【NEZU システム通信】

(Vol.0052)　　発行日 2014.7.18

▼　ごあいさつ　▼　　日頃は **NEZUGROUP** とお取引頂きまして、誠にありがとうございます。

今回の NEZU システム通信は、　①　鉄鋼関連情報(社団法人鉄鋼連盟 2014 年 6 月発表)

②「中に人がいる、しかも悪人が（マン･インザ･ブラウザ攻撃)」についてお届け致します。

①　鉄鋼関連情報

下記 URL より社団法人鉄鋼連盟が発表した『 鉄鋼需給の動き 2014 年 6 月 』の資料を閲覧することが出来ます。(次回公表は 7 月下旬予定です)

http://www.jisf.or.jp/data/jyukyu/documents/jyukyu1406.pdf

②中に人がいる、しかも悪人が（マン･インザ･ブラウザ攻撃)

気がつけば口座残高がゼロ！　(2013 年のネットバンキング被害は 14 億円超に)

法人のインターネットバンキング(以下、バンキングと記述)　被害が多発しています。

これまでの被害は個人口座が中心でしたが、最近は企業などの法人口座が狙われるケースが増えています。三菱東京 UFJ 銀行や福岡銀行など 10 行程度で被害が確認されています。件数は個人に比べれば少ないものの、法人口座は預金額が大きいため、被害額が 1000 万円以上に上るケースも出ています。

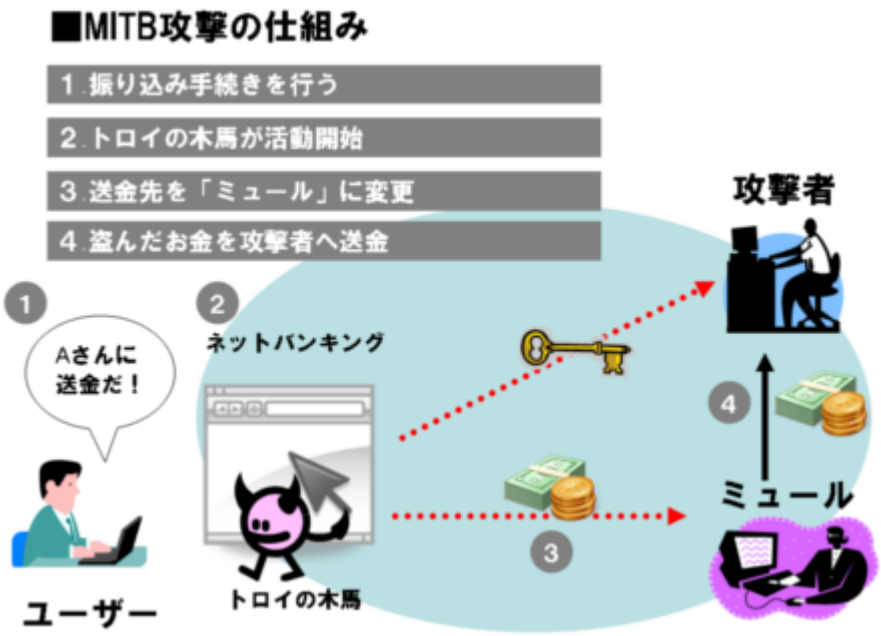
■マン･インザ･ブラウザ(MITB)攻撃■

（意味：ブラウザの中に悪人がいる。）

マルウェア(注1)は感染した PC の Web ブラウザ(注2)を監視し、ユーザーのバンキングのログインが成功すると、不正利用者はブラウザを乗っ取り、送信される情報を改ざんします。

例えば、ユーザーの送金手続きを検知すると、その送金先を、攻撃者が指定した口座（右図ではミュール（運び屋））に変更します。

この点が従来のバンキングの画面に暗証番号を入力させて情報を盗み取る「なりすまし詐欺」と異なる点です。



ユーザーが正しい送金操作を行ったつもりでいても、その裏側で変更されてしまうために被害に気付くのが難しい点が指摘されています。また、マン･インザ･ブラウザ攻撃に使われるマルウェアは、銀行とのユーザー認証が成功した後のブラウザを乗っ取るため、通信の暗号化や、ワンタイムパスワード(注3)などの強固なユーザー認証を導入していても防げない可能性が高いといわれています。

(注 1) マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なプログラムコードの総称

(注2) インターネット上の情報を閲覧するためのアプリケーションソフト

（注 3）ワンタイムパスワードとは、使い捨てのパスワード。パスワード発生装置が毎回違うパスワードを表示。

インターネットバンキング専用の無料ソフト

最近、多くの金融機関が、「Rapport(ラポート)」というバンキング専用のウィルス対策ソフトを利用者へ導入案内を始めています。　＜バンキング　ラポートで検索＞

また同じように、「PhishWall（フィッシュウォール)」という対策ソフトもあります。

多くの金融機関が、バンキングの不正操作対策を呼びかけています。詳しくは金融機関にご相談下さい。

http://www.trusteer.com/ja/products/trusteer-rapport-for-online-banking-ja

http://www.securebrain.co.jp/products/phishwall/

最強の仕組み：トランザクション認証

住信 SBI ネット銀行では「スマート認証」というトランザクション認証のサービスを始めました。

この仕組の動きは、バンキングで振込等の重要操作をする場合には、振込処理をした後に、その取引内容が銀行側からスマートフォンに表示され、利用者はその内容を確認し、確認ボタンを押すと処理が実行される仕組みです。この仕組なら、マン･インザ･ブラウザ攻撃を受けて、振込先や金額を改ざんされても、スマートフォン側で変更された内容が表示されるので実行前に気づく事が出来ます。

最後は利用者の日頃の対応

銀行のトップページには最新のバンキング対策の情報が掲載されています。どのような手口で情報を盗み取ろうとしているか、対策等詳しく説明がありますので閲覧する事で情報収集になります。

http://www.bk.mufg.jp/info/phishing/20131118.html?link_id=p_top_juyo_mail

http://www.smbc.co.jp/security/popup.html

またウィルス対策ソフトの導入は当然ですが、各種ソフトのマメなアップデート、オンラインバンキングに専用 PC を用意するなど、ユーザーの自主的な行動が一番の対策になります。

■ 編 集 後 記 ■

こんにちは。情報システム事業部の樋口です。

今回の記事を作成している内に、自分のバンキング操作も不安になり、暗証番号表からワンタイムパスワードに変更したり、スマート認証を導入しました。

先日コンビニ ATM で現金を下ろそうとしたら、何度やっても「お問い合わせ下さい」と表示され引き出せませんでした。実はバンキングのセキュリティでキャッシュカードの利用のロックをかけている事を忘れていました。今後はこのような事がないように、キャッシュカードに大きくロック中とマジックで記入しました。セキュリティーをかける程、不便になっていきます。しかし今の世の中、自己防衛するしかありません。

発　行：根津鋼材　株式会社　　住　所：〒116-0014 東京都荒川区東日暮里 1-32-5　(TEL)03-3805-5555
メール：hp-master@nezu-g.co.jp　ホームページ：http://www.nezu-g.co.jp/
発行人：根津訓光／監修　樋口良成／編集長
編　集：情報システム事業部