6V-06

標的型メール攻撃対策のための自動訓練メールクライアントシステム

岩田　一希† 中村　嘉隆† 高橋　修†

†公立はこだて未来大学　システム情報科学部

1. はじめに

近年，企業の一個人を対象として，マルウェアを添付したメールや，悪性サイトの URL を添付したメールを送信し，マルウェアをダウンロード・実行させて感染させ内部情報の流出などを行う標的型メール攻撃による被害が増大している[1][2]．2015 年 6 月には日本年金機構が標的型攻撃により大規模な情報流出を起こしていることもあり，今日対策されるべきサイバー攻撃となっている[3]．この攻撃について，マルウェアが侵入しないようにする対策を「入口対策」と呼ぶ．「入口対策」の課題として，この攻撃に使用されるマルウェアは既存の対策ソフトでは検知できない場合が多いという点，またマルウェアへの防御システムは基本的に既知の攻撃にしか対応できない点がある．この課題に対する解決手段として，「人間」に擬似的に攻撃を受けさせ，攻撃に対する訓練をすることで，標的型メール攻撃への耐性をつけるという対策がある．JPCERT/CC が 2008 年に行った標的型メール攻撃に対しての訓練についてのレポートによると，訓練手順は以下のとおりである[4]．

1. 訓練の予告
2. 標的型メール攻撃についての教育
3. 訓練メール配信(1 回目)
4. 訓練メール配信(2 回目)
5. 事後アンケート
6. 種明かし

この訓練によって標的型メール攻撃に対しての訓練には効果があることが証明されている．

2. 関連研究

上記の訓練を応用した関連研究として，標的型メール攻撃を「病原体」と仮定し，それに対する「予防接種」として，擬似標的型攻撃メールを作成し，そのメールを使って人間を訓練することによって，攻撃への耐性向上を図る研究[5]や「標的型メール攻撃の被害に合う」リスクを人がどのように感じているのかを標的型メール攻撃の訓練を利用して検証する研究[6]がある．これらの関連研究の課題として，訓練回数が2回のみであり継続することを考えられておらず，次第に訓練の効果が失われ，攻撃の被害を受けやすくなってしまう点，継続性がないため，訓練をすることで収集できるデータ(訓練データ)を収集できる機会が少なくなり，被訓練者にとってもっとも効果的な訓練を行うことができない点が挙げられる．

3. アプローチ

関連研究で挙げた問題点は，継続的に訓練を実行できる環境を構築することによって解決できる．継続的な訓練によって，個人の訓練の結果を収集・分析することで訓練をより個人に合わせたものにし、訓練の効果を高めることできる．本研究ではこれらを実現するために，自動で継続的に訓練を行うメールクライアントシステムを提案する．

4. 自動訓練メールクライアントシステム

本研究で提案するシステムは図 1 のように構成される．提案システムのユーザを「ユーザ A」とした時，ユーザ A が直接操作するのはメールクライアントの部分である．その他には訓練データを蓄積するサーバが別にあり，一定のタイミングでメールクライアントとデータの送受信をしている．また，メールクライアントは訓練メールを自動生成するツールを内蔵している．

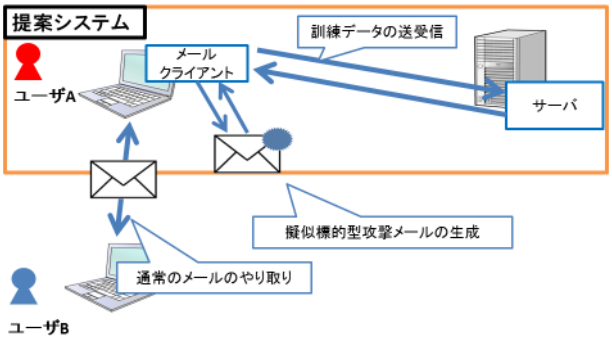

図 1：システム構成図

"Mail client system for automatic training against Advanced Persistent Threat"
Kazuki Iwata†, Yoshitaka Nakamura†, Osamu Takahashi†
†School of Systems Information Science, Future University Hakodate

4.1. メールクライアント

メールクライアントでは，通常のメールのやり取りや，メールの閲覧が可能になっている．また訓練用の標的型攻撃メールをクライアント側で作成し，それを表示して訓練をすることができる機能や，訓練データを収集するサーバに訓練の結果を送信する機能を持つ．さらには受信 BOX のメールを解析し，それを訓練用の標的型攻撃メールを作成するのに活用する機能を搭載している．受信メール解析を行うことにより，ユーザがどのようなメールを信頼して開封しているかを調べることができる．

解析の方法としてまず，メールをメールヘッダ部分と本文部分に分割する．メールヘッダの情報から送信アドレスや，宛先アドレス，件名などの情報の他に文の書かれているタイプやエンコードの情報，さらには経由してきたサーバなどの情報を抽出する．これによってユーザが信頼しているメールの傾向を調べることができる．また本文については形態素解析を行い，メールの差出人の本名や内容，署名などを調べる．これによりユーザが普段多くやり取りしている人物とどのような内容でやり取りを行っているのかを調べることができる．

4.2. サーバ

メールクライアントから送られてきた訓練データを蓄積する．一人のユーザについて以下の 4 種類のデータを蓄積する．

1. 訓練メール開封の有無
2. 訓練の総計回数
3. 前回訓練時からの経過日時
4. 訓練メールのマルウェアの侵入源
5. 訓練メールだと気づく点の位置
6. 訓練メールだと気づく点の個数

1, 2 のデータを分析すると，このツールを使った訓練の効果を検証することができる．1, 3 のデータを分析すると，訓練と訓練の間をどれくらい空けると，最も効果的な訓練の間隔を検証することができる．1, 4, 5, 6 のデータを分析すると，ユーザが開封しやすい標的型メールの傾向を調べることができると考える．

4.3. 訓練メール自動生成ツール

訓練メール自動生成ツールでは，クライアント側でメールの解析を行ったデータと，サーバ側で分析を行ったデータを使って，訓練メールを自動生成する．訓練メールを生成する際には上記のデータの他に，標的型攻撃メールだと気づくことができるポイントをメールに盛り込む[7]．このようにメールを自動生成することによって，繰り返し訓練を行う際に訓練メールを一から作成する手間を省くことができる．さらに個々人のメール情報や訓練のデータを利用して訓練メールを作成しているため，個々人に特化した訓練を行うことができる．これによってユーザは，自分の弱点への対策を行いながら，似たようなメールが送られてきた時に注意をしながら開封することができるようになると考えられる．

5. 今後の課題

提案システムを実現するために，現在プロトタイプの実装を行っている．プロトタイプではメールクライアントの通常の機能と，自動生成をする機能を実装する．これを使って，継続的に訓練を行う実験を行い，訓練を継続することの効果の検証を行う．

6. おわりに

本稿では，標的型メール攻撃への入口対策として，自動的に継続して訓練を行う事ができる，自動訓練メールクライアントシステムを提案する．提案システムでは，メールの解析結果や，訓練データの分析結果から，個人のユーザに特化した訓練を実行する．今後は，実装を完了し，実験により継続した訓練に効果があることを検証しようと考えている．

参考文献

[1]IPA, “2014 年度情報セキュリティ事象被害状況調査報告書,” http://www.ipa.go.jp/files/000043418.pdf, 2015/01, 最終アクセス:2015/11/10
[2]IPA, “2013 年度情報セキュリティ事象被害状況調査報告書,” http://www.ipa.go.jp/files/000036465.pdf, 2014/01, 最終アクセス:2015/8/10
[3]“年金機構の 125 万件情報流出 職員，ウイルスメール開封,” 日本経済新聞, 2015/6/1, 最終アクセス:2015/11/10
[4]JPCERT/CC, “2009 年度 IT セキュリティ予防接種調査報告書,” http://www.jpcert.or.jp/research/inoculation2009.html, 2011, 最終アクセス:2015/11/10
[5]伊藤史人，高見澤秀幸，佐藤郁也, “標的型メールの予防対策,” 学術情報処理研究, No.16, pp.100-110, 2012
[6]寺田剛陽，鳥居悟，安野智子，瀧澤弘和，新真知, “リスク認知に基づく標的型メール対策の検討,” 情報処理学会研究報告, Vol.2013-GN-88, No.9, pp.1-8, 2013
[7] IPA, “IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」,” https://www.ipa.go.jp/files/000043331.pdf, 最終アクセス:2015/11/18