4E-08

インターネットバンキングの不正送金対策

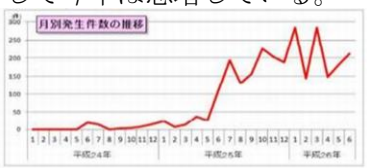
佐野　宏明†　　田中　英彦‡
情報セキュリティ大学院大学‡

1. はじめに

インターネットバンキング（以下ネットバンキング）は利便性が優れている事から利用者は年々増加しており、現在の契約口座件数は約6,500万にもおよぶ。

ただし、便利なシステムが普及することで、不正を行う者も増えている。図１から判る通り、年々発生件数・被害額共には増加している。また、平成25年下期に比べ、多くの地方銀行や信用金庫・信用組合にも拡大しており、日本の銀行が攻撃対象になっている。さらに口座種別をみると法人名義口座に関する被害が昨年はほとんどなかったのに対して今年は急増している。

期間	件数	被害額
H26上	1,254	約18億5,200万円（約148万円/件）
H25下	1,098	約11億9,300万円（約109万円/件）
H25上	217	約2億1,300万（98万円/件）



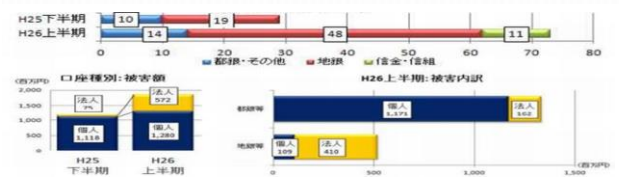


図１：平成26年上半期のインターネットバンキングにおける不正送金事犯の発生状況
（出所：警察庁）

2. 不正送金の攻撃手法

不正送金を引き起こす攻撃手法として、フィッシングサイト攻撃系と中間者攻撃系がある。

フィッシング攻撃系とは、偽サイトに導くなどしてIDとパスワードを盗んで、別の端末・セッションから成りすましを行うもののことを言い、２パターンの攻撃方法がある。

１つは銀行を装った偽のメールを送るなどして、巧みにニセのサイト（フィッシングサイト）へと誘導する方法。もう１つは、パソコンをマルウェアに感染させることにより、ネットバンキング利用時に、銀行を装ったニセのサイトを表示させる方法である。

Consideration of measures for online banking fraud
Hiroaki Sano†,Hidehiko Tanaka†
†INSTITUTE of INFORMATION SECURITY

中間者攻撃系とは、利用者と銀行の間に入り、セッションを乗っ取り、送金先・送金額を変える方法である。

3. 不正送金対策

各銀行は不正送金の被害を減らすため、様々な対策を施している。今回その一例を図２に示す。図からわかるように、不正送金対策を複数個合わせて行なうことでより強固な対策を行っていることが判る。

銀行名	セキュリティ内容						
	乱数表・合言葉	画面キーボード	ウイルス対策ソフトの提供	通知Eメール	ニ経路認証	ワンタイムパスワード	リスクベース認証
A銀行	○	○	○				
B銀行	○	○	○	○	○		
C銀行	○	○	○	○			○
D銀行	○			○			
E銀行	○	○		○			
F銀行				○		○	
G銀行	○	○		○		○	○
H銀行	○	○	○	○		○	
I銀行	○	○		○		○	○
J銀行	○	○	○	○		○	○
K銀行	○	○	○			○	○
L銀行	○	○		○		○	

図２：各銀行のセキュリティ対策

4. 近年の不正送金事例

図２の様にセキュリティ対策を行っていても、不正送金事例は後を絶たない。近年では Zeus、SpyEye などの Banking trojan といわれるネットバンキングに特化した高機能不正プログラム（マルウェア）による被害が全世界で深刻となっている。また、従来安全と言われていたワンタイムパスワードによる対策も破られる事例が日本でも起こった。

その攻撃手法は、MITB（マン・イン・ザ・ブラウザ）攻撃という手法で、これは先ほど述べた中間者攻撃系の１つで利用者のパソコンにマルウェアが侵入しパソコンを乗っ取るといものである。

MITB 攻撃には、２つのパターンがありＰＷ（パスワード）窃取型と取引改ざん型がある。

ＰＷ窃取型とは、サーバから返却された正規の画面に対して、不正な画面やスクリプトを挿し込み、ＰＷを窃取する。

取引改ざん型とは、取引ＰＷは正規のものをそのまま利用し、取引内容（振込先、金額）をマルウェアが改ざんする。

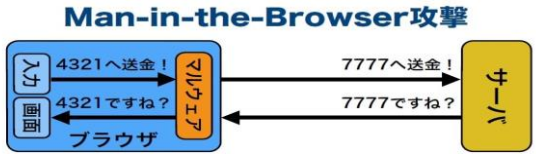


図３：MITB の攻撃方法
（出所：産業技術研究所）

この MITB 攻撃を行うマルウェアの侵入方法には偽メールとサイト経由による２つがある。

偽メール経由での感染とは、攻撃者が有名な企業や利用者にゆかりのある企業名を名乗り、メール内の URL や添付ファイルを実行することで感染させる。

サイト経由での感染とは、攻撃者が第三者のサイトを乗っ取り、利用者がそのサイトにアクセスした瞬間に感染する。

こういったサイトの改ざんはサイトの管理人等により改ざんを検知し元に戻るが、最近ではサイト内にある広告や画像にマルウェアを仕込んでおき、改ざんをばれにくくする手法もとられている。

5. 海外の状況

日本に対する不正送金の攻撃手法は海外で起きた攻撃手法が数か月～数年後に使われる傾向がある。MITB 攻撃を例に見てみると、2009 年に欧米で確認され、2011 年に南米・ロシアと拡大している。海外においては、不正送金の被害は、2012 年頃には欧州、ドイツ、オランダで、2,000 億円の被害が出ている。

現在、国外の被害を見る限りでは MITB 攻撃より新しい攻撃手法は出ていないが、それを行うマルウェアは日々高度化かつ増加している。2012 年の不正送金には Operation High Roller というのは Zeus や SpyEye をベースに、さらに進化したものが出た。また、攻撃者は無作為にターゲットを選ぶのではなく、富裕層に絞るなどといった様に効率よく収益を得るように工夫を凝らしてきている。

ただ、平成 26 年 4 月～6 月には、日本での従来タイプを含めた不正送金マルウェアの検出件数が世界の 24%に上り、米国（14%）を抜きトップとなった。つまり、今までは国外の動向をチェックしていればある程度予想ができた事が出来なくなる。これは、攻撃者が米国から日本に標的を移し、まず日本を狙っているといえる。

6. 不正送金に対する補償

現在の不正送金に対する補償割合を図４に示すように、9 割以上は保障を行ってはいるが全件補償していないも現状である。これは銀行側が利用者に対し「責任」を求めているという意味がある。

	件数	補償件数	割合
平成23年度	87	84	96.60%
平成24年度	101	95	94.10%
平成25年度	956	946	99.00%
平成26年度4～6月	148	138	93.20%

図４：不正送金被害に対して補償を実施した割合
（出所：全国銀行協会）

7. 考察

今まで不正送金に対する攻撃手法等を述べてきた。現在主流である MITB 攻撃に対して有効とされる対策に二経路認証がある。

二経路認証とは、利用者のスマートフォンなどパソコンとは別の端末を利用して、パソコンで入力した取引認証とは別の経路での取引認証を実施する。これにより、別端末で取引認証の通知があり、取引内容も確認できるため、不正にすぐ気付くことができる。種類として内容確認型と取引情報ＯＴＰ（ワンタイムパスワード）型がある。

内容確認型は、別媒体に取引内容の情報が送付され、利用者自身で不正に気が付く。

取引情報ＯＴＰ型は、手元の専用機器で、取引内容を元にＯＴＰを作成し、認証を行い、もし不正がある場合はサーバ側で検知する。

この対策方法が日本の銀行で徐々に導入されているが、ほとんどの銀行では従来の対策しか施されていないし、導入されていても任意の所が多い。

利用者にとっても二経路認証の有用性を理解している人は少なく、せっかくある対策を蔑ろにする可能性がある。そこで、私はこの対策の提供と利用者に対して説明・教育、知らない人・意識の薄い人に対しては周知をするという３つを行うことが必要であると感じる。

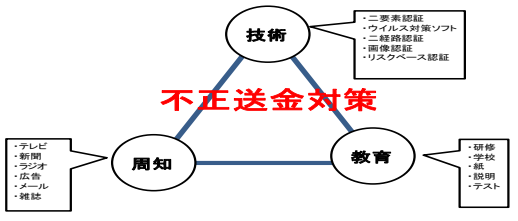


図５：３側面からの対策

8. まとめ

最後になるが、近年若者のパソコン離れが進んでおり、ネットバンキングもパソコンからではなくスマートフォンからの利用が増えていくだろう。銀行も利便性の面から専用アプリの配信をしている。つまり、今後はスマートフォンに対する攻撃が更に増加すると考えられる。その攻撃にどう対処するのかを少しでも早く考えることが不正送金を未然に防ぐ方法だと考える。