5X-04

RNNを用いたペイロード情報のテキスト分類による異常検知方式

中島　嵩也†　　鳥居　直哉†

創価大学　理工学研究科†

1. はじめに

通信技術が発展し，インターネットが様々なものに利用されることで利用者の利便性が高まる反面それらを悪用したマルウェアに遭遇する危険性も高まっている．

マルウェア対策には，シグネチャ型とアノマリ型があり，シグネチャ型は事前に登録しておいた不正なビット列等が含まれていないか調べることでマルウェアを検知しているがマルウェアごとに特徴を示すシグネチャを用意する必要があり，短時間で大量に出現する新しいマルウェアの検知に対応できないという欠点がある．

アノマリ型の検知は事前に正常な状態を定義し，そこから離れた異常な動作を見つけ出す方法である．そのため新種のマルウェアに対しても有効な方法である．

従来，再帰型ニューラルネットワーク（RNN）を用いたマルウェア検知手法にはマシンアクティビティデータメトリックを使用して実行ファイルが悪意のあるものかを判断するもの[1]や送信元アドレス，ポート番号などによって分類されたフローをもとに動作モデルを作成し検出するものなどがある[2]．

本稿では，従来のように複数の特徴量ではなくボットネット通信やマルウェアが C&C サーバと行う通信のペイロード情報という単一の特徴量についてテキスト分類を行うことで異常検知を行う手法を提案している．評価の結果，ボットネット通信とトロイの木馬型のマルウェアにおいて 99 %以上の精度で検知することができた．

2. 提案手法

トロイの木馬型のマルウェアやそれらを利用しているボットネットはその挙動の中に C&C サーバーなどと通信を行う．通信データの中でも情報量の多いペイロード情報に着目し，それを学習させることで異常検知を行う手法を提案する．

RNN は，時系列，あるいは，連続した情報を扱うためのニューラルネットワークである．本手法では，ハードビート通信などを時系列情報とし，ペイロード情報の文字列を数値ベクトルに変換したものを入力とすることで，悪性と正常を分類した結果を出力する．

提案手法では，先ず通信パケットのログからヘッダー情報などを除いたペイロード情報のみを抽出し，ASCII 文字に変換を行う．

次に，変換した ASCII 文字を N-gram 法を用いて分割し一定の長さ以下になるように文字列を作成する．RNN は数値データしか扱えないため分割した文字列を数値ベクトルに変化する．変換の方法は文字列が出現した順に番号付けをした辞書を作成し，そその辞書を用いて文字列を数値ベクトルに置き換える．

最後に置き換えた数値ベクトルを特徴量として RNN に学習させ評価を行う．

3. 実験

3.1 データ

使用するデータセットはボットネット通信として CTU-DATASET[3]，トロイの木馬として BOS2018[4]を使用している．正常データとして創価大学のネットワークをキャプチャソフト Wireshark を用いてキャプチャしたものを使用した．テストデータは，学習データの感染と正常の合計の 20 %をランダムに抽出したものを使用した．表 1 に使用したファイルのサイズを示す．

3.2 実験

使用した RNN は分類器に SoftMax 関数を使用しており，悪性を 0，正常を 1 とした出力をする．学習のパラメータは隠れ層を 200，バッチサイズ 1024，エポック数 1 で実験を行った．

N-gram による文字の分割は，1 文字と 2 文字の 2 種類について実験を行った．評価は，精度，正解率，検出率，F-score の 4 つの指標を用いた．

表 2 に分類の正誤を表す混同行列を示す．表 2 から誤って感染時通信であると判断した割合を示す偽陰性率は FN/P と表せる．

それぞれの実験の混同行列を表 3 に，評価の結果を図 1 に示す．CTU については感染データ数が少なく評価が不正確になるため BOS の評価結果のみを示す．

Attack Detection with Text Classification of Payload Information Using RNN

†Shuya Nakashima and Naoya Torii, SOKA University Graduate School of Science and Engineering

Copyright ©2021 Information Processing Society of Japan.
All Rights Reserved.

表 1　データサイズ

	1-gram	2-gram
正常	264 MB	316 MB
CTU	20.1 MB	23.9 MB
BOS	134 MB	160 MB

表 2　混同行列について

実際の分類	予測した分類	
	悪性	正常
悪性(P)	真陽性(TP)	偽陰性(FN)
正常(N)	偽陽性(FP)	真陰性(TN)

表 3　実験の混同行列

データ	予測した分類			
			悪性	正常
CTU 1-gram	実際の分類	悪性	0 %	100 %
		正常	0 %	100 %
CTU 2-gram		悪性	99.9 %	0.1 %
		正常	0.1 %	99.9 %
BOS 1-gram		悪性	41.1 %	58.9 %
		正常	1.1 %	98.9 %
BOS 2-gram		悪性	98.0 %	2.0 %
		正常	0.1 %	99.9 %

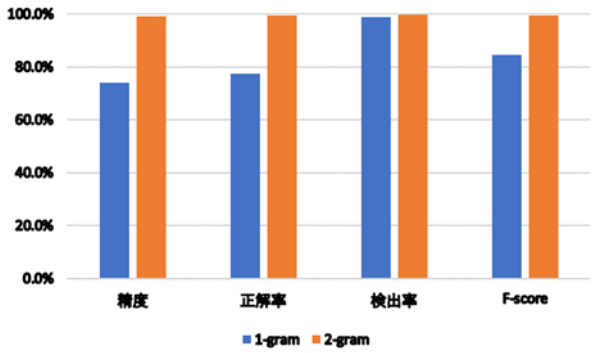

図 1　BOS データセット評価結果

1-gram による分類においてはどちらのデータセットも感染時通信を正常通信であると判定する偽陰性の値が大きくなっている．特に，CTU データセットにおいては，偽陰性率 100 %となり，感染通信すべてを正常通信と誤って判断しており感染時通信を検出できていない．

2-gram による分類においてはどちらのデータセットも偽陰性率が CTU の場合 0.1 %，BOS の場合 2 %と小さく抑えられていることがわかる．

4.　考察

本実験において，高精度での検知ができた理由を知るために，学習で用いた，ペイロード通信を調べた．その結果，共通なペイロード情報を持つパケットが多数確認できた．特にトロイの木馬型のマルウェアの感染データに関しては末尾部のみが変化したパケットが連続して通信されていることがわかった．これは，C&C サーバーに生存を通知するためのハートビート通信であると思われる．

類似した通信が繰り返して行われたことが 2-gram での攻撃検知の精度を高める要因となったと考える，また 1-gram では通信の類似性を十分に学習できなかったことが 1-gram での精度の低下に関係していると考えられる．

5.　おわりに

ボットネットとトロイの木馬に感染したサーバの通信ログから感染を検知する検知手法を提案した．

検知方式は，RNN を用い，N-gram 法を用いて分割した文字列を学習し分類を行った．CTU と BOS のデータを使用し，1-gram では偽陰性率が高かったが，2-gram では精度，正解率，検出率，及び F-score のいずれも高く，感染を検知できることがわかった．また，偽陰性率も低く押さえられていることが分かった．

今後は他のデータセットに対しても同様に分類できるのか，また感染時通信を正しく分類するために有効な文字列の調査などを行う．

参考文献

[1] M. Rhode, P. Burnap, K. Jones,"Early Stage Malware Prediction Using Recurrent Neural Networks,"Computers & Security,vol.77, pp. 578-59,2018

[2] P. Torres, C. Catania, S. Garcia and C. G. Garino, "An analysis of Recurrent Neural Networks for Botnet detection behavior," 2016 IEEE ARGENCON, pp. 1-6, 2016

[3]M. Grill, J. Stiborek and A. Zunino, "An empirical comparison of botnet detection methods" Sebastian Garcia," . Computers and Security Journal, Elsevier. Vol45, pp. 100-123, 2014

[4] 荒木粧子, 他, "ウェア対策のための研究用データセット ～ MWS Datasets 2019 ～, 情報処理学会, Vol.2019-CSEC-86, No.8, 2019

Copyright ©2021 Information Processing Society of Japan.
All Rights Reserved.