



Finding the Banking Trojan in Eastern Asia

Noriaki HAYASHI

Senior Researcher

Forward-looking **T**hreat **R**esearch



CeCOS VII - Buenos Aires



Unifying the
Global Response
to Cybercrime

Introduction

林 憲明

Forward-looking **T**hreat **R**esearch

- オンライン詐欺
- スマートフォン
- 組込機器 / 車載機器



フィッシング対策協議会
運営委員



トレンドマイクロ株式会社
シニアリサーチャー

Agenda

1. 背景

2. Banking Trojanの変遷

3. 日本における“Citadel”の報告

4. Mobileを狙った攻撃

5. 協議会による取り組み

Agenda

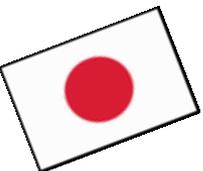
1. 背景

2. Banking Trojanの変遷

3. 日本における“Citadel”の報告

4. Mobileを狙った攻撃

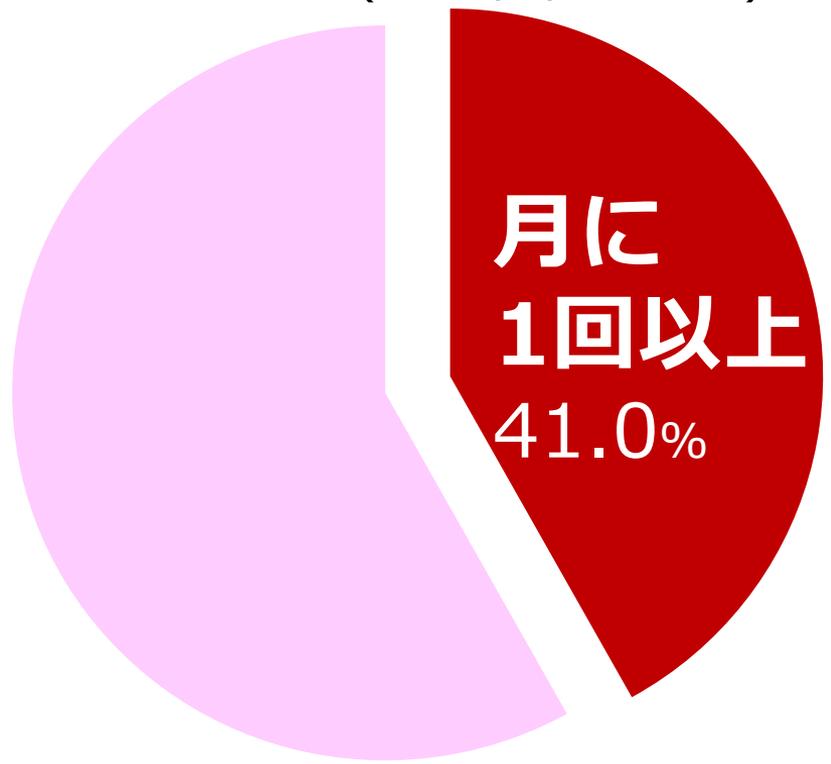
5. 協議会による取り組み



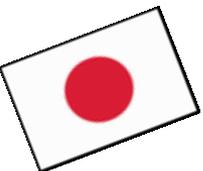
アクセス頻度

オンラインバンキングに関する調査

※出典：楽天リサーチ株式会社(2012/5/29 - 30)、N = 1,000



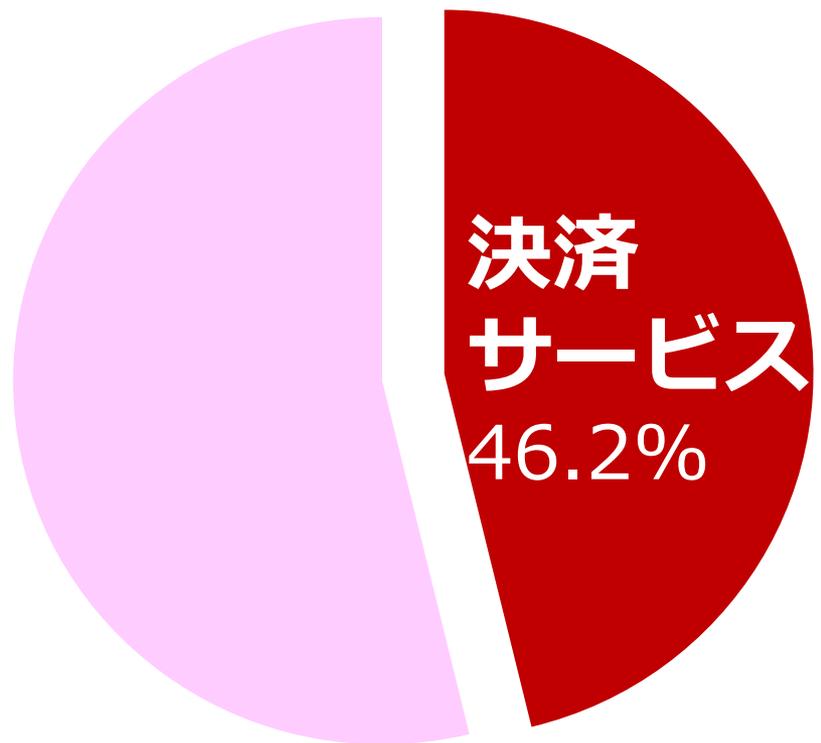
 <http://research.rakuten.co.jp/report/20120621/>



アクセス頻度

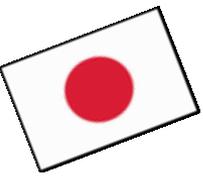
オンラインバンキングに関する調査

※出典：楽天リサーチ株式会社(2012/5/29 - 30)、N = 1,000



 <http://research.rakuten.co.jp/report/20120621/>

日本のインターネットを釣場とする フィッシャー



言語がフィッシングに及ぼす影響



VISA カード保有者のみなさまへ

VISA カードをお持ちのお客様は自動的に VISA 認証サービス プログラム** にご加入いただいております。

VISA 認証サービスでは、お客様の個人パスワードをお持ちの VISA カードのセキュリティを強化します。オンラインストアでのお支払い手続きの際に、ATM で暗証番号を入力するのと同じようにパスワードを入力していただきます。これにより、実際にお店でカードを使用するときと同じように、VISA カードをオンラインで安全に使用することができます。

サービスの中断を避けるため、できる限り早急にカード情報をご確認させていただく必要がございます。ご確認のうえ、サービスが中断しないよう、早急にご対応ください。

たいへんお手数ですが、次のカード情報確認ページ* へのリンクをクリックしてください。
<https://www.visa.co.jp/secure/>

- お手続きは、次の手順に従ってください。
- 上記のリンクをクリックして、カード情報をご入力ください。
- VISA カード情報を照会して、個人パスワードを再入力してください。
- これでアカウントが更新され、サービスが中断されることなく引き続きカードをご使用いただけます。

このサービスにより引き起こされるご不便に関しては、深くお詫び申し上げます。

VISA 社員一同

- * ご注意: VISA カードの更新に失敗した場合、一時的にカードが使用できなくなります。
- * クレジットカードを 2 枚以上お持ちの場合は、フォームを再送信してください。
- * クレジットカードを 2 枚以上お持ちの場合は、カードに別々のパスワードを設定することができます。



Copyright 2004, Visa International Service Association. All rights reserved.
このお知らせは 2004 年 10 月 30 日まで有効です。

フィッシングメールの変遷

2003年

世界初、英語のフィッシングメール
※オーストラリアの銀行を標的

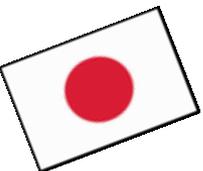
2004年

日本語

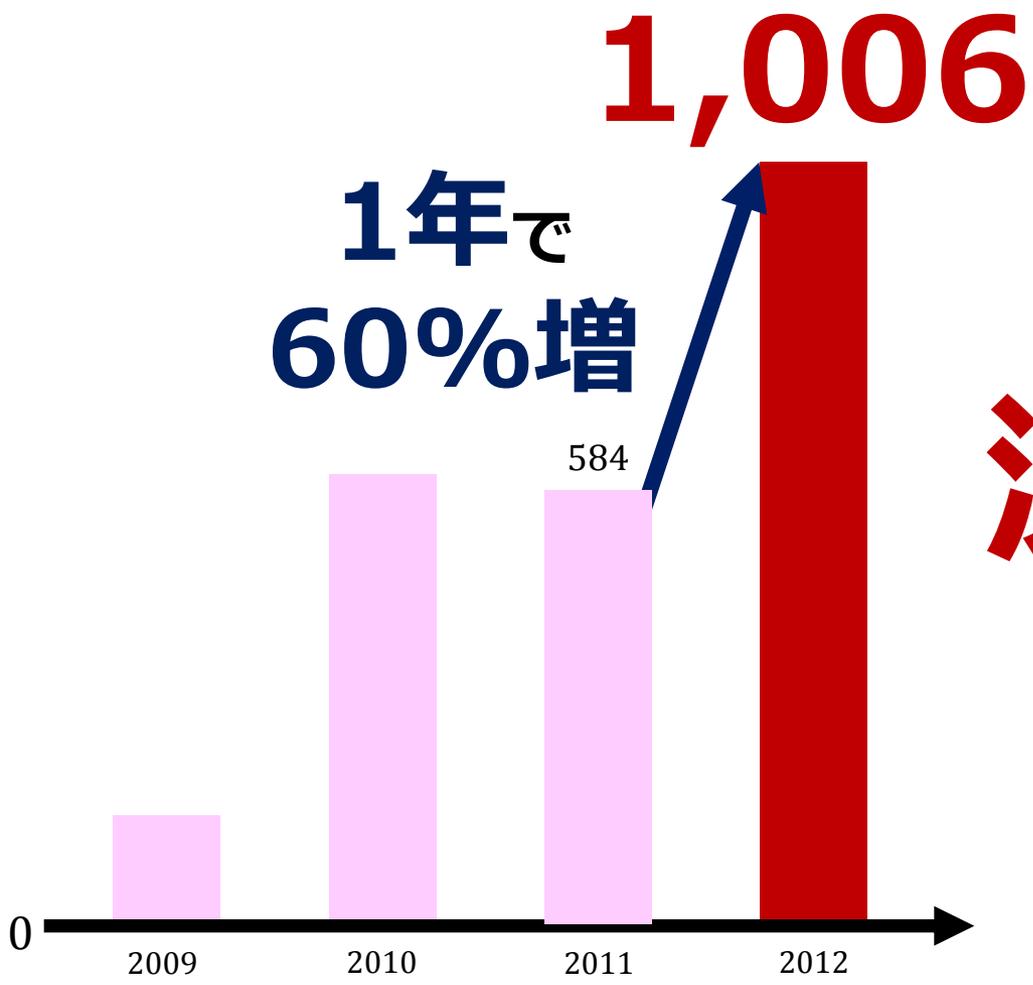
のフィッシングメール

脅威が言語の壁を 超えた



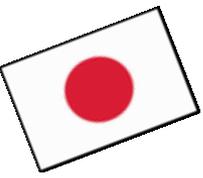


フィッシングサイトのURL件数



深刻な被害

※出典：フィッシング対策協議会 月次報告書



ファイッシャーが狙う4つの業界

Financial

Sanwa Bank (三井住友銀行) and Sanwa Net Bank (三井住友ネット銀行) website screenshots. The Sanwa Bank page shows a login form with fields for '契約者番号の入力' (Contractor number input) and '第一暗証の入力' (First PIN input). The Sanwa Net Bank page features a '新生生活応援キャンペーン' (New Life Support Campaign) with a '1,000円' (1,000 yen) offer and a '火災保険' (Fire Insurance) section. A calendar grid is visible on the right side of the Sanwa Bank page.

Social Network

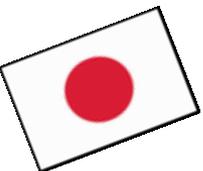
Screenshots of social media login pages. Twitter shows a 'Your session has timed out, please re-login.' message. Facebook shows a 'Facebook Login' form with fields for 'Email' and 'Password'. Ameba shows a colorful promotional banner with the text 'おいしいハイボール ついでにみませんか。' (Delicious Highball, why not try it?).

Online Game

Screenshots of online game websites. The top left shows a game interface for Final Fantasy XIV. The bottom left shows the IMAGINE website with a 'DB Member Login' section and a '新規会員登録' (New Member Registration) button. The bottom right shows another game website with a 'ログイン' (Login) button.

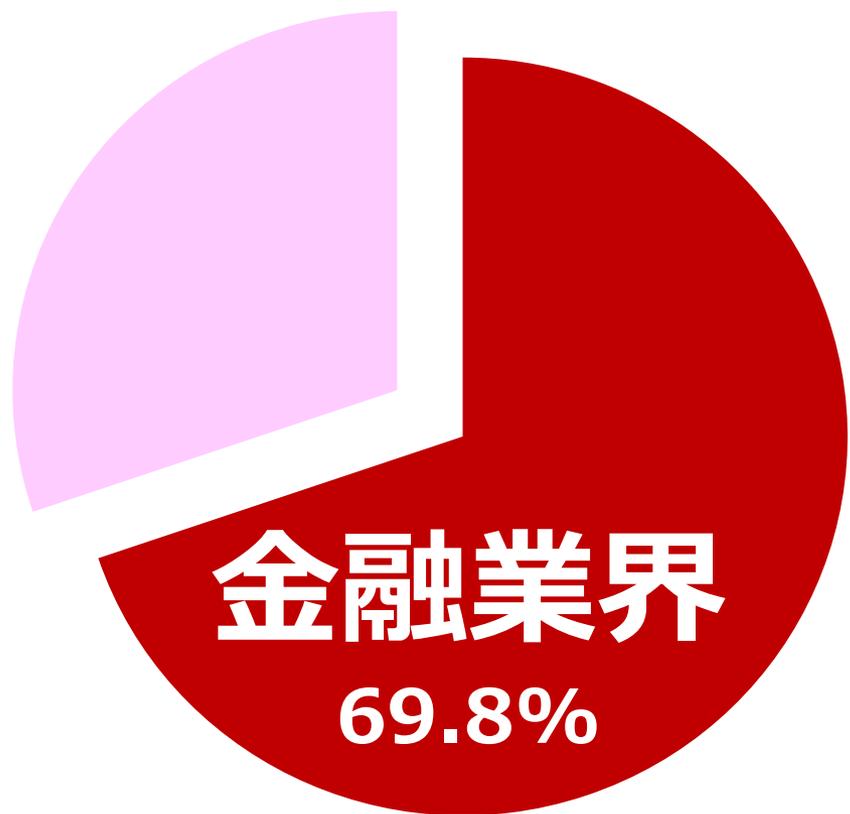
ISP

Screenshots of ISP websites. OCN Mail shows a 'メールアドレスをlook upでログイン' (Login with email address using look up) section. BIOLABE Mail shows a 'モバイル対応でどこでもメール' (Mobile compatible, email anywhere) section and a 'BIOLABEメール ログイン' (BIOLABE Mail Login) section.



金融業界

最も深刻な被害



Agenda

1. 背景

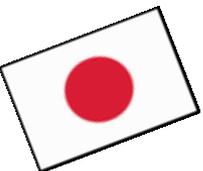
2. Banking Trojanの変遷

3. 日本における“Citadel”の報告

4. Mobileを狙った攻撃

5. 協議会による取り組み

日本のオンライン銀行詐欺ツール



2011
Fake Popup
Two-Factor Auth

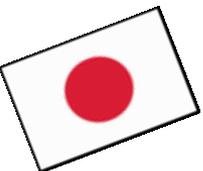


2011年
フィッシャーが見つけた
新たな標的



NEW 標的

二要素認証情報
搾取手口
偽のポップアップ



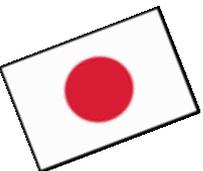
2005
KeyLogger
Sniffing ID & Pass

2011
Fake Popup
Two-Factor Auth

この頃の特徴は…
オンライン銀行詐欺ツールはまだ原始的

利用者が注意すべき「指標」がある。

- 疑わしいURL / 添付ファイル
- あり得ない問い合わせ
- 不自然な日本語



2005

KeyLogger
Sniffing ID & Pass

2011

Fake Popup
Two-Factor Auth



2004

Phishing
日本語のFake Site

2012 - 2013...

Webinjects / MITB
Knowledge-based Auth

犯罪技術は年々進化

MITBにより被害の舞台は本物へ



Agenda

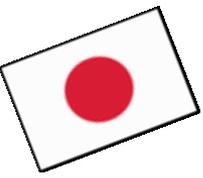
1. 背景

2. Banking Trojanの変遷

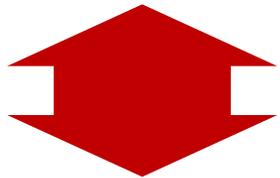
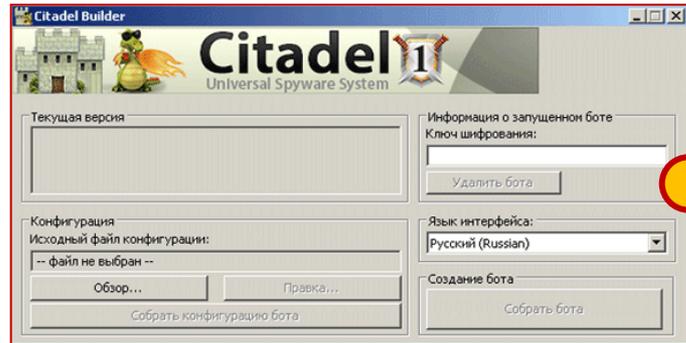
3. 日本における“Citadel”の報告

4. Mobileを狙った攻撃

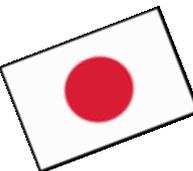
5. 協議会による取り組み



Citadel の標的を探る



“config.bin”
の**解読**により
標的を知る



多くの銀行で採用されるEVSSL

ゆうちょダイレクト | ログイン(お客さま番号入力) - Windows Internet Explorer

https://direct.jp-bank.japanpo... JAPAN POST BANK Co., Ltd.

Web サイトの認証

VeriSign
で、このサイトを次のように認証しました:
JAPAN POST BANK Co.,Ltd.
Chiyoda-ku, Tokyo
JP

このサーバーへの接続は暗号化されています。
このサイトを信頼するべきですか?

証明書の表示

お客さま番号を入力し、
お客さま番号を忘れた場合は
[照会・再発行の手続き](#)

新規登録のご案内

お知らせ

- 【重要】不正にポップアップ画面を表示させてゆうちょダイレクトの情報を盗み取ろうとする犯罪にご注意ください。([詳細はこちら](#))
- 取扱確認メールアドレスのご登録がないお客さまには、ログイン時に登録画面が表示されますので、登録をお願いします。([詳細はこちら](#))
- 取扱確認メールアドレスを登録しておけば、万が一、不正な取引があった場合でも、早期に発見することができます。また、合言葉の初期化をインターネットでお手続きいただくこともできます。([詳細はこちら](#))
- 入金お知らせメールをご利用のお客さまも、取扱確認メールアドレスの登録をお

お客さま番号 (半角数字) [] - [] - []

お客さま番号は、4桁 - 4桁 - 5桁と区切って半角で入力してください。

[新規登録のご案内はこちら](#)

ホームへ

ご利用上の注意

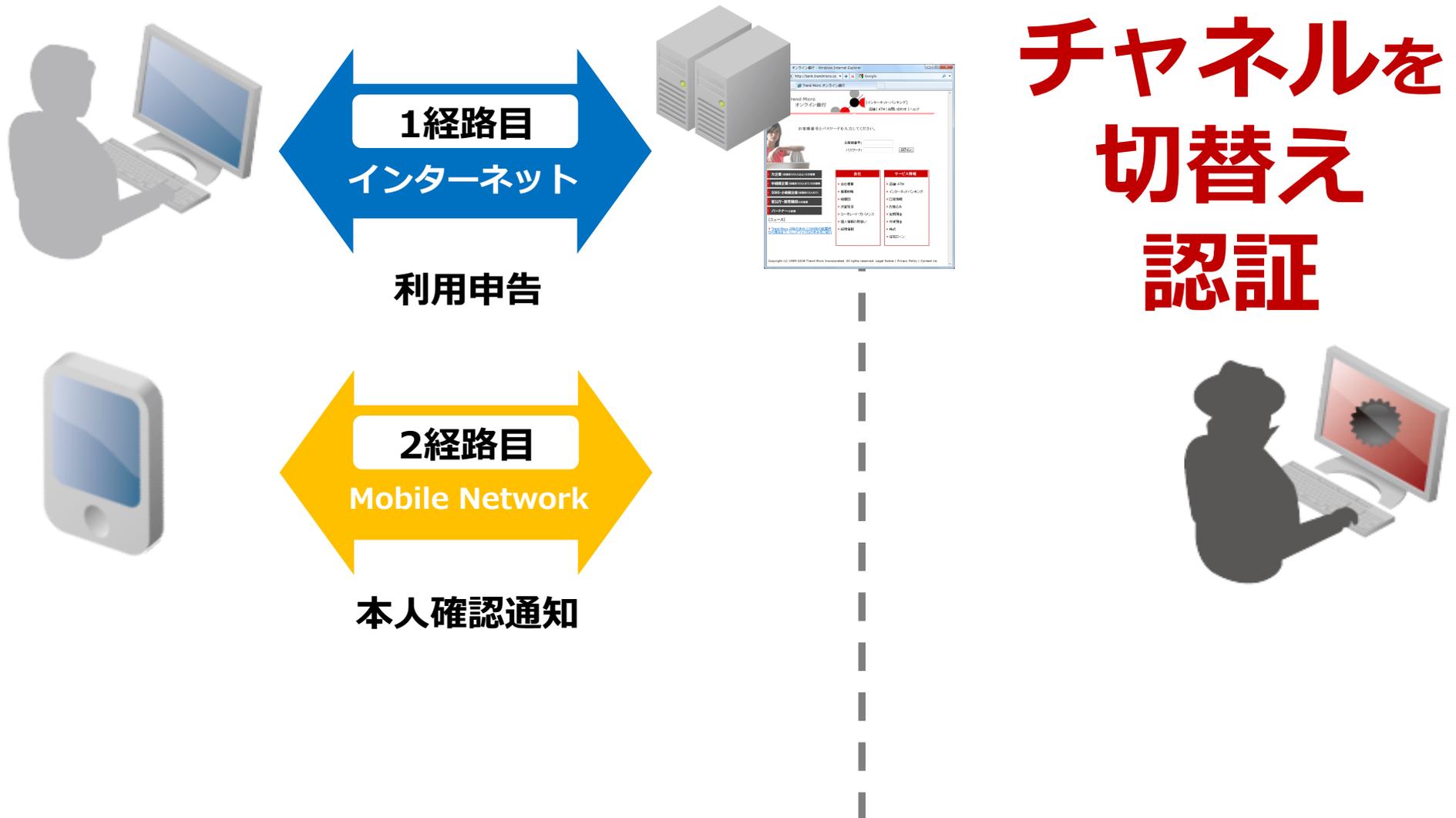
- 暗証番号のお取扱いにご注意ください。([詳細はこちら](#))
- ブラウザの「戻る」「進む」ボタンは使用しないでください。
ゆうちょダイレクトの画面上のボタンで操作してください。

ページが表示されました

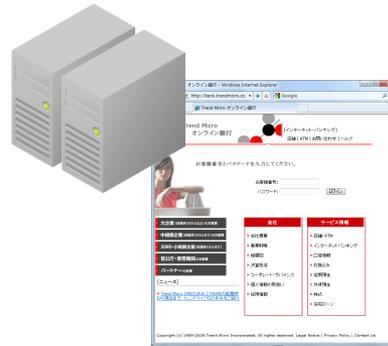
スタート sample ゆうちょダイレクト | ログ... 14:26

「なりすまし」から身を守る術

二経路認証 (OUT-OF-BAND Auth)



二経路認証 (OUT-OF-BAND Auth)



チャンネルを 切替え 認証



不正な
利用申告



Agenda

1. 背景

2. Banking Trojanの変遷

3. 日本における“Citadel”の報告

4. Mobileを狙った攻撃

5. 協議会による取り組み



SMS + Phishing = Smishing

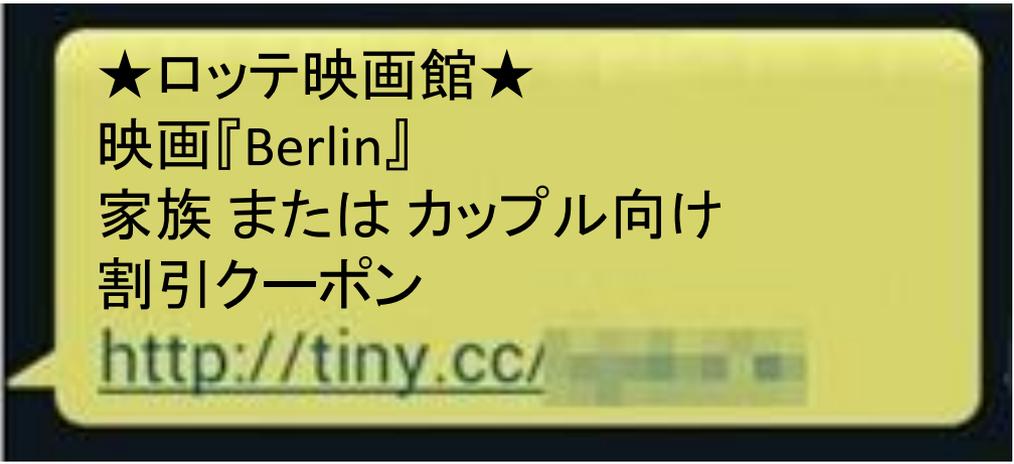
スミッシング詐欺

SMSで短縮URL通知

オンラインストレージ

経由で配布

AndroidOS_CHESTIA



※トレンドマイクロにてSMSの内容を翻訳



クーポンアプリを偽り配布 ハイジャックモバイルを作成

警戒心を解くために 悪用された ブランド





Fake Error Message

Android OS - CHESTIA





認証番号の横取り

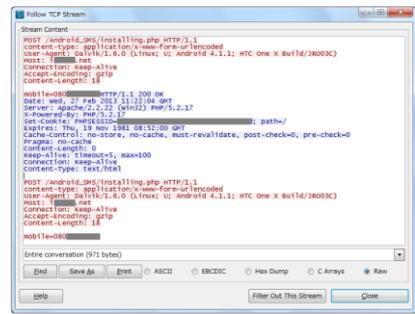
- 発信元が
- 利用者へ
- 攻撃者へ



のみ監視
を見せない
を転送



Android CHEST.A



androidtest view - Windows Internet Explorer

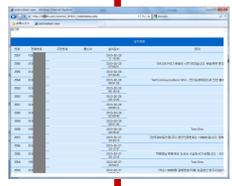
주소창 http://192.168.0.10/Android_SMS/installstatus.php

주소 androidtest view

| 번호 | 전화번호 | 주민번호 | 통신사 | 발착일시 | 발착내량 | 문자 |
|------|------|------|-----|---------------------|------|---------------------------------------|
| 2567 | 156 | | | 2013-02-28 11:16:49 | | |
| 2566 | 010 | | | 2013-02-28 07:56:51 | | [카드] 배송이 시작되었습니다. 배송관련 문의 |
| 2565 | 010 | | | 2013-02-28 07:56:49 | | |
| 2564 | 010 | | | 2013-02-28 08:51:26 | | Tell Communications SPA - 만기요청해결요로 인한 |
| 2563 | 010 | | | 2013-02-28 08:51:18 | | |
| 2562 | 156 | | | 2013-02-28 08:12:26 | | |
| 2561 | 010 | | | 2013-02-28 03:05:16 | | |
| 2560 | 010 | | | 2013-02-28 02:01:40 | | |
| 2559 | 010 | | | 2013-02-28 00:51:46 | | |
| 2558 | 156 | | | 2013-02-28 00:26:32 | | Test Sms |
| 2557 | 010 | | | 2013-02-27 23:30:15 | | [한국투자증권(주)] 본인인증번호는 14904입니다. 정척 |
| 2556 | 010 | | | 2013-02-27 23:13:37 | | |
| 2555 | 010 | | | 2013-02-27 23:12:16 | | 백화점년 회원제로 오셔서 수납하시기 바랍니다. - SO |
| 2554 | 156 | | | 2013-02-27 22:54:21 | | Test Sms |
| 2553 | 010 | | | 2013-02-27 22:54:21 | | (예) 30000원 국제전화/이월 요금한선 청구(내/가 |

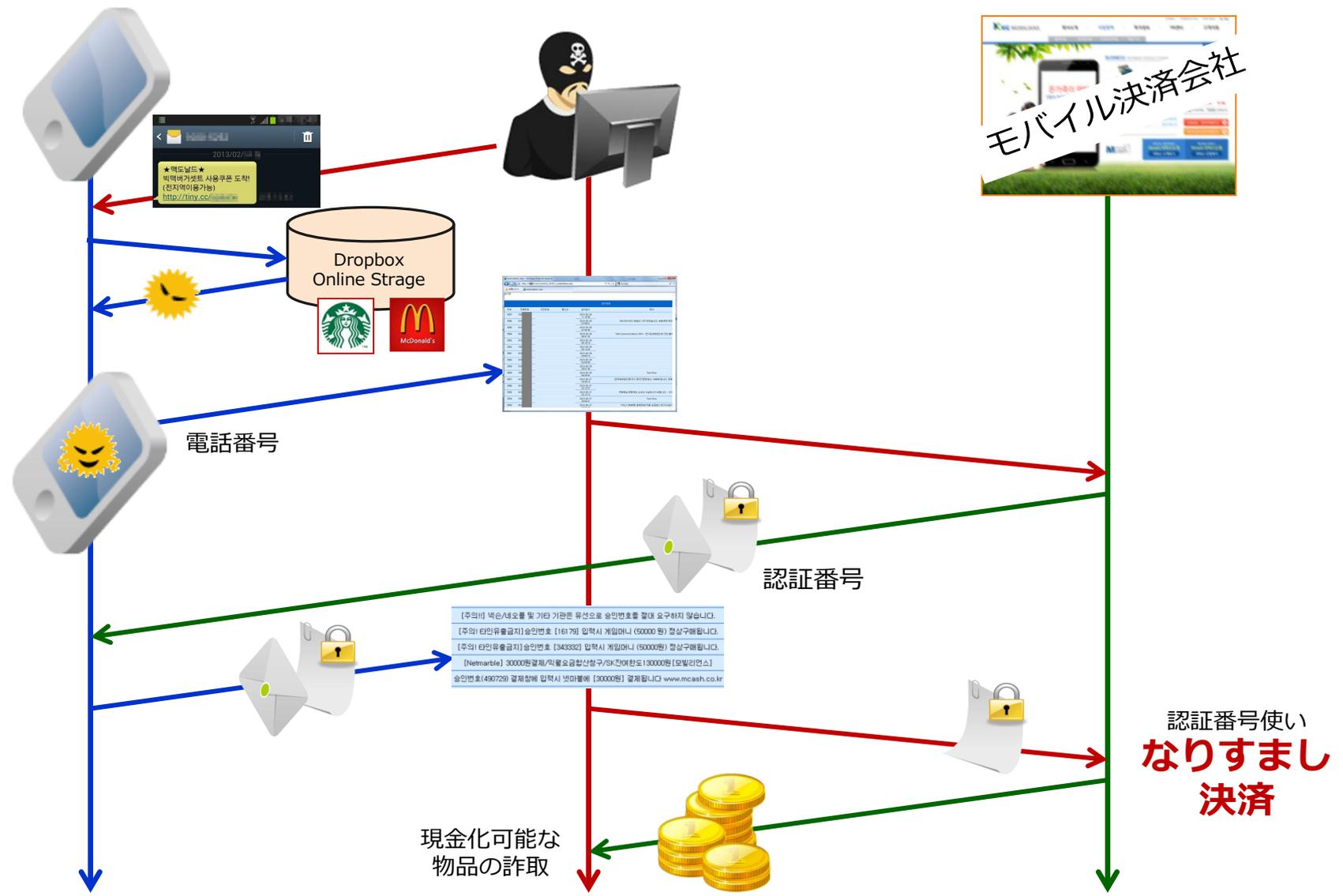


AndroidOS_CHEST.A





AndroidOS_CHEST.A



Agenda

1. 背景

2. Banking Trojanの変遷

3. 日本における“Citadel”の報告

4. Mobileを狙った攻撃

5. 協議会による取り組み

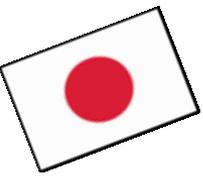
利用者へアドバイス

1. 怪しいメールに注意
2. 正しいURLにアクセス
- 3. パソコンを安全に保つ**



消費者向けフィッシング詐欺対策
ガイドライン

2012年12月



感染の連鎖を絶つ脆弱性対策

MyJVN バージョンチェッカ



MyJVNバージョンチェッカ

実行 終了 全てを選択 選択をクリア 結果出力

「選択されたソフトウェア製品を「実行」することで、最新バージョンであるかをチェックします。「最新のバージョンではありません」と表示された場合には、表示ボタンを押下後ツール下部の内容を参考にして、ベンダから最新のバージョンを入手してください。利用に関する情報は、[MyJVNのウェブページ](#)を参照ください。

| ソフトウェア製品名 ▲ | チェック結果 ▲(×○一順) | 結果詳細 ▲ |
|--|-----------------------------|--------|
| <input checked="" type="checkbox"/> Adobe Flash Player (ActiveX) | × 最新のバージョンではありません | 表示 |
| <input checked="" type="checkbox"/> JRE | × 最新のバージョンではありません | 表示 |
| <input checked="" type="checkbox"/> Adobe Flash Player (Plug-in) | ○ 最新のバージョンです | 表示 |
| <input checked="" type="checkbox"/> Adobe Reader | ○ 最新のバージョンです | 表示 |
| <input checked="" type="checkbox"/> Mozilla Firefox | ○ 最新のバージョンです | 表示 |
| <input checked="" type="checkbox"/> Adobe Shockwave Player | — インストールされていないか、対象外のバージョンです | |
| <input checked="" type="checkbox"/> Becky! Internet Mail | — インストールされていないか、対象外のバージョンです | |
| <input checked="" type="checkbox"/> Lhaplus | — インストールされていないか、対象外のバージョンです | |
| <input checked="" type="checkbox"/> Lunascape | — インストールされていないか、対象外のバージョンです | |
| <input checked="" type="checkbox"/> Mozilla Thunderbird | — インストールされていないか、対象外のバージョンです | |
| <input checked="" type="checkbox"/> OpenOffice.org | — インストールされていないか、対象外のバージョンです | |
| <input checked="" type="checkbox"/> QuickTime | — インストールされていないか、対象外のバージョンです | |
| <input checked="" type="checkbox"/> VMware Player | — インストールされていないか、対象外のバージョンです | |

MyJVN セキュリティ設定チェッカ



MyJVNセキュリティ設定チェッカ

実行 終了 全てを選択 選択をクリア 結果出力

「選択されたチェック項目を「実行」することで、セキュリティに関するPC設定値が参考値を満たしているかをチェックします。「参考値を満たしていません」と表示された場合には、表示ボタンを押下後ツール下部の内容を参考にしてPC設定値を変更してください。利用に関する情報は、[MyJVNのウェブページ](#)を参照ください。

| チェック項目 ▲ | 参考値 | PC設定値 | チェック結果 ▲(×○順) | 結果詳細 ▲ |
|--|-----|-------|----------------|--------|
| <input checked="" type="checkbox"/> USBメモリ自動実行に関するパッチ(KB971029) 適用 | 適用済 | 適用済 | × 参考値を満たしていません | 表示 |
| <input checked="" type="checkbox"/> USBメモリ自動実行機能の無効化設定 | 設定済 | 設定済 | ○ 参考値を満たしています | 表示 |

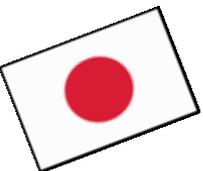
詳細情報

USBメモリ自動実行機能の無効化設定: 詳細情報

このセキュリティ設定は、自動起動をオンにすると、USBメモリをコンピュータに挿入した際に、メモリの内容に従った処理が自動実行されます。自動実行をオフにすると、USBメモリをコンピュータに挿入しても、自動的に実行されなくなります。

<http://jvndb.jvn.jp/apis/myjvn/vccheck.html>

<http://jvndb.jvn.jp/apis/myjvn/sccheck.html>



パスワード管理を託す

Gadget



パスワードマネージャー「ミルパス」
MIRUPASS
PASSWORD MANAGER PWIO

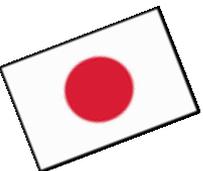
<http://www.kingjim.co.jp/sp/pw10/>

Software



パスワードマネージャー

<http://safe.trendmicro.jp/purchase/pm.aspx>

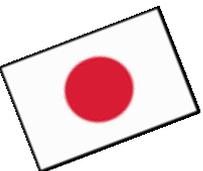


利用者を救済する責任を果たす…

フィッシング対策機能を提供する事業者に対して、
ブラックリストURLを提供する。

14社に提供中(2013年4月現在)





利用者に注意 責任を果たす...

Yahoo!ツールバー フィッシング警告

! このページはフィッシング詐欺サイトの疑いがあります。

表示ドメイン **yahoogoo.co.jp**
表示アドレス **http://www.yahoogoo.co.jp/test/phishing/yahoo.phshing.htm**

表示ドメインが、ご利用サイトの正しいドメインかどうかをご確認ください。
なお、Yahoo! JAPANのサイトの場合は **yahoo.co.jp** と表示されます。

フィッシング詐欺サイトの疑いがある場合は、ページを閉じることを強くお勧めします。
パスワード、クレジットカード番号などの個人情報は入力しないでください。

※報告する情報には、個人情報は含まれません。

ウイルスバスター for Mac

ウイルスバスター for MacによりWebサイトをブロックしました

このWebサイトを開くとセキュリティを脅かす可能性があります。

このウィンドウを閉じるか、[対処方法]の指示を参照してください。

URL: **http://...**
評価: **不審**

評価キー

- 警告
表示しようとしているWebサイトは、不正プログラムをダウンロードするWebサイトや、オンライン詐欺に遭うWebサイトです。
- 不審
表示しようとしているWebサイトは、不正プログラムをダウンロードするか、オンライン詐欺に関係している可能性があります。
- 未テスト
フィッシング詐欺対策機能が「高」に設定されているので、安全のために、未調査のサイトはすべてブロックされています。

対処方法

- 他のサイトにアクセスして必要な情報を探してみてください。
- このサイトが安全と考えられる場合は、[トレンドマイクロにこのページを確認するように通知](#)してください。
- ブロックされたページにアクセスする場合は、次の手順に従ってください。
 - ウイルスバスター for Macのコンソールを開きます。
 - [Web対策] をクリックし、[フィッシング詐欺対策] タブをクリックします。
 - カギのアイコンをクリックし、パスワードを入力します。
 - [許可するWebサイト...] ボタンをクリックします。
 - + (プラス記号) ボタンをクリックします。
 - ブロックされたWebサイトのアドレスをリストにコピーアンドペーストします。



Thank You!



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

- Contact presenter at management@antiphishing.jp, noriaki_hayashi@trendmicro.co.jp if you are interested in:
 - Asking questions
 - Helping with the project



CeCOS VII - Buenos Aires



Unifying the
Global Response
to Cybercrime