RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

IPとテレフォニー犯罪の集結
– 目を覚まし、現実を知り、保護する！

セッションID：JPN-T10

Andy Dancer

ディレクター
Evolved Intelligence
@_AndyDancer

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

IP犯罪：
皆がよく分かっていること

マルウェアの進化

- 犯罪者
  - 過去：自室の若者
  - 現在：犯罪の組織化
- 動機
  - 過去：自らの賢さの証明
  - 現在：金儲け
- 期間
  - 過去：「突発的」
  - 現在：ゆっくり内密に

通常、一番の標的はインターネット バンキング

- プロの攻撃者は現金を求めている
- 攻撃の価値が次第に低下
  - アンチウイルス ソフトウェアが検出を開始
  - パッチが使用可能
- そこで、価値の高い攻撃に最初に焦点を当てる
  - 現金に近い

- インターネット バンキング

100%の防御は不可能

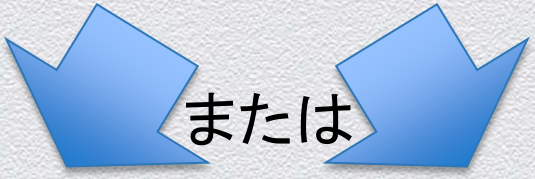
- ほとんどの防御が事後対応型
  - クラウド データベースはアンチウイルスによる迅速な対応に役立つが、やはり事後対応型である
- 攻撃を予測することで一部を防御可能
  - ただし、攻撃者が防御を突破することもある

- 他の防御レイヤーが必要

フォーカス: バンキング防御システム

攻撃の特徴

- ログイン認証情報がターゲット
  - ログイン認証情報を盗んだサイバー犯罪者は、口座の現金を完全に制御できる



- フィッシングによって盗む
  - ユーザーが偽のWebサイトにアクセスするよう仕向ける
  - 銀行のふりをする
  - 入力されたユーザー資格情報を取得する
- キー ロギングによって盗む
  - ユーザー マシンの一部のマルウェアを取得する
  - ユーザーが本物の銀行サイトにログインするときにキー操作/データをインターセプトする

IPバンキング不正は他人事ではない…

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

Zeus Bank Malware Surges On Facebook

Old threat makes a comeback, targeting Facebook users' bank credentials and more.

By Mathew J. Schwartz, InformationWeek
June 05, 2013
URL: http://www.informationweek.co.uk/security/attacks/zeus-bank-malware-surges-on-facebook/240156156

(click image for larger view)
The Syrian Electronic Army: 9 Things We Know
Zeus malware, long popular with the cybercrime underground, has seen a resurgence in the first half of 2013, becoming a weapon of choice for attacks distributed via spam emails as well as social networks such as Facebook.

That finding comes from security firm Trend Micro, which has reported seeing a spike in attempted Zeus Trojan application infections beginning in February 2013 and peaking in May. Zeus malware targets personal and financial data stored on Windows PCs and is controlled via a "Zbot" botnet.

"Old threats like Zbot can always make a comeback because cybercriminals profit from these," said Jay Yaneza, senior technical manager at Trend Micro, in a blog post. "Peddling stolen banking and other personal information from users is a lucrative business in the underground market. Plus, these crooks can use your login credentials to initiate transactions in your account without your consent."

…しかし、常に作り変えられている

強化された防御 – 部分データ

- パスワード全体を入力するのは高リスク
  - 1回のインターセプションで攻撃者はログインできる

- データの部分リクエストによりリスクを低減
  - 9文字のうちの3文字で7個のエントリーを取得して、9文字すべてを取得可能
  - しかし…
    - 3回実行可能
    - 決めるのは不正行為者。銀行ではない

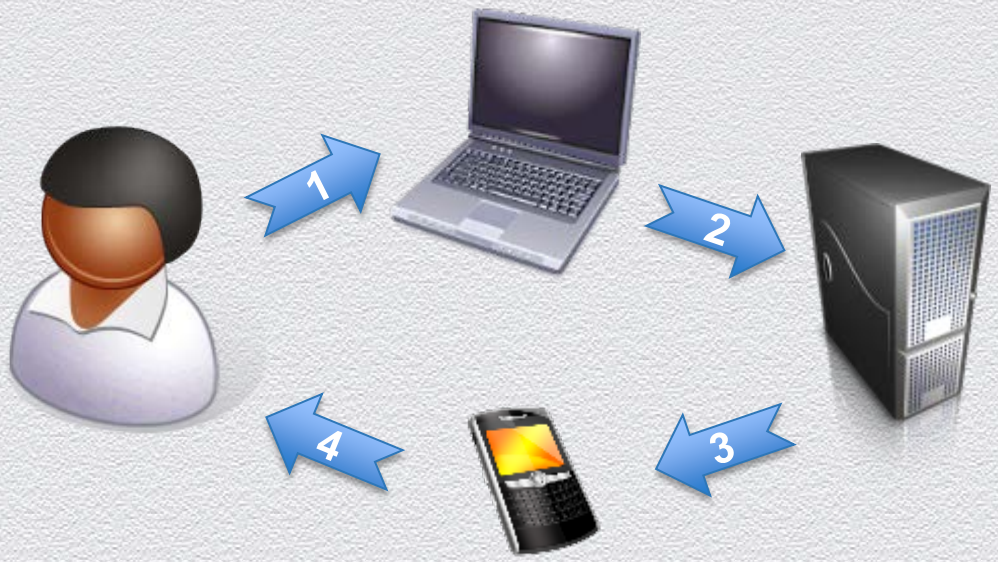
セカンダリ防御 – 2ステップ検証

- ユーザーが所有しているものとユーザーが知っている情報
  - パスワードは知っているもの
  - 所有しているものを追加する必要がある
    - トークン（RSA SecurID）の可能性がある
      - ただし、ユーザーはトークンがいっぱいのキーチェーンを持ち歩かない
    - 銀行の多くが電話を使用
      - お客様に問い合わせるためのインターネット以外の2番目のチャネルを使う手法を提供

IPとテレフォニーの統合

…銀行は「インターネット チャネルの外」の認証で応答…

- テレフォニー チャネルを使用
  - 音声またはテキスト
- ときどき自動
  - プロセスのログの一部
- ときどき目を向ける
  - 新しい支払先
  - 価値の高いトランザクション



...「せめぎ合い」が繰り広げられる！

CRN

Malware Hijacks Two-Step Verification, Drains Bank Accounts

By Robert Westervelt, CRN 10:50 AM EST Tue. Jun. 11, 2013

Banking malware that has been notorious for stealing up to $200,000 a day for cybercriminal gangs has been updated to capture banking customer's text messages, hijacking a key verification service used in high-value transactions to validate the identity of customers.

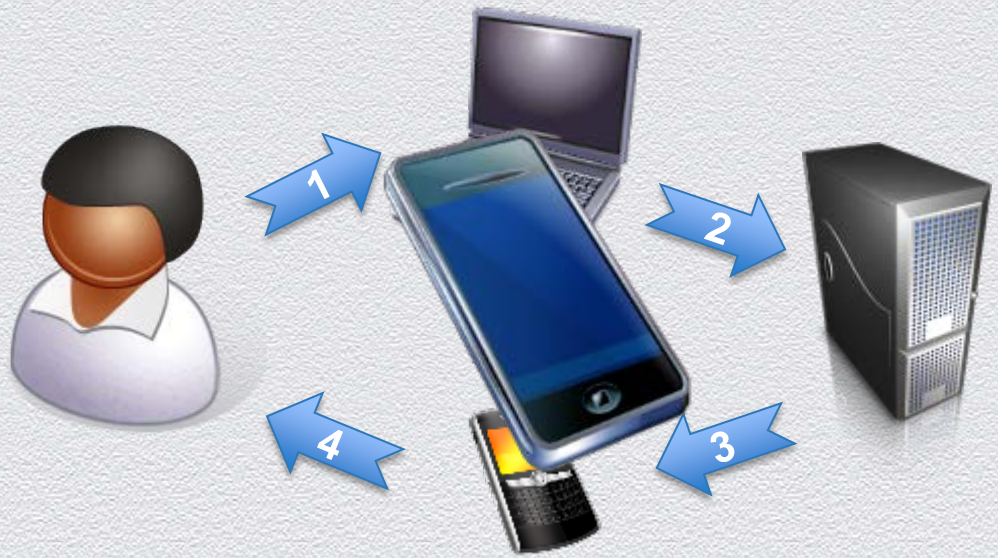
The Bugat Trojan, also known as Cridex, copied two-factor authentication hijacking from the Zeus and SpyEye malware families by adding a mobile text messaging capture feature. The malware is used by financially motivated cybercriminals that target individuals who conduct high-value transactions, according to Limor Kessem, a cybercrime and online fraud communications specialist at RSA's FraudAction Labs. The new technique actually is seen as good news, according to Kessem's analysis of the threat.

"It is very likely that Bugat's operators started seeing a diminished ability to target high-value accounts due to added authentication challenges, forcing them to resort to developing a malware component that is already used by many mainstream banking Trojans in the wild," Kessem wrote.

[**Related:** Top 5 Android Malware Threats]

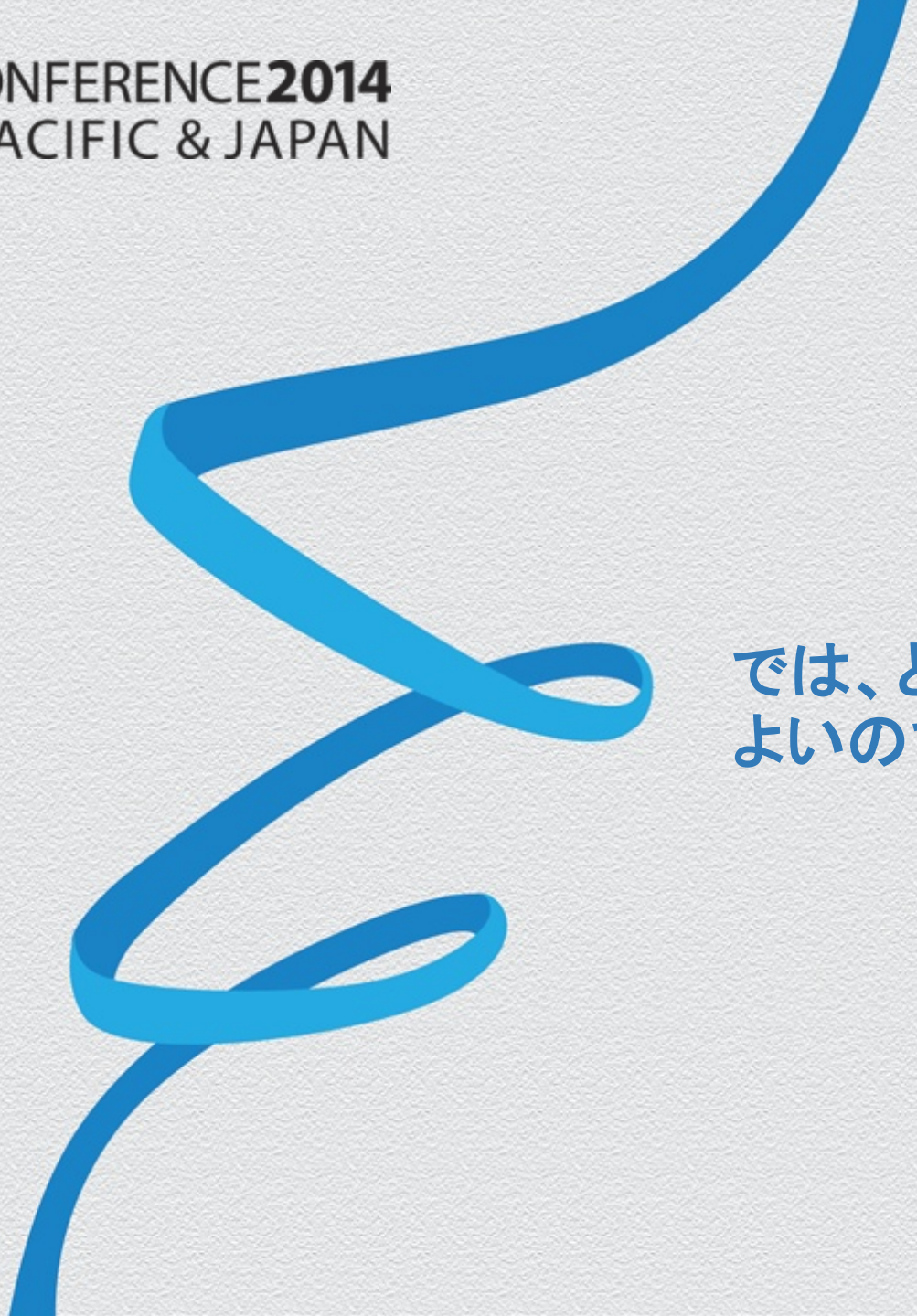
The authors of the Bugat Trojan are coming in late to the game, Kessem said. Zeus-in-the-mobile attacks are documented as far back as 2010. Security firms have been closely monitoring threats to mobile devices and see much of the mobile malware activity, a tiny fraction of the overall malware landscape, in Eastern Europe, Russia and Asia. Banking Trojans that hijack two-factor authentication are among the most dangerous attacks. Meanwhile, SMS Trojans that silently rack up premium text messaging charges are also a growing threat.

The main threat from Bugat and other banking malware is on the desktop, where the Trojan attempts to hijack the victim's browser session. It spreads via the Black Hole automated attack toolkit. The mobile functionality is triggered when two-factor authentication is requested to verify the victim's identity. Victims are then prompted by the cybercriminals to download the BitMo mobile malware to their Android, BlackBerry or Symbian phones as a result of a newly implemented data encryption policy instituted by the victim's bank.



チャネルが再統合されている場合は特に脆弱

Webアクセスおよびテレフォニーに対して同じデバイスが使用されている場合



では、どのようにすれば
よいのでしょうか。

マルウェア

- 新世代のトロイの木馬の出現
- キーストロークのログ、スクリーン グラバー、コール転送
- 例:
  - ZitMo（Zeus、モバイル内）
  - SMS Zombie
  - Perkel
  - Wroba
- 多くの人がマルウェアを話題にしている
  - ただし、それは使用されている手法の1つに過ぎない！

標的に電話する
電話会社になりすまして
電話をかける

話を信じ込ませる
「電話回線に
問題があります…」

解決策を提案する
次の番号を入力して
ください…

**入力された番号が
電話に転送される**
コールとテキスト

不正をはたらく
セキュリティ コードが
不正行為者に送信される

標的のソーシャル エンジニアリング

新たな解釈が加えられた従来の不正

インサイダー詐欺

- 電話会社の共犯者が着信コールと受信テキストをリモートでリダイレクト
  - オペレーター間？
- 不正の後に電話をリセット可能
  - 不正行為後の追跡が困難を極める

SIMのスワップ

- SIMカードを変更するいくつかの正当な理由
  - 新しいタイプの電話
  - 故障または紛失
  - サービス プロバイダーの移動
- 新しいSIMの挿入時に古いSIMがロックされる

標的をフィッシングする
セキュリティQ&Aなどの調査

https://www.youtube.com/watch?v=F7pYHN9iC9I

公共料金の請求書を入手する
共有玄関、ごみ箱、オンライン請求

電話ショップに行く
経験の浅いエージェントを選ぶ

ズタズタのSIMカードを見せる
「ペットの犬が食べてしまいました」

新しいSIMを挿入する
標的の電話が犯罪者の手におちる

不正をはたらく
セキュリティ コードが不正行為者に送信される

SIMスワップ不正

サプライ チェーンのソーシャル エンジニアリング

両方のチャネルを「おとす」

- パスワードを攻略
  - マルウェア
  - フィッシング
- 電話を攻略
  - マルウェア
  - SIMのスワップ
  - ネットワーク コール転送

- 両方のチャネルをおとす

ぞっとする話

- http://www.bbc.co.uk/programmes/p00ylgk7

- 携帯電話に電波が入らないことに気が付きました
- 「4,500ユーロ（7,500米ドル）が銀行口座から引き出されていました」
- 「家に電話したら、東ヨーロッパ訛りの男が電話に出ました」

ニュースで紹介された例…

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

Money › Banks and building societies

Hacking case exposes potential flaw in Halifax and Lloyds' security

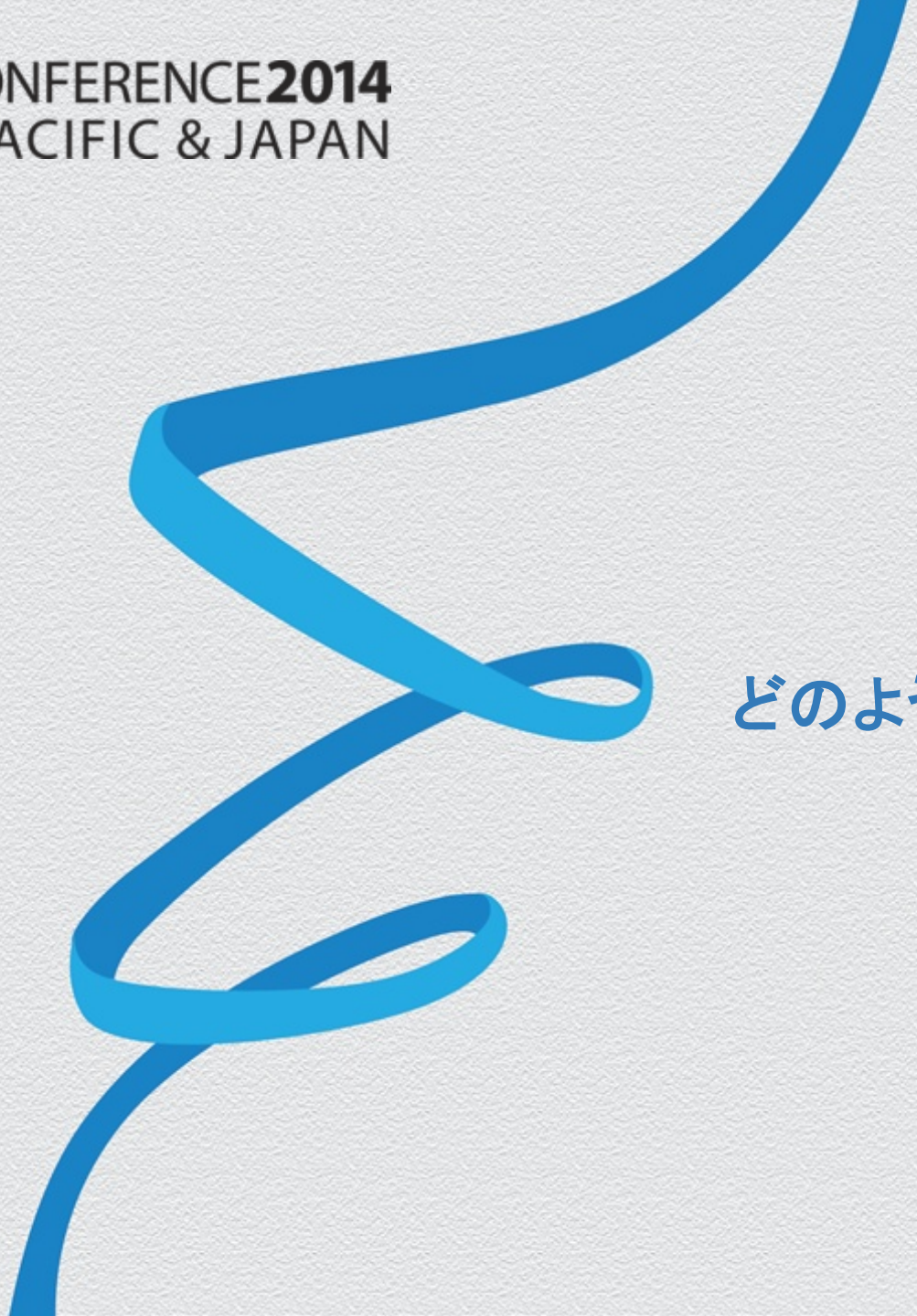
Hackers have found a way to get round a crucial step in Halifax and Lloyds online safety check

Miles Brignall
The Guardian, Friday 30 May 2014 10.43 BST
Jump to comments (42)

A reader exposes a bank security flaw. Photograph: Alastair Grant/AP

A Guardian Money reader has exposed a potentially major flaw in the security of the 22m current accounts operated by Lloyds and Halifax after hackers attempted to empty his account of £7,200.

- http://www.theguardian.com/money/2014/may/30/halifax-lloyds-banking-online-security-ハッカー
- オンライン アカウント所有者に対する銀行の極めて重要なセキュリティチェックの1つを回避する方法を不正行為者が開発しました。
- こうした不正行為者はBT（地域の電話会社）に連絡して、電話を自分達の携帯電話に転送するようにリクエストしており、さらにアカウントをすでにハッキングしていたため、コードは入力できました。



どのように防御しますか？

テレフォニー不正チェック

「ライブ不正チェック」で行うこと

SIMのスワップ

- SIMカードごとに一意のコードがある
  - IMSI –「International Mobile Subscriber Identity」
- このコードが変更された場合、それは新しいSIMカードが発行されたから

- これが行われる正当な理由がある
- ただし、その場合も十分に気を付ける必要がある

コール転送

- 電話ネットワーク スイッチング システムは、電話が転送されたかどうかを認識する
  - 確認するために実際に電話する必要がない

- これには正当な理由がある
  - 留守番電話へ転送
  - 固定電話から携帯電話へ転送
- ただし、注意が必要

メリット

- 電話システム エキスパートが不要
  - 電話システムに下位レベル アクセスする必要がない
  - 下位レベル スイッチング プロトコルを理解する必要がない
  - さまざまな多くの電話会社に統合する必要がない
- SaaSソリューションが使用可能
  - お客様に電話をかける前にSOAPコール
  - そのコールを信頼するかどうかに関する信頼因子を取得
- また、一部のコール センター ソフトウェア プロバイダーは、テレフォニー不正チェックをソフトウェア内からオプションとして統合する

結論

- 銀行やその他のセキュア サービスの多くが、セカンダリ認証用の個別のセキュリティトークンよりもテレフォニーをお客様が好むと考えている
- 不正行為者は一連の手法で対応して、テレフォニー チャネルを侵害した
- 現時点では、テレフォニー チャネルを保護し、不正行為者の先を行くための手法が存在する
- 次に何が来るか？

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

ありがとうございます

質疑応答