# 【調査】HTTP リクエスト/レスポンスによるマルウェア検知

山下 尚彦

2020 年 4 月 25 日

## 1 はじめに

昨今のサイバー攻撃は巧妙化しており a, マルウェア感染を未然に防ぐことは困難となっている. なぜなら, 特定の組織やターゲットの機密情報を窃取する標的型攻撃が盛んになり, それとともに攻撃が高度化・複雑化しているからである. 独立行政法人情報処理推進機構 (IPA) によると, こういった高度な標的型攻撃は以下の 7 つの段階で構成されている [1].

**計画立案**
: 攻撃対象の調査・決定する

**攻撃準備**
: C2 サーバを用意するなどの攻撃の準備をする

**初期侵入**
: 標的型メール, 水飲み場型攻撃などによって対象のネットワークに侵入を行う. これらの攻撃者の行動はファイアウォールやアンチウイルスソフトウェア, 侵入検知システムでも完全には防ぐことはできない.

**基盤構築**
: C2 サーバとのバックドア通信を構築し, 感染端末が司令を受け取れるようにする

**内部調査**
: 他の端末への侵入などによって対象となるネットワークの情報を調査する.

**目的遂行**
: 機密情報の窃取やシステムの破壊活動を行う.

**再侵入**
: 初期侵入時に利用した脆弱性や攻撃者が設置したバックドアから再び侵入し, **内部調査**や**目的遂行**を繰り返す

また, 従来のマルウェアは C2 サーバとの通信に IRC や独自のプロトコルを利用するため, ファイアウォールやプロキシ, トラフィックデータやログデータなどから振る舞いを学習させて検知するアノマリ検知によってその通信を遮断することは比較的容易であった. しかし, 一般的な業務で頻繁に使用されている HTTP プロトコルを用いて C2 サーバと通信を行う高度なマルウェアの登場も検知を回避される要因となっている.

そこで, 小川らはトラフィックデータから取得した HTTP リクエストおよび HTTP レスポンス情報から特徴量を抽出し, Support Vector Machine(SVM) によって 2 値判定を行うことで検知する手法を提案した [2]. 実験の結果, マルウェア感染由来の HTTP トラフィックの検知において高精度で検知することができ, またその見逃し率も低いという結果が出た.

## 2 提案手法

前述したとおり, 小川らは正常な通信とマルウェア感染時の通信のリクエストの間隔とレスポンスのボディサイズから特徴量を抽出し, SVM によって 2 値判定を行うことでマルウェア感染由来の HTTP トラフィックの検知を目指す. 関連研究では, レスポンスのボディ自体を参照するためプライバシーの観点から課題が存在したが, この手法はボディサイズのみ着目するためプライバシーの保護に優位性があるとしている.

以下に示す手順によって識別機に学習させる.

1. **リクエスト/レスポンスのペアと構成**
   トラフィックデータから HTTP トラフィックを抽出し, さらにリクエスト時間, リクエストの送信元 IP アドレス, リクエストの送信先 IP アドレス, レスポンスのボディサイズを抽出し, リクエストとレスポンスの情報をペアにする
2. **通信ホストごとにペアを分割**
   マルウェア感染によってある通信先との間でトラフィックが発生しても, その他の通信先との間で正常なトラフィックが多く発生した場合, 抽出する特徴量が正常トラフィックの影響を大きく受けてしまう可能性があるため通信ホスト

ごとに分割する

3. **特徴ベクトルの抽出**
   以下のように通信ホストペアごとに分割した HTTP リクエスト/レス ポンスペアから, 特徴ベクトルを抽出する.
   (a) 通信ホスト毎に分割した HTTP リクエスト/レスポンスペアからリクエスト間隔およびレスポンスボディサイズのリストを抽出する
   (b) 抽出したリクエスト間隔及びレスポンスサイズを昇順にソートする
   (c) ソート済みのリクエスト間隔及びレスポンスのボディサイズのリストからそれぞれ, ”最小値, 25 パーセンタイル値, 中央値, 75 パーセンタイル値, 最大値, 平均値, 標準偏差” の 14 個の特徴量を抽出
4. **正規化**
   特徴量間でスケールが大きく異なる場合が起こりうるので, 平均 0, 分散 1 となるようにデータセットから抽出した特徴量データの, 各特徴ベクトルの各値について平均値及び標準偏差を求めて個別に正規化する

## 3 実験

小川らは正常/感染トラフィックのデータをあわせた 2945 個のデータセットをランダムに 5 分割, 各々のデータをテストデータとし, 残りのデータを学習データとした評価実験を 5 回実施した. 実験に使用したデータセットは, 正常/感染トラフィックのうち通信ホストペアで HTTP リクエストが 5 個以上存在し, 特徴量を抽出できたものそれぞれ 2378 個と 568 個を使用した. 評価方法には, 数に偏りがあっても評価できる **Precision** と **Recall** を用いた. それぞれの評価式が以下の**式 1** から**式 4** である.

$$Precision_N = \frac{TN}{TN + FN} \tag{1}$$

$$Precision_P = \frac{TP}{TP + FP} \tag{2}$$

$$Recall_N = \frac{TN}{TN + FP} \tag{3}$$

$$Recall_P = \frac{TP}{TP + FN} \tag{4}$$

$Precision_N$
: 正常データと判定したデータの中で正しく正常と判定できた割合を示す

$Precision_P$
: 感染と判定した中で正しく感染と判定で来た割合を示す

$Recall_N$
: 正常データの中で正しく正常データと判定できた割合を示す

$Recall_P$
: 感染データの中で正しく感染と判定できた割合を示す

$TruePositive(TP)$
: 実際は感染由来の通信であるものを正しく感染と判定したもの

$FalsePositive(FP)$
: 実際は正常であるが予測では誤って感染と判定したもの

$TrueNegative(TN)$
: 実際は感染であるものの正しく正常と判定したもの

$FalseNegative(FN)$
: 実際は感染であるものの誤って正常と判定したもの

## 4 実験結果

実験を行った結果, 算出された Precision と Recall を**表 1** に示す. $Precision_N$ および $Precision_P$ について, 正常と判定したもののうち 96% が正常であると正しく判定でき, 感染と判定したものについては, 93% が正しく判定できているため, 誤判定は少ないと言える. また, $Recall_N$ や $Recall_P$ について, すべての正常データのうち 98% は正しく判定できており, すべての感染データのうち 85% は正しく判定できているため, 見逃しは少ないと言える.

表 1 実験結果

| | $Precision_N$ | $Precision_P$ | $Recall_N$ | $Recall_P$ |
|---|---|---|---|---|
| 1 回目 | 0.96 | 0.94 | 0.99 | 0.82 |
| 2 回目 | 0.97 | 0.96 | 0.99 | 0.88 |
| 3 回目 | 0.96 | 0.88 | 0.97 | 0.84 |
| 4 回目 | 0.96 | 0.92 | 0.98 | 0.83 |
| 5 回目 | 0.97 | 0.94 | 0.99 | 0.86 |
| 平均 | 0.96 | 0.93 | 0.98 | 0.85 |

## 5 おわりに

従来の研究のように, マルウェア感染由来の通信が発生している同一のタイムスロットで正常通信が多く発生している場合, 抽出した特徴量に対してのマルウェア感染由来の通信の影響は弱まるという課題があった. そこで小川らは, HTTP リクエストとそれに対応した HTTP レスポンスのペアを通信ホストごとに分割して特徴量を抽出することで, 同一タイムスロット内の正常な通信がどれだけ多く発生しても, 抽出量に影響を及ぼさない手法を提案した.

正常な通信とマルウェア感染時の通信のデータをあわせたデータセットを分割して学習と判定を行い, この手法の実験を行った. その結果, 誤判定や見逃しは少なかった.

私の研究では, Lomb-Scargle ピリオドグラムという手法を用いて, トラフィックデータの HTTP リクエストの間隔から送信元 IP アドレスと送信先 IP アドレスの通信間で周期性があるかどうかを判定し, ボットと C2 サーバの通信を検知する. しかし, 現状では周期的に通信を行っている IP アドレスのペアを検知することはできるが, それが正常な通信かマルウェアの感染による通信なのかを区別することができないため, 小川らの検知手法と組み合わせることでより精度の高い検知ができるのではないかと考えられる.

## 参考文献


[1] 独立行政法人情報処理推進機構. 「『高度標的型攻撃』対策に向けたシステム設計ガイド」の公開, 2014. https://www.ipa.go.jp/security/vuln/newattack.html.

[2] 小川秀貴, 山口由紀子, 嶋田創, 高倉弘喜, 秋山満昭, 八木毅ほか. リクエスト間隔とレスポンスのボディサイズに基づくマルウェア感染由来の http トラフィック検知. コンピュータセキュリティシンポジウム 2016 論文集, Vol. 2016, No. 2, pp. 408–415, 2016.