3Z-3

難読化された攻撃コードの挙動を反映したトラフィック可視化による攻撃解析支援のためのインタフェース

松井 拓也† 義則 隆之† 佐藤 両† 廣友 雅徳‡ 毛利 公美†† 神薗 雅紀‡‡ 白石 善明†

†名古屋工業大学 ‡佐賀大学 ††岐阜大学 ‡‡（株）セキュアブレイン

1. はじめに

マルウェアの感染活動は，攻撃者の操作により感染させる能動的攻撃に加え，ユーザが行う何らかの操作を契機として感染させる受動的攻撃が用いられるようになった[1][2]．受動的攻撃の具体例として，攻撃コードが埋め込まれた Web サイトを閲覧したユーザを悪性サイトへ誘導し，マルウェアに感染させる攻撃がある．他にも，攻撃コードを含んだファイルを添付したメールをユーザに送信し，受信したユーザがファイルを開くことで攻撃コードが実行され，ユーザを悪性サイトへ誘導し感染させる方法がある．このような受動的攻撃のマルウェア感染による被害の拡大を抑えるためには，感染した端末の通信データを解析して悪性サイトの URL を特定し，ファイアウォールなどでフィルタリングするのが基本的な対策となる．このとき，文字情報で表された通信データは理解しづらく，一連の通信からなる攻撃フローを絞り込むのは容易ではない．また，攻撃コードは難読化が施されていると攻撃フローの全容把握を妨げる．

そこで，悪性サイトの URL を含む攻撃フローを抽出する通信データの解析を支援することを目的として，難読化された攻撃コードの挙動を反映したトラフィックを可視化したインタフェースを本稿では提案する．

2. 関連研究

2.1. 地理的可視化

通信データは文字情報で表されるよりも，地理的に可視化する方が理解しやすい．パケットの送信元 IP アドレスから得られる地理的情報に基づきパケットを地図上に可視化している nicter[3]などがある．

2.2. 対話機能による調査作業の支援

人間が通信データを解析する際には対話機能が必須と言われている[4]．ここでの対話機能とは，条件や解析範囲を変更して解析対象を絞り込む機能のことである．対話機能によって，アクセス先や受信したファイル形式などの複数の条件で通信データをフィルタリングできるのが望ましい．

2.3. 難読化 JavaScript コードの解析

解析を妨害するために攻撃コードが難読化されているものが増えている．Web サイトや，PDF ファイルに埋め込まれる難読化された JavaScript の解析に，静的解析によって難読化を解除する手法[5]や，動的解析によって挙動を監視する手法[6]がある．

3. 通信データ解析を支援するための機能

通信データの解析支援には，地理的可視化と対話機能が有用であると期待できる．可視化結果は正確でなければ支援を妨げるので難読化コードに対応しなければならない．そこで，次の機能を持つ攻撃解析支援のためのインタフェースを提案する．

[世界地図上に描画する機能] 地図は位置情報を空間的に表すことができ，通信の全容を直感的に理解できる．まず，通信データから，パケットごとにアクセス先の IP アドレスを取得し，IP アドレスと地理的情報を対応付ける．IP アドレスごとに世界地図上にプロットする．そして，通信データは地図上の IP アドレスを時間順に有向辺で結んでいくことで地理的可視化を行う．2 次元あるいは 3 次元空間上に時系列データを見やすく表現するためにアニメーションをさせる．

[対話的なフィルタリング機能] 表示範囲の指定や，異なる条件をもとに描画する通信フローを絞り込むことで，通信データから攻撃フローの抽出を支援する．絞り込みの条件を，アクセス先国名，送信元ポート番号，宛先ポート番号，通信プロトコル，受信したファイル形式とする．

[難読化された攻撃コードの挙動を反映する機能] 難読化された攻撃コードがあった場合，難読化を解除するのではなく動的解析によりアクセス先を取得し，世界地図上に反映する．難読された攻撃コードを含む通信フローは攻撃である可能性が高いので，他の通信と区別できるよう有向辺の色を変えて表示する．

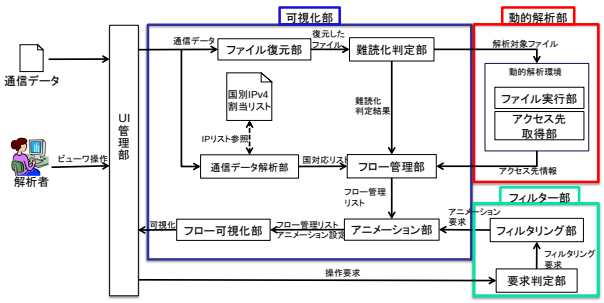

図 1 システム構成

4. インタフェースの設計

4.1. インタフェースの構成要素

本インタフェースのシステム構成を図 1 に示す．本インタフェースの 3 つの構成要素を以下に示す．

[可視化部] 通信データから世界地図上に通信フローを出力する．また，通信データからファイルを復元し，難読化されたコードを含む場合，動的解析部に解析を要求する．フィルター部から受けとった結果を可視化に反映する．

[フィルター部] 解析者から操作要求を受け取り，解析対象のフィルタリングを行い，その結果を可視化部に返答する．

[動的解析部] 可視化部から要求された解析対象ファイルを実行し，アクセス先情報を取得する．取得したアクセス先情報を可視化部に返答する．

4.2. 処理の流れ

本インタフェースは準備フェーズと操作フェーズからなる．準備フェーズでは，入力された通信データから，ファイル復元，難読化判定，動的解析，可視化する．操作フェーズでは，操作要求を受け取り，解析対象をフィルタリングする．

[準備フェーズ]

step1. UI 管理部から可視化部が通信データを受け取る．

step2. 通信データから，パケットヘッダを読み，IP アドレスとそれに対応する国名／地域名を取り出す．断片化されているパケットの場合，結合をしてファイルを復元し，ファイル内の難読化コードの有無を判定する．もしも，難読化されているならば動的解析する．ヘッダ情報，難読化判定結果，動的解析結果をフロー管理部に渡す．

step3. フロー管理部の情報から，通信フローを描画する．

[操作フェーズ]

step1. UI 管理部から操作要求を受け取り，要求内容を判定する．要求内容をもとに，解析対象をフィルタリングする．

Interface for Supporting Attack Analysis with Traffic Visualization Reflecting the Behavior of Obscure Attack Code

† Takuya MATSUI, Takayuki YOSHINORI, Ryo SATO and Yoshiaki SHIRAISHI・Nagoya Institute of Technology

‡ Masanori HIROTOMO・Saga University

†† Masami MOHRI・Gifu University

‡‡ Masaki KAMIZONO・ Secure Brain Corp.

step2. フィルタリング結果をもとにアニメーションシナリオを再設定し，可視化インタフェースに反映する．

5. 実装したインタフェース

実装したインタフェースを図 2 に示す．本インタフェースは，世界地図ウィンドウ，URL 一覧ウィンドウ，フィルター操作ウィンドウの 3 つのウィンドウで構成されている．

5.1. 世界地図ウィンドウ

図 2 の(1)は，3D で世界地図を表示し，宛先 IP アドレスごとにポールをたて，通信データに含まれている順番にポール間に有向辺を接続する．その接続された有向辺を順番に描画していくことで，通信フローをアニメーション表現する．3D のカメラの位置はマウスで操作できる．左ボタンのドラッグでカメラの焦点を中心に回転，右ボタンのドラッグで平行移動，マウスホイールの回転で，拡大，縮小ができる．

5.2. URL 一覧ウィンドウ

世界地図ウィンドウ上のポールをクリックすると，吹き出しが表示される．吹き出し中の URL List のリンクをクリックするとその IP アドレスに対応し図 2 の(2)の画面を表示する．この画面にはアクセスした URL の一覧を表示する．

5.3. フィルター操作ウィンドウ

図 2 の(3)は，通信データの詳細情報を表示する．また，フィルタリングの条件の入力と結果の表示をする．

グラフは，単位時間当たりのパケットの総量を示す．グラフ下のスライドバー，さらにその下のボタンでは世界地図ウィンドウのアニメーション操作を行う．スライドバーを操作することで，解析対象箇所を変更できる．また，アニメーションの再生，一時停止，巻き戻し，早送りの操作を行う 3 つのボタンを用意している．

アクセス先の国名を Country で，括弧内の数字で各国あたりのアクセス回数を示す．利用した送信元ポート番号，宛先ポート番号を Source Port, Destination Port で表す．HTTP,TCP,UDP など，どのプロトコルが使われているかを Type of Packet で，括弧内の数字はその発生件数を示す．受信したファイルの拡張子の一覧を Type of Files で，括弧内の数字はそれぞれの拡張子のファイル数を示す．これら 5 つの条件により解析対象の通信データをフィルタリングする．

6. 解析支援システムの比較

提案インタフェースと他の解析支援システムを比較したものが表 1 である．比較項目 A~E を以下に示す．

A：通信量に着目した解析
B：特定の国に着目した解析
C：地理的な可視化
D：対話的なフィルタリング
E：難読化された攻撃コードに着目した解析

解析支援では通信量は定量的に判断できるものなので A を挙げている．B は悪性サイトが置かれる場所は特定の国に偏っていることがあるので，着目されることが多い．C，D，E は 3 章で説明した提案インタフェースの特徴的な機能である．C は世界地図上に描画する機能，D は対話的なフィルタリング機能，E は難読化された攻撃コードの挙動を反映する機能に対応する．

文献[7]で通信量の増減をグラフにし，ボットネットによるスキャン活動を解析することが提案されている．文献[8]で通信量と特定の国の情報を組み合わせて解析し，特定のマルウェアを発見するための支援システムが提案されている．文献[4]，[9]で通信量と特定の国の情報に着目した解析ができることに加え，対話機能によるフィルタリングを用いることで，通信データからあるマルウェア抽出することが提案されている．文献[3]，[10]で通信データを地理的に可視化し通信の全容を把握して，異常を検出することを目的としたシステムが提案されている．

本研究では通信データを地理的可視化により通信全体を把握し，対話的なフィルタリングにより攻撃フロー抽出することができるので，C，D を組み合わせた支援になっている．また，E についてはこれまでの解析では着目されなかった点であり，本研究で新たに着目した機能である．

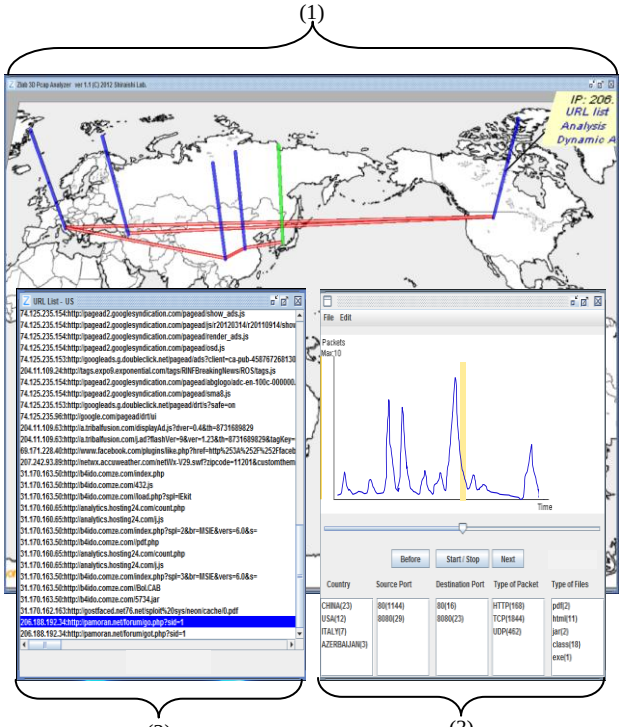

図 2　インタフェースの画面

表1　関連システムとの比較

	A	B	C	D	E
[7]	○	-	-	-	-
[8]	○	○	-	-	-
[4],[9]	○	○	-	○	-
[3],[10]	○	○	○	-	-
本研究	○	○	○	○	○

7. まとめ

本稿では，世界地図上に描画する機能，対話的なフィルタリング機能に加え，正確に可視化するために，難読化された攻撃コードの挙動を反映する機能を持つインタフェースを提案した．他の解析支援システムと比較し，持っている機能の違いを示した．

今後はユーザ実験による評価を行う予定である．

参考文献

[1] 青木一史，川古谷裕平，秋山満昭ほか：能動的攻撃と受動的攻撃に関する調査及び考察，情報処理学会論文誌，Vol.50，No.9，pp.2147-2162 (2009).
[2] 情報処理推進機構：近年の標的型攻撃に関する調査研究，http://www.ipa.go.jp/security/fy19/reports/sequential/seq_rep.pdf(参照 2012-11-30).
[3] NICT：nicter，http://www.nict.go.jp/glossary/nicter.html，(参照 2013-01-10).
[4] 高田哲司，小池英樹：人間による Honeypot の攻撃ログ調査を支援する User Interface の提案，マルウェア対策人材育成ワークショップ(MWS 2008)，pp.81-86(2008).
[5] 神薗雅紀，西田雅太，小島恵美，星澤祐二：抽象構文木解析による不正な Javascript の特徴点抽出手法の提案，Vol.2011，No.3，pp.474-479(2011).
[6] 神薗雅紀，西田雅太，星澤祐二：動的解析を利用した難読化 Javascript コード解析システムの実行と評価，電子情報通信学会技術研究報告(ICSS)，Vol.110，No.475，pp.47-52(2011).
[7] 池田潤一，岩村誠，秋岡明香，村岡洋一：通信トラフィックの時系列分析によるボット活動の可視化と特徴検出，コンピュータセキュリティシンポジウム 2009(CSS2009)論文集，pp.271-276(2009).
[8] 警視庁，@police，http://www.npa.go.jp/cyberpolice/detect/observation.html (参照 2012-01-10)
[9] Kiran Lakkaraju, William Yurcik, and Adam J Lee, NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness, ACM SIGSAC, pp. 65-72(2004).
[10] 金子博一：地理的可視化を用いたマルウェアの統合解析，CSS2011，179-184(October 2011，コンピュータセキュリティシンポジウム 2011(CSS 2011)論文集，pp.179-184(2011).