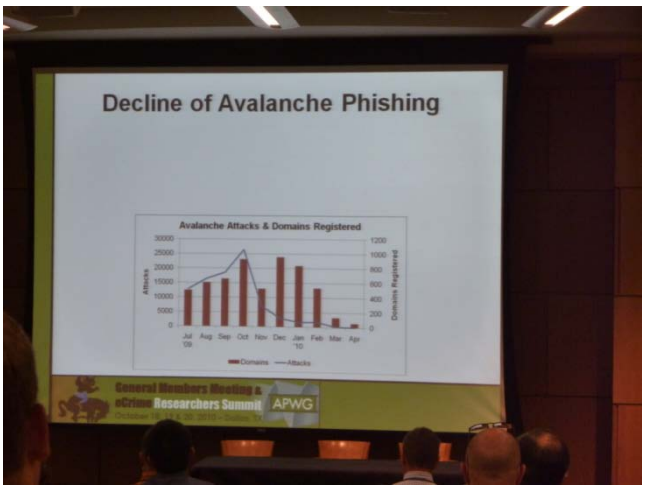
「Tabnabbing Attack」の対策について

1. パスワードマネージャの活用。（パスワードマネージャは URL を認識することで、その URL に見あった「ID」「パスワード」を自動入力する。）
2. ブラウザの「スクリプト」動作の禁止または制限する設定を行う。
3. ユーザ自身が URL のチェックを注意深くチェックする。

以上

【付録】会場の写真

会場全体図



APWG の Avalanche 対策の成果を示すグラフ

日立情報　丹京様の発表

会場前に設置されたバナー

パネルセッションの様子