doc, pdf, zip 拡張子を持つ金融機関を狙った マルウェアの解析とその考察

湯下　弘祐　　伊藤　俊一郎

奈良先端科学技術大学院大学情報科学研究科
630-0192 奈良県生駒市高山町 8916 番地の 5
{yushita.kosuke.yf5, ito.shunichiro.in0}@is.naist.jp

概要　標的型攻撃は特定の組織や情報を狙って機密情報などを窃取する攻撃である．標的型攻撃に用いられるマルウェアはその特性上，標的となる対象ごとに何らかの特徴や傾向があると思われる．本研究では，誰もが利用している金融機関を狙ったと思われるマルウェアのうち doc，pdf，zip の拡張子を持つものに焦点を絞って解析を行う．またより簡易な解析によりマルウェアの傾向を知るため，malwr にて検体を入手し解析ツールの viper で解析する．その結果，今回の検体において doc ファイルは 5 種類， pdf は 4 種類に大別でき， zip の中身の 73%は exe 系であった．

Analysis result of doc, pdf, zip file malware and its consideration

Kosuke Yushita　　Shun'ichiro Ito

Graduate School of Information Science，Nara Institute of Science and Technology
8916-5 Takayamacho，Ikoma，Nara 630-0192，JAPAN
{yushita.kosuke.yf5，ito.shunichiro.in0}@is.naist.jp

Abstract　Targeted threats aim at specific organizations to steal sensitive information. It can be said that the malware used in the targeted threat has different features depending on the target. In this paper, we perform an analysis focusing on malware with the .doc, .pdf and .zip extensions which can be thought of as aimed financial institutions which all people use. Our analysis tools were malwr and viper. Finally, we classified the files in this sample into several categories, namely: 5 categories of .doc files and 4 categories of .pdf files. We additionally found that 73%of .zip files were .exe files.

1　はじめに

近年ではサイバー攻撃手法の 1 つである標的型攻撃が複雑化・巧妙化し，個人から企業や官公庁に至るまで重大な脅威となっている．現に，内閣サイバーセキュリティセンター公表資料においても標的型攻撃による被害として，日本年金機構の情報流出事案や標的型攻撃数の増加が紹介され注意を促している [1].

標的型攻撃の特徴としては特定の組織や情報を狙って機密情報などを窃取することが挙げられる．この際，標的となる対象に合わせた電子メールを送りつけ，添付しているファイルを開かせてマルウェアを実行させる．そのため，攻撃においては対象に合わせたメールや添付ファイルが必要となる．このことから，標的となる対象ごとに標的型攻撃の特徴があると考えた．本研究ではインフラとして誰もが利用している金融機関に焦点を絞り，金融関連の単語をファイル名に含むマルウェアを解析ツールにより解析しその傾向を確認した．また従来のマルウェア解析においてはリバースエンジニアリングやサンドボックスによる研究が多く取り組まれてきた．しかし，本研究ではより簡易な解析によ

りマルウェアの傾向を確認できるかを目標に，実証的にファイル解析を行った．

今回調査した検体においては exe 拡張子が最も大きな割合を占めていた．しかし，exe 拡張子は一般的にメールの添付ファイルとしてやり取りをする場合が少なく，警戒して拡張子でフィルタリングすることも可能であるため，本研究では解析対象から除外した．一方，doc，pdf，zip 拡張子については exe 拡張子に続き大きな割合を占めており，かつ，一般的にメールの添付ファイルとして使用することも多いため，この 3 つの拡張子を持つファイルを本研究の解析対象とした．

2　関連研究

Wei-Jen Li らの研究も本研究と同様に Microsoft word の doc ファイルに焦点を絞りマルウェアの解析を行っている [2]．その研究の中で新たな脅威としてマクロについて言及しているが，マクロ無効化は必ずしも効果的ではなく，ワードそのものを使わないことには及ばないとしている．しかし，マクロを含むマルウェアの比率などの言及はなかったため，今回はその点についても考察を行った．また本研究の解析の際には，Jiyong Jang らの研究などを参考にしつつ，今回は viper で抽出した情報である strings や version，author，作成日などでクラスタリングを行った [3]．

Md.Enamul Karim らの研究によると，マルウェアにもソースコードの作りなどで系統が存在するが [4]，本研究においても似た個体を多数検出できたことから，ある程度それを実証することができたものと判断する．

pdf ファイルのマルウェアに関する類似研究として文献 [5] があり，ファイルサイズやオブジェクト数等の単純な量的特徴に関する解析が行われている．本研究ではそれらに加え，strings からの情報による分類なども行った．

金融系マルウェアに関する研究としては，文献 [6] があり，VAWTRAK や Neverquest などと呼ばれるマルウェアを解析対象としているが，本研究においては，金融関連の単語をファイル名に含むマルウェアを対象とした．他にも，個人情報等に着目した標的型攻撃の情報共有 [7]，Kullback-Leibler 情報量を用いた亜種マルウェアの同定 [8] や統計的手法によるマルウェアの判定 [9] の研究が過去に行われている．

3　解析手法

本研究では，検体の入手先として malwr[10] を用いた．malwr はマルウェア解析サービスを行なっており，マルウェアを含むファイルの挙動等が記載され，検体がアップロードされている．malwr にアップロードされている検体には，アンチウイルスソフトで検知されないが動的解析でマルウェアの挙動が検知されているものが多く存在し，これらは標的型攻撃に用いられたものだと考えられる．解析する検体の選定にあたり，malwr における検体の流通量と社会的脅威度の高さを鑑み，以下の金融関連の単語をファイル名に含むものとした．

- 世界 20 大銀行名 [11]
- credit
- bank
- ATM
- money
- cash
- payment
- financial
- deposit

検体の解析は，viper[12] をオープンプラットフォームである docker[13] の環境下において使用した．viper はバイナリ解析フレームワークでありファイルの一般情報を表示できるほか，ファイル形式に応じたコマンドを使用することでバイナリファイルの解析を行うことができる．使用したコマンドについては後述する．以上の環境下において，金融関連の単語をファイル名に含むマルウェアの解析を行いその傾向について考察した．

4　解析結果と考察

本章では，解析結果及びその考察について拡張子ごとに述べる．

4.1　doc ファイル解析結果

金融関連の単語で検索したマルウェアのうち，拡張子が doc，docx である 63 検体を解析した．

解析に使用した viper のコマンドは以下のとおりである．

- info：
  ファイル名，ファイルサイズ及び MD5 などのハッシュ値を表示する．
- office -o：
  マクロの有無などの OLE 情報を表示する．
- office -m：
  タイトルや著者などのメタ情報を表示する．
- office -s：
  stream 情報を表示する．
- office -v：
  マクロコードの解析を行う．
- shellcode：
  既知の shellcode の有無を表示する．
- strings -a：
  全 strings 情報を表示する．

4.1.1 大分類

今回 viper を用いて各検体の strings を比較したところ，その特徴によって 5 種類に大別することができた．大分類は以下のとおり．なお，各名称はこちらで独自に設定したものである．

1. 有意味文字列
2. 無意味文字列
3. MERGEFORMATINET
4. コード (msword 表記)
5. コード (非 msword 表記)

以下，それぞれの詳細について述べる．

4.1.2 有意味文字列

検体数：12 検体
小分類：author ごとに 4 つに分類
この種類の特徴：

1. strings -a コマンドで有意文が検出される．（勧誘やお知らせなど）．
2. 12 検体中，author が shad の 2 検体にマクロが存在．
3. version は 786432，726502，983040 の 3 種類．
4. author は user，fair，owner，shad の 4 種類．
5. template は全て Normal.
6. 作成日付は 2014.11.5-2015.7.24 の間の 4 つの期間に集中している．
7. doc ファイルや xls ファイルが開かれるとマクロが自動的に起動する．
8. マクロの解析結果，Open，Binary，Environ，CreateObject，Chr，Write，Put の文字を確認．
9. マクロのある 2 検体が，アンチウイルスソフトでウイルスとして検知された．
10. ファイル名に financial，payment の単語が含まれる検体が計 8 検体であった．

考　察：author が同じで作成時期が近い場合，ほぼ同じ内容の有意文が検出される．1 つの原型の検体を改造して，使い回しているものと推測される．またマクロが使われているものは，自動でファイルの作成書き込みを行うものと思われる．

4.1.3 無意味文字列

検体数：7 検体
小分類：無意味文字列の長さで 2 つに分類
この種類の特徴：

1. strings -a コマンドで，冒頭に改行と空白の無い，4 万字を超える非常に長い無意味文字列が検出される．
2. 全検体にマクロが存在．
3. 検出される無意味文字列は，文字は全て異なるが，改行の位置やスペースの間隔がよく似ている．
4. version は 983040 の 1 種類．
5. author と更新者は，英数字の組み合わせであり，検体ごとに異なる．
   (例：author 6199l ，last saved by 6199d)
6. template は全て Normal.dotm で作成されている．

7. 作成日付は 2015.7.22-27 の 6 日間.
8. doc ファイルや xls ファイルが開かれるとマクロが自動的に起動する.
9. マクロの解析結果，Open，OpenObject，Chr，Output，Print，CreateObject，Environ，Shell の文字を確認.
10. マクロの動作は全検体で同様と思われる.
11. 5 検体がアンチウイルスソフトでウイルスとして検知された.
12. 全てファイル名に bank という単語が含まれる検体であった.

考　察：strings は何か意味があってのことであり，その文字数を埋めることに意味が有るものと推測する．またマクロが使われているものは，ファイルの作成や書き込みなどを含む同様の動作を行うものと思われる．またファイル名に bank という単語が含まれる検体が多かったことから，銀行系を狙った攻撃で多用されていると推測する.

4.1.4　MERGEFORMATINET

検体数：27 検体
小分類：作成年と author により 3 つに分類
この種類の特徴：

1. strings -a コマンドで，MERGEFORMATINET の記述に引き続き，words の version 選択のような記述が出る.
2. 27 検体中全てにマクロが存在.
3. version は 786432(2009 年製)，983040（ld 作，ins 作）の 2 種類.
4. author は l ○ d，l ○ j，i ○ n．s の 3 種類（○は数字）.
(例：author i2957n，last saved by 2957s)
5. template は全て Normal.dotm.
6. 作成日付は 1 つだけ 2009 年．その他は全て 2015.2.25-27 の 2 種類.
7. 2009 年の検体はスペイン語で作成されており，トロイ系の exe と同じ動きをする.
8. doc ファイルや xls ファイルが開かれるとマクロが自動的に起動する.
9. マクロの解析結果，Kill，Open，vbNormal，Windows，Chr，Write，Output，Print，User-Agent，Shell，Environ の文字を確認.
10. 2009 年の検体のみマクロの内容が異なり，Shell，vbNormalFocus，CreateObject，DownloadFile，StrReverse，ADODB.Stream，SaveToFile，Environ，Write，MicrosoftXML-HTTP の文字が確認できる.
11. 18 検体がアンチウイルスソフトでウイルスとして検知された.
12. 26 検体はファイル名に money の単語が含まれていた.

考　察：author が同じで作成時期が近い場合，ほぼ同じ内容の有意文が検出され，それに引き続く無意味文にはところどころ同じ文字列が見られる．このことから，原型となる 1 つの検体を改造して，使い回しているものと推測される.

また ld 作と ins 作の検体について，ld 作は author が○ l で最終更新者が○ d であり， ins 作は author が i ○ n で最終更新者が○ s となっている．名付けのパターンが同じであることから，組織的に作られたマルウェアである可能性がある.

マクロに関しては 27 検体中 25 検体は検出された単語が同じであったことなどから，25 検体はプロセス終了やファイルの作成，書き込みなどを含む同様の動作を行うと思われる.

4.1.5　コード (msword 表記)

検体数：13 検体
小分類：author ごとに 2 つに分類
この種類の特徴：

1. strings -a コマンドで，Microsoft Office Word の記述に引き続き，コードのようなものが最初から散見される.
2. 13 検体中 12 検体にマクロが存在する.
3. version は 730895(GN 作)，983040（作者不明）の 2 種類.
4. author は 1 で更新者は GN のものと，author 及び更新者が空欄の検体の 2 種類.
5. template は GN 作の検体は Normal.dot，作者不明の検体は Normal.dotm.

6. 作成日付は，GN 作の検体は 2015.1.19，4.23，4.27 と 5.7．作者不明の検体は 2015.7.8．
7. 2015.1.19 作成のものは更新日は 4.17．
8. doc ファイルが開かれるとマクロが自動的に起動する．
9. マクロの解析結果，11 検体に，Lib，Open，Binary，CreateObject，Write，Put，Chr，Xor の文字を確認．
10. 残り 1 検体にはマクロ中に Open，Chr，Output，Print，Shell，Open，CreateObject，Chr，Environ の文字が確認できる．
11. 12 検体がアンチウイルスソフトでウイルスとして検知された．
12. 12 検体はファイル名に credit という単語が含まれていた．

考　察：author が同じで作成時期が近い場合，ほぼ同じ内容の有意文が検出される．このことから，1 つの原型となる検体を改造して，使い回しをしているものと推測される．またマクロが使われている検体は全て，ファイルの作成や書き込みを含む同様の動作をするものと思われる．

4.1.6　コード (非 msword 表記)

検体数：4 検体
小分類：2013 年製，2015 年製に分類
この種類の特徴：

1. strings -a コマンドで，Microsoft Office Word の記述が出ずに，コードのようなものが最初から散見される．
2. 全検体でマクロが使用されていない．
3. OLE ファイルではないため，version 情報，template 情報は得られなかった．
4. 全検体に対して，xml が用いられていると見られる．
5. 作成日付は 2013 年が 2 つと 2015 年が 2 つ．
6. 全検体がアンチウイルスソフトでウイルスとして検知されなかった．
7. 4 検体にファイル名に financial という単語が含まれていた．

考　察：マクロがない代わりに，ファイル内に一緒に含まれるものに仕掛けがあると思われる．

4.1.7　doc ファイル全体についての考察

本研究において，金融機関を狙ったマルウェア 722 検体中 doc・docx ファイルは 140 検体であった．その 140 検体の中から，ダウンロードできた 63 検体を特徴ごとに 5 つに大別した．その特徴とは，viper の strings -a コマンドを用いた際現れた顕著な差であり，それによって分類を行った．

大別した結果，それぞれの種類に明確な違いが確認できた．例えば，マクロの有無は分類ごとに多い少ないが存在した．このことを用いて，分類とマクロの有無を組み合わせれば，有効なフィルタリングに寄与できると考える．またアンチウイルスソフトで検知した 37 検体は全てマクロが使われている検体であり，半数以上のアンチウイルスソフトがウイルスとして検知した検体は，コード (msword 表記) の 1 検体のみであった．

また今回の検体からは既知の shellcode は 1 つも検出されなかった．今回の調査だけで結論づけることはできないが，少なくとも金融機関を狙った doc ファイルに関しては shellcode を用いた攻撃は主流ではないと考える．むしろマクロが 63 検体中 48 検体と約 76%もの検体に使用されており，解析の結果，doc ファイルの悪意ある攻撃の多くはマクロに起因すると考えられるため，セキュリティの観点からは必要がなければマクロを無効化しておくことが望ましい．また全体的に，原型となる 1 つの検体を改造して作ったようであり，template や version，作成年月日や製作者によって 5 つの分類をさらに細かく分類し，全部で 14 の小分類に区分することができた．

4.2　pdf ファイルの解析

4.2.1　解析結果

金融関連の単語で検索したマルウェアのうち，拡張子が pdf である 33 検体を解析した．なお，33 検体中 3 検体のみがアンチウイルスソフトでウイルスとして検知された．またマルウェアを含まない正常な pdf ファイル 5 つとの比較も行った．ここで言う正常な pdf ファイルとは自らが作成した pdf ファイルのことである．解析に使用したコマンドは以下のとおりである．

- info：
  ファイル名，ファイルサイズ及び MD5 などのハッシュ値を表示する．
- pdf id：
  pdf ファイルのバージョン，エントロピ及び obj や JavaScript のカウント数を表示する．
- pdf streams：
  pdf ファイルのストリームオブジェクト情報を表示する．
- shellcode：
  既知の shellcode の有無を表示する．
- strings -a：
  全 strings 情報を表示する．
- strings -H：
  全 strings から IP アドレスとドメインを表示する．

これらのコマンドを使用し解析した結果，全体的な特徴として pdf バージョンが古い検体が多く，バージョン 1.5 以下が全検体の約 90 %を占めた．また pdf 作成日における特徴としては 2014 年以降作成の検体が約 60 %，作成日不明が約 21 %であり，作成日が 2013 年以前の検体は少なかった．

pdf ファイルのメタ情報においては，Title，Author，Keywords，Creator，Producer，CreationData が設定できるが，本研究における対象である金融関連のファイルを想定できる Title は 4 検体のみであった．Author では，user，Administrator，人物名や英数字の羅列といった情報が記載されていたが，他の情報との関連性は認められなかった．またメタ情報がまったく記載されていない検体もあり，その数は 11 であった．

strings からドメインが検出された検体が約 79%であり，44 種類のドメインが存在した．これらのドメインを PhishTank[14] を利用し，フィッシングの調査を行った．結果，まだフィッシングと判定はされていないがフィッシングと疑われるドメインは 1 つであり，このドメインが含まれる検体は 1 つしか存在しなかった．

その他，viper での解析においては，Launch，RichMedia，EmbeddedFile の自動で起動する機能や組込型のファイルの有無を確認することもできるが，本研究における検体ではいずれも確認できなかった．

また解析により得られた検体の特徴から 4 種類に大別できた．

1. 正常な pdf ファイルと有意な差がない検体
   該当数：27 検体
2. JavaScript が含まれる検体
   該当数：2 検体
3. shellcode が含まれる検体
   該当数：1 検体
4. 大量の数字が strings に含まれる検体
   該当数：3 検体

マルウェアを含んでいると思われる検体のほとんどは，出力結果の概要が正常な pdf ファイルと有意な差がないという結果が得られた．

また pdf id コマンドを使用した出力では pdf ファイル全体のエントロピを表す Total Entropy，ストリーム中のエントロピを表す Entropy In Streams，ストリーム以外のエントロピを表す Entropy Out Streams の 3 つの値が出力され，エントロピにおいても差別化を図ることができた．

- 正常な pdf ファイル（平均）
  Total Entropy ：7.971735
  Entropy In Streams ：7.978538
  Entropy Out Streams ：5.092406
- 全検体（平均）
  Total Entropy ：7.822677
  Entropy In Streams ：7.956151
  Entropy Out Streams ：5.047358
- JavaScript が含まれる検体（平均）
  Total Entropy ：6.552932
  Entropy In Streams ：7.787304
  Entropy Out Streams ：5.271851
- shellcode が含まれる検体
  Total Entropy ：7.994018
  Entropy In Streams ：7.996027
  Entropy Out Streams ：5.204328

- 大量の数字が strings に含まれる検体
  （平均）
  Total Entropy ：7.607669
  Entropy In Streams ：7.951019
  Entropy Out Streams ：4.299523

上記のように，正常な pdf ファイルと全検体のエントロピにおける平均値はいずれも有意な差は見られなかった．しかし，JavaScript が含まれる検体の Total Entropy 平均値は正常な pdf ファイルと全検体の平均値と比べ 1.2 以上小さく，大量の数字が strings に含まれる検体の Entropy Out Streams 平均値では 0.7 以上小さい．shellcode が含まれる場合においては，エントロピにおける差は見られなかった．

4.2.2 pdf の考察

pdf ファイルの解析においては，33 検体中 3 検体のみがアンチウイルスソフトでウイルスと検知された．このことから，pdf ファイルにおいてはアンチウィルスソフトに検知されないマルウェアが多く含まれており危険度が高いと考える．今後は，検体数を増やしその動向を探る必要がある．

解析結果による全体的な傾向として，pdf の古いバージョンを使用し，ファイル作成日が新しい pdf ファイルがマルウェアを含んでいる可能性が高いことを確認できた．またフィッシングと疑われるドメインを含む検体は 1 つのみであり，フィッシングを用いてマルウェアを含んだ pdf ファイルの判定要素とすることはあまり効果が期待できないものと考える．そして，本研究における解析結果の特徴から 4 種類に大別できることも判明したが，出力結果の概要からはその多くは正常な pdf ファイルとの有意な差は認められず，有力な傾向がつかめたとは言い難い．しかし，JavaScript が含まれていないファイルが本研究においては多かったが，pdf ファイルには不正なフォントを埋め込み悪意ある遠隔コード実行につながる脆弱性が報告されている．よって，JavaScript が含まれていない pdf ファイルでも攻撃コードが含まれていないとは言い切れないため，それらの脆弱性に関する調査も今後行っていく．

またエントロピに着目すると正常な pdf ファイルと出力概要が類似している検体においては，エントロピの平均値においても差異がなく，改めて類似性を確認できた．特徴が得られた検体においてはエントロピの値に差異があることが判明した．以上の結果から，pdf ファイルの特徴とエントロピとの関連性を見出すことができ，エントロピの値から JavaScript 等の有無を推測できるものと考える．一方で，現状の検体数ではメタ情報からは有力な情報は得られず，マルウェアを含む pdf ファイルを判別する際にはメタ情報からの情報は期待できないものと推測する．

4.3 zip ファイル解析結果

4.3.1 調査結果

金融関連の単語で検索した zip 拡張子のマルウェア 73 検体を unzip コマンドで解凍した．その結果，zip の中身は下記のとおりであった．

scr 18，html 2，exe-exc 1，exe 34，xml 3，doc 1，xls 1，pdf 1，txt 2，txts 2，empty 2，asc-txt 1，js 4，解凍不可 1
合計 73 検体

4.3.2 zip の中身に対する考察

scr，exe-exc，exe を同じ exe 系として数えると，73 検体中 53 検体と実に約 73%が exe 系のファイルであった．この比率は今回調べたマルウェアで exe 系が 722 検体中 253 検体と，約 35%だったことを考えると，zip の中身における exe 系の比率は，金融機関一般で流通している exe 系の比率よりも明らかに高かった．

この理由としては「exe は危険」という認識が浸透したことから，exe で攻撃する場合には，偽メールなどに添付した zip ファイルを開けさせる手法も広く用いられているためと推測する．実際に zip を解凍して出てきたファイルのうち相当数が exe や doc のマルウェアとしても報告されている検体と同一のものであった．

5 おわりに

本論文では，金融機関を狙ったと思われる，doc，pdf，zip の拡張子をもつマルウェアの検体に対して viper を用いたバイナリ解析を行い，その傾向を探った．その結果として，doc ファイルは 5 種類に大別することができ，主に strings の大まかな様式で分類することが可能であった．また doc ファイルのマルウェアでマクロを含む

検体の比率は約 76%であったため，必要がなければマクロの無効化が望ましい．pdf ファイルは 4 種類に大別でき，shellcode の有無などで分けることができ特徴が判明したものの，検体のほとんどは正常な pdf ファイルとの有意な差を確認することはできなかった．zip ファイルは中身の約 73%は exe 系のファイルであり，偽メールなどで釣られて開けないような啓蒙活動を引き続き行うことが必要だと考える．またオープンソースの機材を用いた比較的簡易な解析を行ったが，上記のような結論を導くことができたことから，一定の成果は上げることができたものと判断する．

今後の課題としてはこのような解析結果を増やしてデータの蓄積を行い，将来的には特定の条件を満たした検体に対して自動的にふるいにかけ，マルウェアの検知時に警告を発するような有効なフィルタリングに寄与できることが望ましい．また様々な業種や地域ごとにサンプルをとり，攻撃目標と攻撃手法の相関性を調べ，その統計をとることで，より傾向を知ることができるようになると考える．

本研究のような解析結果を広く収集して積み重ねることで，高度な技術と多大な労力を要する解析手法を用いずとも，マルウェアについての判断が実現できるように引き続き研究を行う必要がある．

参考文献

[1] サイバーセキュリティ戦略本部，サイバーセキュリティ政策に係る年次報告（2014 年度），2015 年 7 月 23 日，http://www.nisc.go.jp/active/kihon/pdf/jseval_2014.pdf，最終確認日 2015 年 8 月 21 日．

[2] Wei-Jen Li, et al. A Study of Malcode-Bearing Documents. Proceedings of the 4th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment(DIMVA '07), pp.231-250, July 2007.

[3] Jiyong Jang, et al. BitShred: Feature Hashing Malware for Scalable Triage and Semantic Analysis. Proceedings of the 18th ACM Conference on Computer and Communications Security(CCS '11), pp.309-320, October 2011.

[4] Md.Enamul Karim, et al. Malware Phylogeny Generation using Permutations of Code. Journal in Computer Virology, Vol.1, No.1-2, pp.13-23, November 2005.

[5] 今野由也，角田裕．Drive-by-Download 攻撃における悪性 PDF の特徴に関する考察．マルウェア対策研究人材育成ワークショップ 2014，2014 年 10 月．

[6] 西田雅太，他．静的解析と挙動観測による金融系マルウェアの攻撃手法の調査．マルウェア対策研究人材育成ワークショップ 2014，2014 年 10 月．

[7] 齊藤真吾，他．標的型攻撃情報共有のための文書型マルウェアの墨塗り手法．マルウェア対策研究人材育成ワークショップ 2013，2013 年 10 月．

[8] 中村燎太，他．Kullback-Leibler 情報量を用いた亜種マルウェアの同定．マルウェア対策研究人材育成ワークショップ 2013，2013 年 10 月．

[9] 田中恭之，他．統計的手法を用いたマルウェア判定の実験結果．マルウェア対策研究人材育成ワークショップ 2014，2014 年 10 月．

[10] malwr，https://malwr.com，最終確認日 2015 年 8 月 24 日．

[11] 世界 20 大銀行，http://thetally.efinancialnews.com/2014/07/whos-biggest-bank，最終確認日 2015 年 8 月 23 日．

[12] viper，http://viper.li，最終確認日 2015 年 8 月 24 日．

[13] docker，https://docs.docker.com，最終確認日 2015 年 8 月 21 日．

[14] PhishTank，https://www.phishtank.com，最終確認日 2015 年 8 月 23 日．