

フィッシングの最新動向と対策技術について

株式会社セキュアブレイン

中田 太



SecureBrain

本日のアジェンダ

- ◆ 株式会社セキュアブレインのご紹介
- ◆ 海外のフィッシング動向 -APWGからの情報-
- ◆ 中国の状況
- ◆ 対策について



株式会社セキュアブレインのご紹介

◆ 株式会社セキュアブレイン

- ◆ 所在地: 〒102-0083 千代田区麹町2-6-7 麹町RKビル
- ◆ 設立: 2004年10月5日
- ◆ 資本金: 2億1,620万円
- ◆ 取引銀行: 三井住友銀行 日比谷支店、みずほ銀行 四谷支店、りそな銀行 虎ノ門支店、八十二銀行 東京営業部

より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する

“Security Specialist Team”



SecureBrain

当社の実績



“Security Specialist Team”



SecureBrain

AntiPhishing Working Group(APWG)

- ◆ 2003年設立 - www.apwg.org
- ◆ 1,800以上の企業スポンサー、3,500名以上のメンバーを抱える、世界最大のフィッシング対策NPO
 - ◆ 金融機関
 - ◆ ISP
 - ◆ EC
 - ◆ セキュリティベンダー
 - ◆ 政府機関
 - ◆ 捜査機関
- ◆ フィッシング詐欺のみに留まらず、関連するオンライン犯罪の手口、その対策手法についての研究、教育、政府機関との連携、啓発活動を全世界で行う
- ◆ 2回/年 カンファレンスを実施
 - ◆ 日本国内では2008年4月に開催



Dave Jevans



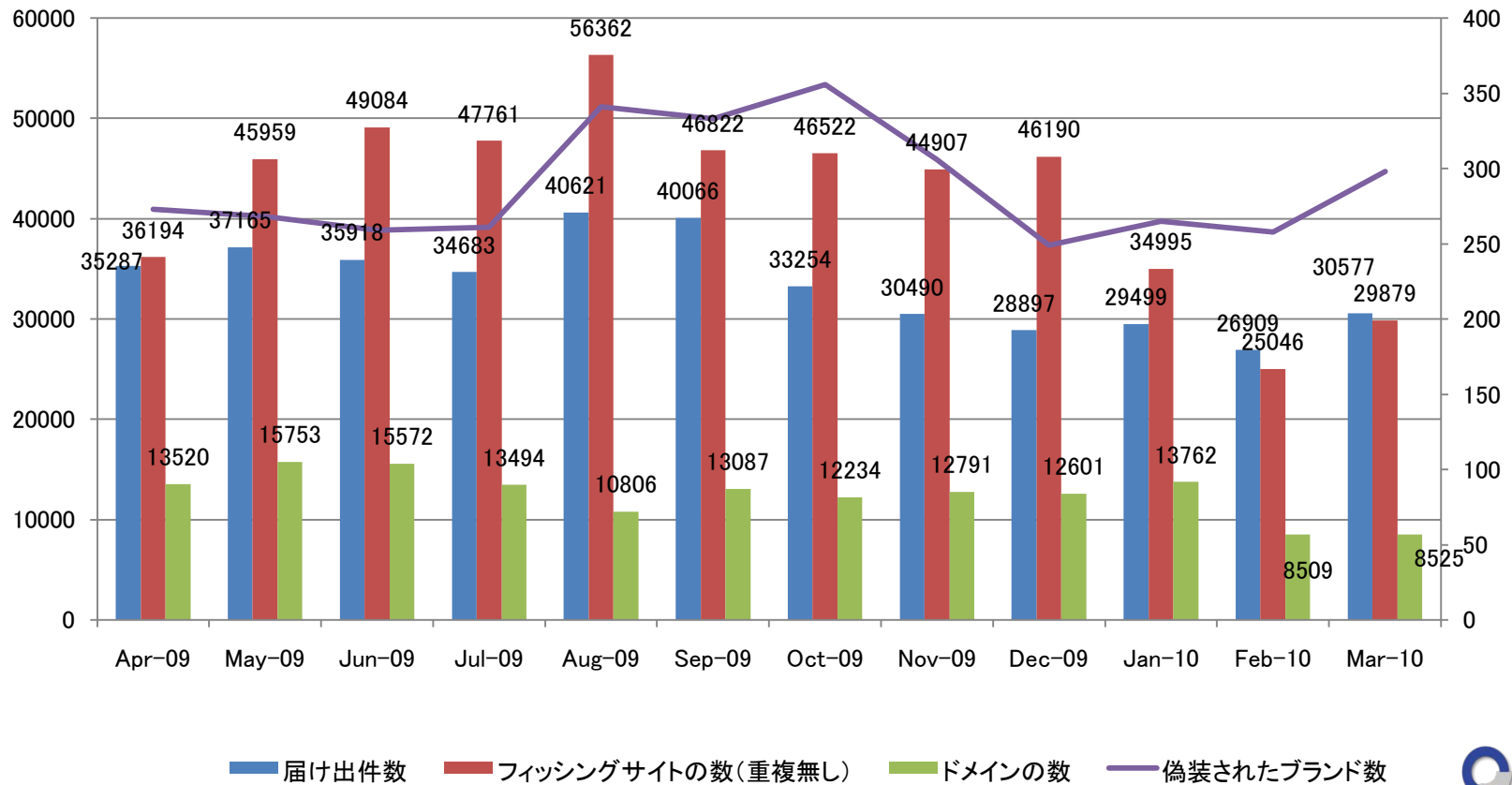
Peter Cassidy



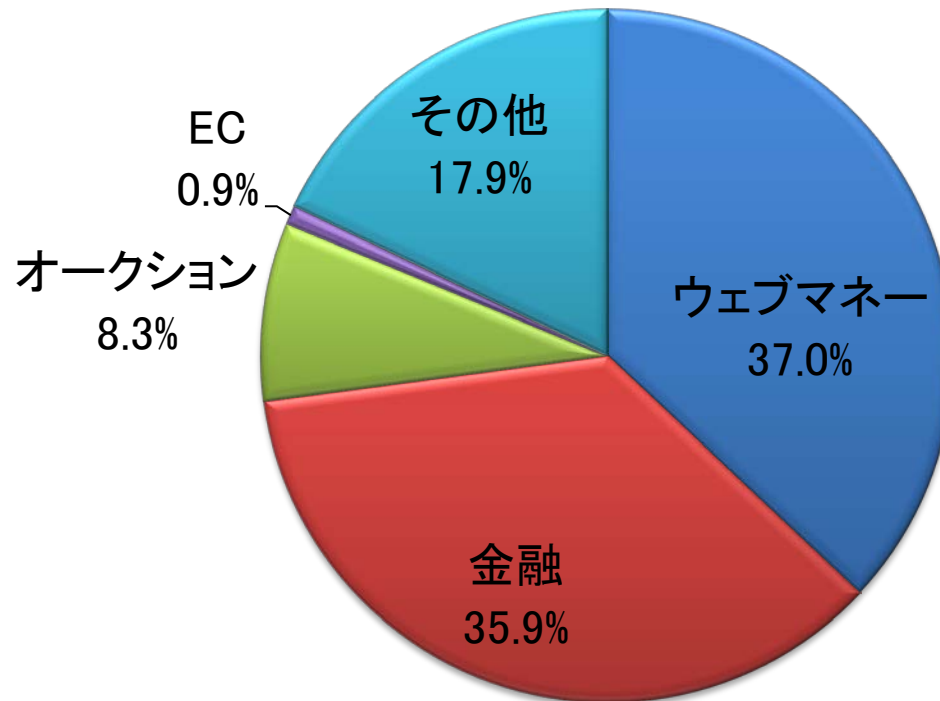
Foy Shiver



APWGフィッシング詐欺の届け出傾向



フィッシング詐欺の対象となった業種(2010/Q1)



その他にはSNSやオンラインゲームが含まれる(前期比37%増)



海外のフィッシング詐欺動向

- ◆ 依然として金融関連を狙ったフィッシング詐欺が主流
- ◆ インタネットバンキングではフィッシング詐欺により「\$1billion以上(1,000億円)」が被害に
- ◆ 「Mule(運び屋)」の存在
- ◆ SNSを狙った活動も活発になっている
- ◆ 日本に比べて多数のブランドが被害に遭っている
- ◆ フィッシングに利用されているドメインの数は、2010年に入ってから減少傾向にある



Multi-function Financial Crimware



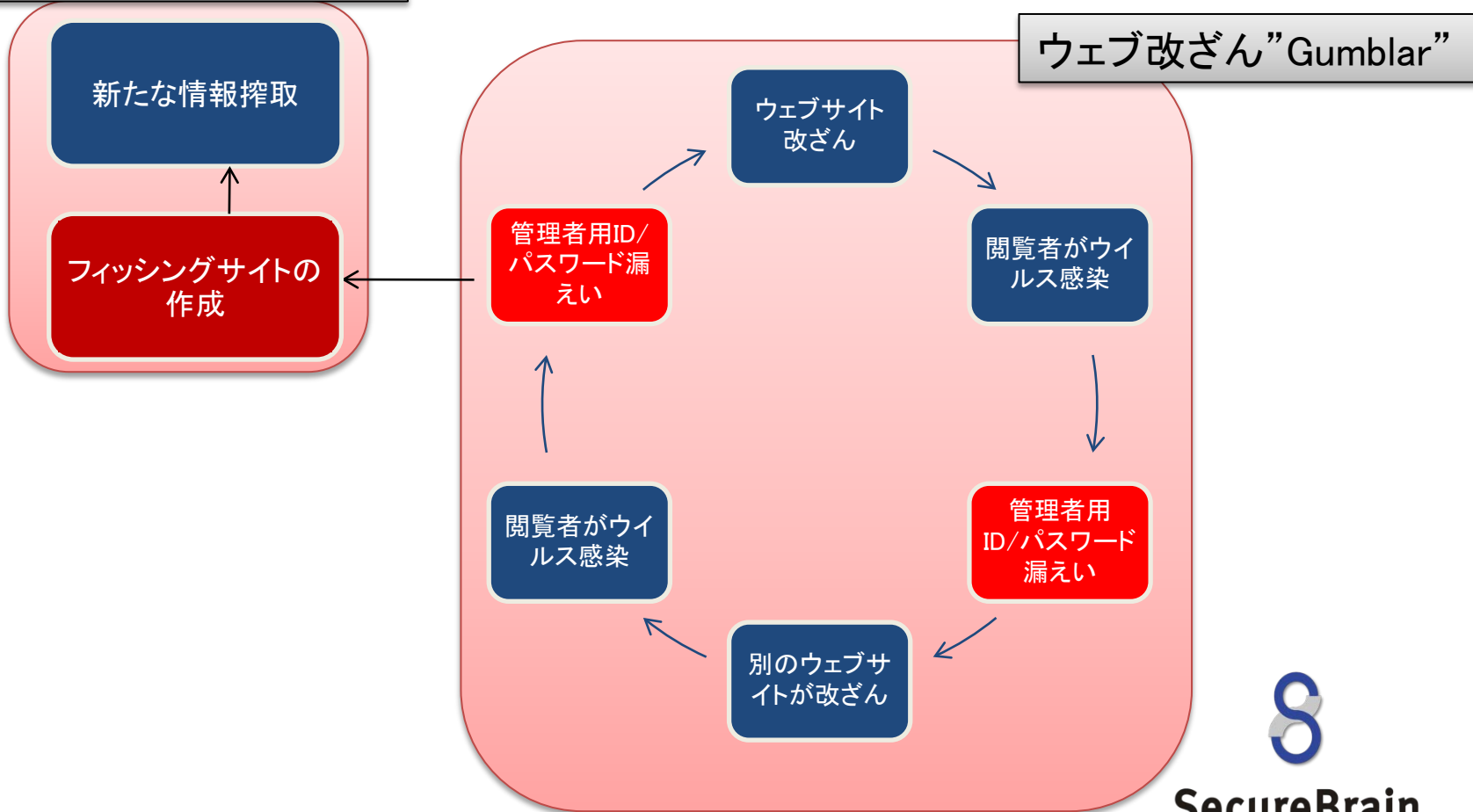
新しい手法と、旧来の手法が併用されている。

マルウェアを使って搾取したデータの二次利用



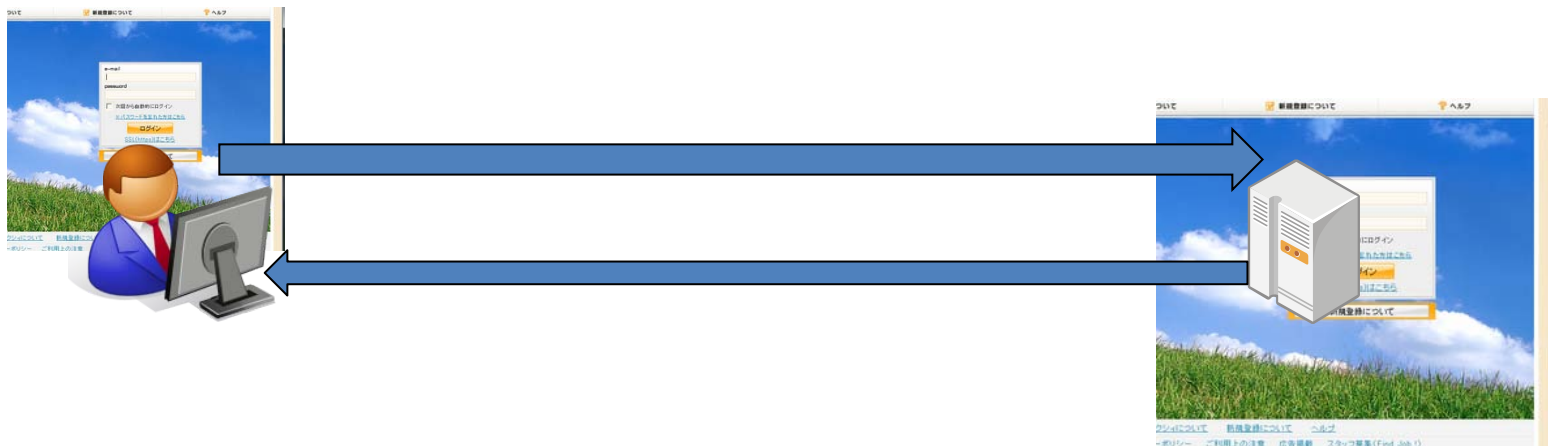
最近の攻撃事例 - Gumblar+フィッシング詐欺

二次被害・予測困難



リアルタイムな情報搾取

Man in Middle



SecureBrain

リアルタイムな情報搾取

Man in Middle



SecureBrain

APWG vs 犯罪組織

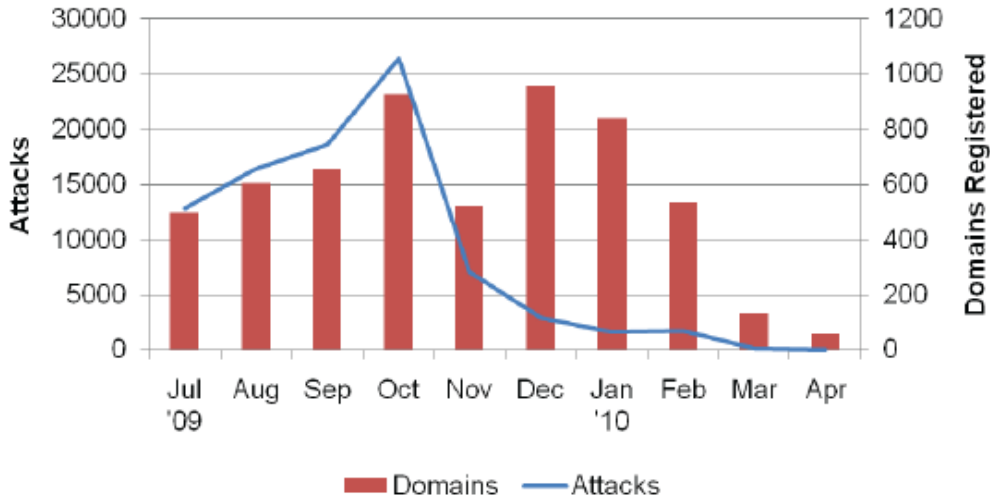
- ◆ APWGの活動として、フィッシング詐欺を行う「犯罪組織」の活動を阻止するという取り組みがある。
- ◆ 世界的に有名な組織は「Avalanche」
 - ◆ 全世界のフィッシング詐欺の80%を占めている
 - ◆ 不正なドメインを取得して、そこにフィッシングサイトを作成する



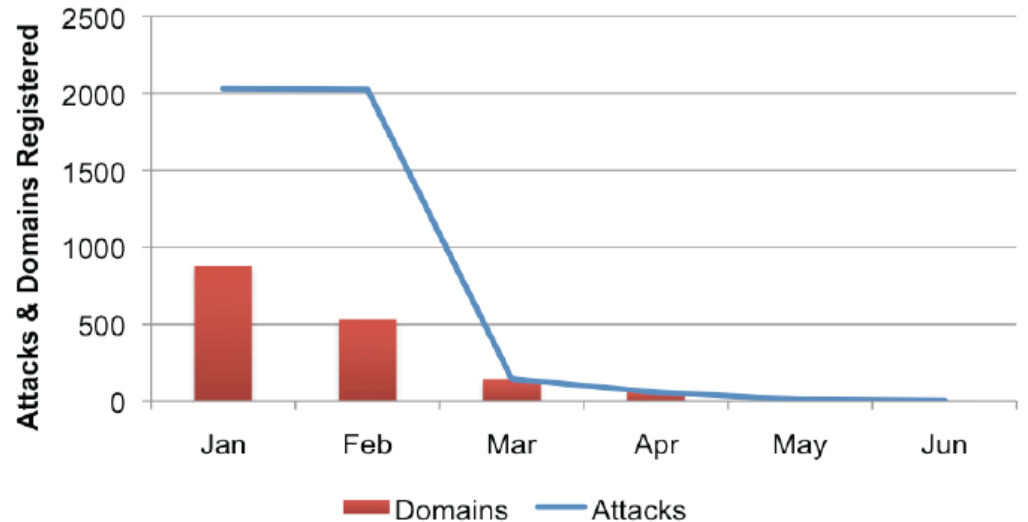
APWGの取り組みにより、2010年に入ってから「Avalancheドメイン」は急激に減少している。



Avalanche Attacks & Domains Registered



2010 Avalanche Attacks & Domains Registered



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、一般のサーバをハッキングし、フィッシングサイトを設置する事例が増加している。
- ◆ 28,646個のフィッシングサイトの83%は一般のウェブサイト



新たな攻撃手法: Tabnabbing Attack

- ◆ 2010年5月頃に発表された「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

Yahoo! JAPAN x Top 10 Security ... x STOP.THINK.CO... x APWG: Resources x Amazon.co.jp : ... x Tabnabbing: A ... x

I'm **Aza Raskin** @azaaza. I make shiny things. I simplify.
I make **cardboard** furniture. Check out **Bloxes.com**.

Algorithm Ink Firefox Mobile Ubiquity

TABNABBING: PHISHING ATTACK

The web is a general... Sometimes I think I missed my calling; being devious is so... too bad my parents brought me up with scruples.

Most phishing attacks depend on an original deception. If you detect that you are at the wrong URL, or that something is amiss on a page, the chase is up. You've escaped the attackers. In fact, the time that wary people are most wary is exactly when they first navigate to a site.

SPONSORED BY
It's the easiest
\$250
you'll ever make.
Earn \$250 for every business you refer that buys a Clover website before 2011.

What we don't expect is that a page we've been looking at will change behind



おまけ：海外にもある、振り込め詐欺

“I was mugged in London, please send money...”
(ロンドンで強盗にあってしまいました、大至急お金を送ってください……)

Hello!

I'm sorry I didn't inform you about my traveling... am presently in London, United Kingdom on short vacation and as i write to you now.. its unbelievable am stuck here, got mugged at gun point on my way to the hotel and my money, credit cards, phone and other valuable things were taken off me at gun point, thanking Almighty God for save keeping my passport., i really need your urgent assistance quickly ? **I JUST NEED SOME FEW HUNDREDS \$\$\$ TO SORT OUT MY HOTEL BILLS AND** i promise to refund it back to you once i get home cause i still have some cash in my account but i cant access any here right now ,already canceled all my cards immediately after the muggers took my things off me!!! still at the public internet library where am making use of the free internet access, i will forever be grateful if you can help me, Waiting to hear from you quickly cos my flight leaves in few hrs but need to sort the hotel bills and please save me from been embarrassed.

Thanks.
Michele



SecureBrain

中国の状況

- ◆ 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。
- ◆ 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。
- ◆ 北京オリンピックの際にはチケット販売の偽装サイト、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。

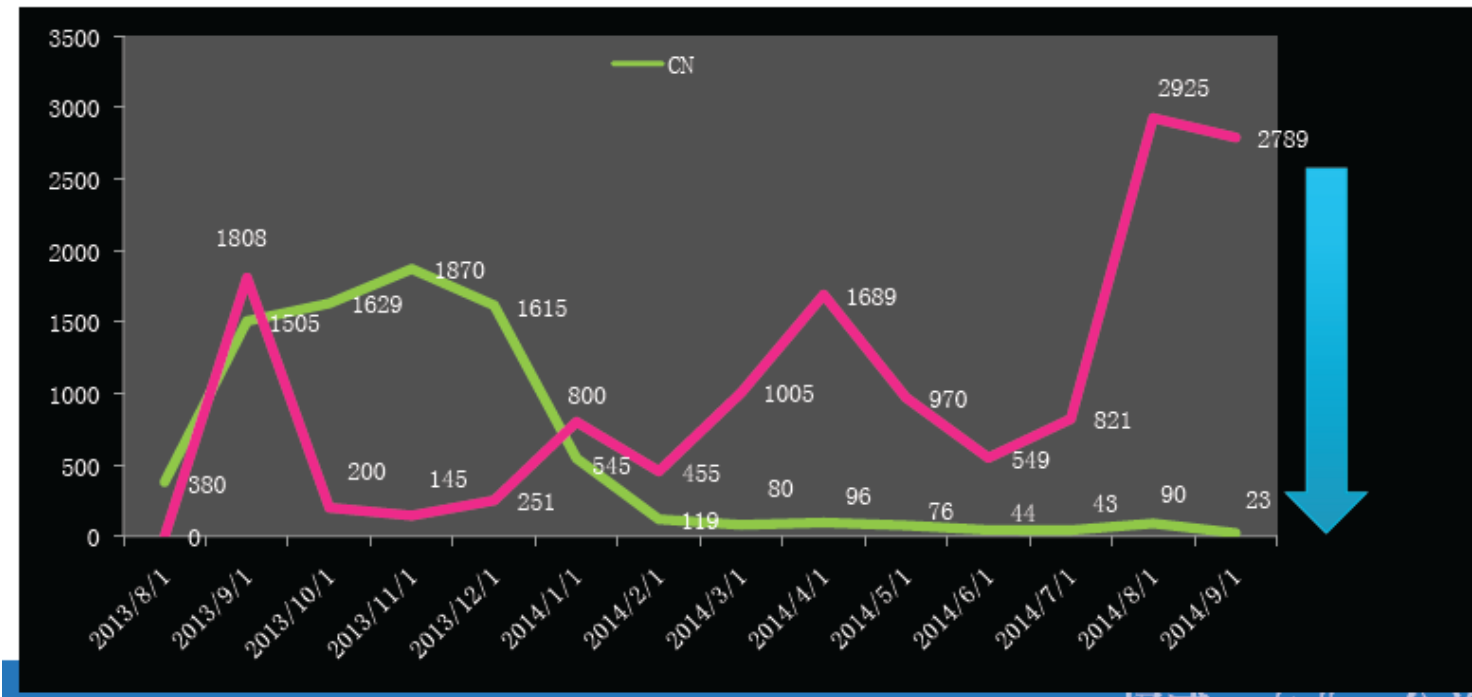
Official: www.tickets.beijing2008.cn



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



CNDメインの正常化への努力



フィッシング対策技術について



PC・クライアント側の対策



サーバ側の対策



ISP側の対策



SecureBrain

PC・クライアント側の対策

アンチウイルス

詐欺対策

情報漏えい防止

スパムメール対策

悪質なウェブサイト
対策

情報収集



サーバ側の対策について



ISP側の対策について

安全なサーバ運営

教育

情報収集・提供

監視体制

バックアップ体制

連携



SecureBrain

従来のセキュリティ対策に加えて！

従来の対策と併用して「フィッシング対策」
を考えていく必要性があります

フィッシング対策

情報漏えい対策
不正アクセス対策
スパム対策



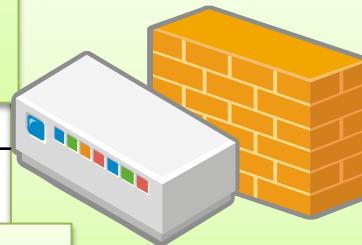
ファイルサーバ



メールサーバ



ウェブサーバ



ルーター・ファイアウォール

情報漏えい対策
不正アクセス対策

ウイルス対策
情報漏えい対策
ウェブフィルタリング



顧客



取引先

対外的な施策



インターネット



他の企業



クラウドコンピューティング

正しく安全な
サービス選択



SecureBrain

まとめ

- ➡ フィッシング詐欺の攻撃手法は日々進化しています。
- ➡ ウイルス・スパイウェア・改ざん・不正アクセス等、組み合わせは無限です。
- ➡ 旧来の手法が再び活用されることもあります。
- ➡ アプリケーション・サービス・プラットフォームの進化は、新たな脅威を生みます。
- ➡ 対策については「ソリューションの活用」と同時に「情報収集」「教育」も重要なポイントです。
- ➡ フィッシング対策協議会、セキュリティベンダーは今後とも、フィッシング詐欺と戦い、安全なインターネット環境の構築に努力していきます。



ご清聴ありがとうございます。



SecureBrain