

## 個人に牙をむくサイバー攻撃… 狙うは、ずばり「お金」です

トレンドマイクロ株式会社  
リージョナルトレンドラボ  
木村 仁美

# 自己紹介

- 木村 仁美 (きむら ひとみ)
  - 電子認証/PKI
  - オンライン銀行を狙うマルウェア

4月 17 OpenSSL の HeartBleed脆弱性に対し、我々が注意すべきこと  
by セキュリティスペシャリスト 木村 仁美



7月 10 法人ネットバンキングを狙う電子証明書窃取攻撃を解明  
by セキュリティスペシャリスト 木村 仁美

★★★★☆ (9 投票, 平均値/最大値: 3.22 / 5)

ブックマークへ追加  

昨年 2013年を通じ日本国内において最大の脅威となったのは、「オンライン銀行詐欺ツール」  
たらされる脅威はさらに凶悪化し拡大しています。これまで、ネットバンキングを通じた不正送  
とみられてきましたが、現在では法人に対する被害も確認されています。

多くの法人向けネットバンキングでは、認証強化のために「電子証明書」による SSL/TLSクライアント認証が導入されています。正しい



社会生) になった) はず、ま  
トレンド  
Faceb)  
の有料  
れる、新  
カウント

# Agenda

- 狙われる個人のお金
- 最近の流行
  - ワンクリック詐欺
  - ランサムウェア
  - グレーウェア・アドウェア
  - オンライン銀行詐欺ツール
  - おまけ
- まとめ
- 身の守り方

# 狙われる個人のお金

- × ~~サイバー犯罪者がサイバー犯罪をやっている~~
- 「犯罪者が効率を上げるためにサイバー犯罪をやっている」 と思ってもらうほうが自然

# 消費者シーンでの流行

- エッチな画像をデスクトップに出して脅迫するもの
  - ワンクリック詐欺
- 写真を暗号化して脅迫するもの
  - ランサムウェア
- いつの間にかいる邪魔なもの
  - グレーウェア・アドウェア
- オンラインバンキングから自動で送金するもの
  - オンライン銀行詐欺ツール

すべてが  
金銭  
目的

# ワンクリック詐欺

- 日本特有。これを語らずして何を語るか

**有料アダルトサイトへのご入会ありがとうございます。**

有料アダルトサイトへご入会が完了し、**お客様ID番号**を発行しました。ご入会前に利用規約及び確認ページにて確認しました通り、ご入会と同時に**ご利用料金**が発生しております。期限内にお支払い下さいますようお願い申し上げます。お客様のご入会情報は登録情報確認ボタンを押して頂くことで確認出来ます。また、ご不明な点などございましたらお問い合わせボタンのメールフォームよりご連絡下さい。

※この画面は**お客様ID番号**でのご入金確認後に消えます。  
※ご入金の際は、振込み名義を**お客様ID番号**でご記入下さい。  
お名前でのご入金ですとこの画面が消えない場合がございます。

**キャンペーン実施中**

**お客様登録情報**

**お支払いについて**

**動画ページ**

**お問い合わせ**

**お電話でのお問い合わせはこちら**  
平日 10:00~20:00 土曜日 11:00~18:00  
定休日 日曜日・祝日

お客様ID番号	[blurred]
ご入会日時	2014/06/05 15:21:06
お支払い期限	2014/06/12 ※ただいま割引期間中

# ワンクリック詐欺

- 詐欺なのでくれぐれもお金を払わないように！
- 無視するのが一番。連絡先を渡さないこと。

## [参考]

- 国民生活センター

あわてないで!! クリックただけで、いきなり料金請求する手口

<http://www.kokusen.go.jp/news/click.html>

→なんと、2004年12月13日に公開された歴史あるページです

- 総務省

国民のための情報セキュリティサイト – ワンクリック詐欺に注意

[http://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/security/enduser/security01/06.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/06.html)

# ランサムウェア

- 盛り上がりを見せた「暗号化型」



企業の業務用PCが感染し  
ネットワークドライブのファイルが  
軒並み暗号化される事例も  
観測されています…☠



# ランサムウェア

- 警察を装いPCをロックする手口も引き続き観測

**PCEU** Police Central e-crime Unit  
Specialist Crime Directorate  
**Police Central e-crime Unit**

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of **100 GBP**.

All activity of this computer has been recorded  
If you use a webcam, videos and pictures were saved for identification

Video-recording: **ON**

You can be clearly identified by resolving your IP address and the associated hostname  
**Your IP Address: 103.5.6.195**  
**Your Hostname: PH-02019.dlsc-ms.org**  
**Location: Philippines, Gulbarga**

**Your Computer has been locked!**

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.  
Described below are possible violations, you have made:

**Article 274 – Copyright**  
A fine or imprisonment for the term of up to 4 years (The use or sharing of copyrighted files – movies, software)

**Article 183 – Pornography**  
A fine or imprisonment for the term of up to 2 years (The use or distribution of pornographic files)

**Article 184 – Pornography involving children (under 18 years)**  
Imprisonment for the term of up to 15 years (The use or distribution of pornographic files)

**Article 104 – Promoting Terrorism**  
Imprisonment for the term of up to 25 years (You have visited websites of terrorist organizations)

**Article 297 – Neglect computer use, entailing serious consequences**

1. 2. 3. 4.

**Ukash**  
You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.

Where can I buy Ukash

Exchange your cash for a Ukash voucher and use your voucher code in form below.

Code:   
1 2 3 4 5 6 7 8 9 0

**paysafecard**  
Paysafecard is available from 450,000 sales outlets worldwide, in the United Kingdom, exclusively from all PayPoint outlets

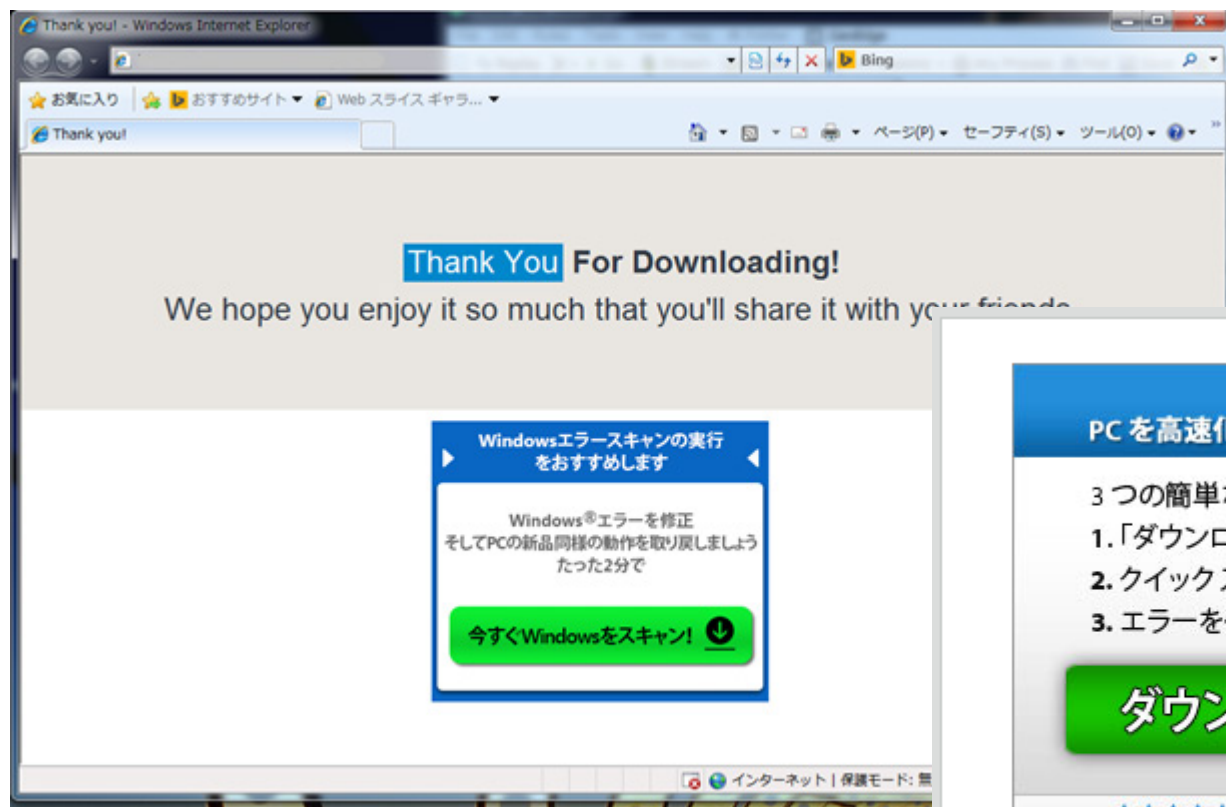
Where can I buy Paysafecard

Exchange your cash for a Paysafecard voucher and use your voucher code in form below.

# グレーウェア・アドウェア

- いつの間にかいる

Flashを  
インストールした  
つもり



Web広告  
として出ている

広告

推奨事項

PCを高速化するための3つのステップ

3つの簡単なステップ:

1. 「ダウンロードを開始」をクリックします。
2. クイックスキャンを実行します。
3. エラーを修復します。

**ダウンロードを開始**

★★★★★  
5つ星評価を100件以上獲得

# グレーウェア・アドウェア

- 日本の検出数TOP10を独走するアドウェア (当社SPN調べ)
- ためしにTOP3は何かというと… (2014年第3Q集計／当社SPN調べ)

順位	検出名	数
1	ADW_INSTALLCORE	314,000
2	ADW_OPENCANDY	74,000
3	ADW_SENSAVE	49,000

- ちなみにアドウェアを除いたTOP3は… (2014年第3Q集計／当社SPN調べ)

順位	検出名	数
1	JS_AGENT.APS	17,000
2	JS_NEVAR.A	16,000
3	WORM_DOWNAD.AD	2,000

# オンライン銀行詐欺ツール

- バンキングマルウェア/トロロジャンとも呼ばれる
- Webインジェクションと呼ばれる手法で猛威を振るう
- 2013年6月に日本へ本格上陸
- 2014年、ついに自動送金機能が観測された
- 例) ある検体の標的
  - 国内の銀行 17行
  - クレジットカード会社 20社
  - インターネット通信販売会社 2社

# オンライン銀行詐欺ツール

- 新しく観測されているものの特徴 (VAWTRAKファミリー)
  - 感染してしまうと、かつての護身術が通用しない
    - お気に入りからアクセスしているから大丈夫
      - 正しいURLにアクセスしている
    - アドレスバーが緑色だから大丈夫
      - EV SSLサーバ証明書もちゃんとみどり (検体の種類によるが)
    - SSLクライアント証明書を使っているから大丈夫
    - ワンタイムパスワードトークンを使っているから大丈夫

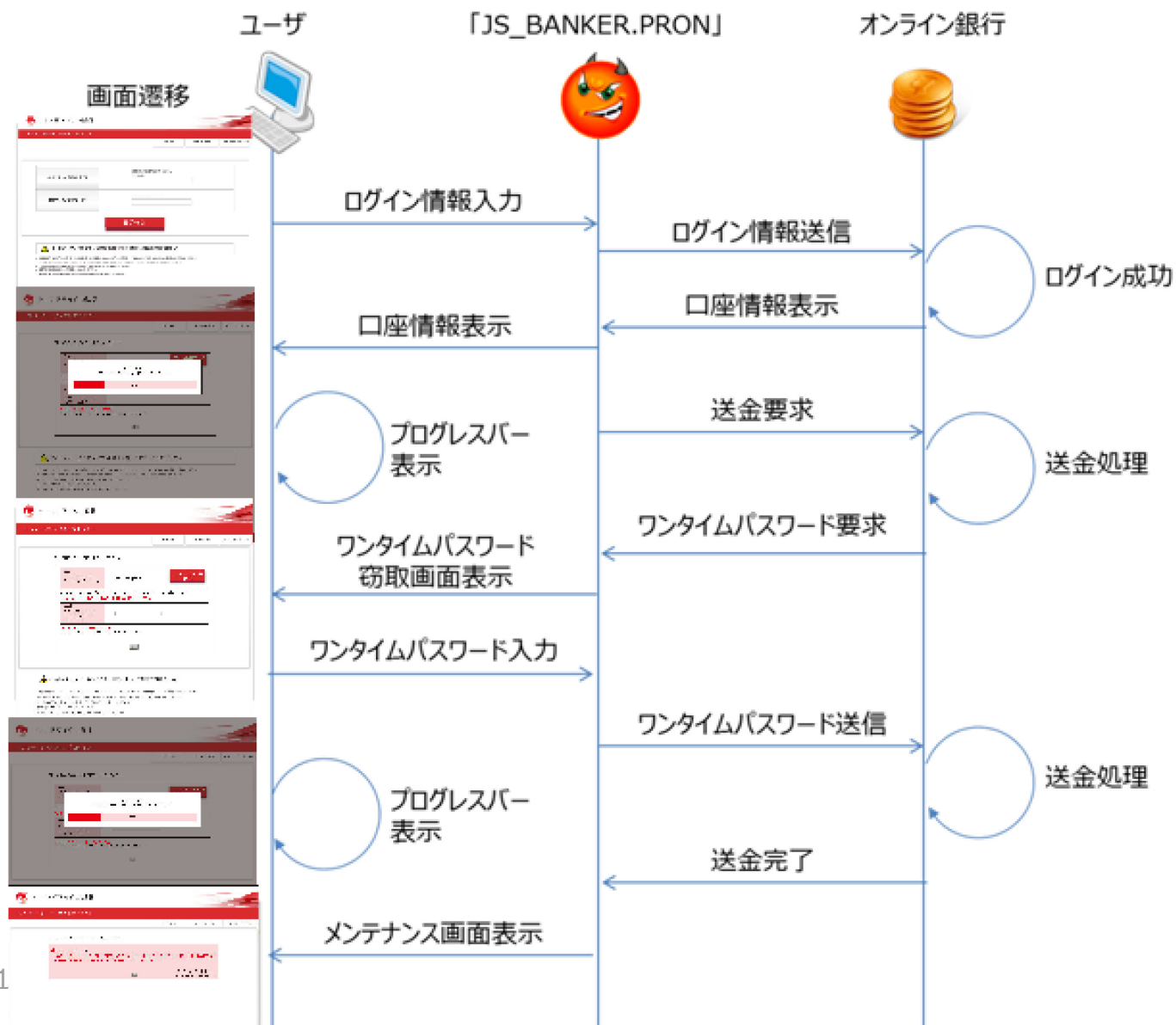
→すべて通用しません…

# オンライン銀行詐欺ツール

- ユーザー体験はこんなふう (VAWTRAKファミリー) :  
ブックマークからオンライン銀行にログインしたら、なんかステータスバーが表示されて、しばらくしたらメンテナンス画面が表示された。後日確認したら、残高がほぼ0に！



# オンライン銀行詐欺ツール



# おまけ：DOWNADの話

- 未だ検出上位のDOWNAD

順位	検出名	数
1	JS_AGENT.APS	17,000
2	JS_NEVAR.A	16,000
3	WORM_DOWNAD.AD	2,000

アドウェアを除いた国内検出TOP3(2014年第3Q集計/当社SPN調べ)

- 近年珍しい、大規模拡散型のウイルス
- これが出たらとにかく面倒くさい
- パッチが不十分なWindowsXPに主に感染します
- 出入りの業者の**USBメモリ**が怪しい！



# まとめ

- うわ～！ウイルスに感染してしまった！
  - 特に慌てる必要ないです (DOWNAD以外は)
  - パッと見て変な動きをしているようなら対応は簡単
    - ワンクリック詐欺は無視して削除すればいいだけ
    - アドウェア・グレーウェアも、削除すればいいだけ
      - ウイルス対策ソフトが駆除したらそれでOK
  - 写真を暗号化されてしまった
    - 来る日に備えて、今日この後すぐバックアップを取ろう！
      - 「バックアップ大事」と君が言ったから、11/19はバックアップ記念日

# まとめ

- 本当に怖いウイルスは派手な動きをしません
  - 「バックドア」
    - 企業の業務パソコンなどに感染し、情報窃取を狙う
    - 画面上、動作上変化がないので感染に気付かない
    - ひっそり入ってきて、ひっそりとずっといる
    - これはまた、別の話…。

# 身の守り方

- 王道しかないんです

面白くなさ過ぎて今さら改めて言いづらい

- パッチを当てる

- OS・ブラウザ・Java・Adobe Reader・Flash などなど

- ウイルス対策ソフトのパターンを最新にする

- 実行ファイルを実行するときは出所に注意する

- OKボタンを連打しない

- メールの添付ファイルやリンクは開かない

- 怪しいサイトに行かない