ISS-SP-207

Android マルウェアによるスキャン活動の分析

鈴木 男人　　鈴木 貴之　　宮保 憲治
東京電機大学大学院　情報環境学研究科

1. はじめに

マルウェアによる感染を防止する対策として，ソフトウェアアップデートの迅速な実施が挙げられる．しかしながら，経済的な問題などの理由により，古いバージョンを使用し続ける人々も多い．特に近年普及が著しい Android OS のバージョン別のシェアは，2015 年 1 月の時点で，約 1 割が古い 2 系であると報告されている[1]．そのため，バージョンによりマルウェアの感染状況が実際にどの程度異なるのかを把握し，ユーザに対して適切に対策を促す必要がある．

本稿では，Android マルウェアによるスキャン活動の分析[2,3]を更に進める．具体的には，Android OS のバージョン間において，パケットのヘッダ情報で差異が見られた特徴の組み合わせを用いることで，スキャン活動を行う Android マルウェアのバージョン別の分布を分析した結果を述べる．

2. ヘッダ情報の比較実験

Android OS のバージョンにより，パケットのヘッダ情報が異なることを検証するため，Android OS のバージョン 2 系および 4 系の端末 139 種類の TCP SYN パケットを収集した．

ヘッダ情報の比較を行った結果，TCP ヘッダの Winodw サイズと Window スケールで差異が見られた．図 1 に，Window サイズおよび Window スケールの，Android 端末数の累積分布関数の比較を示す．図 1 より，Window サイズは，2 系は 5840，4 系は 14600 で端末数が大きく増加しているのが分かった．また，Window スケールは，2 系は 5 以下，4 系は 6 以上が多い傾向にあることが分かった．表 1 に，Window サイズの閾値を 8192 に，Window スケールの閾値を 6 に設定したときの端末数の比率を示す．閾値により，7 割以上の確率で，バージョン 2 系と 4 系の Android 端末による通信の弁別が可能であることが確認できた．

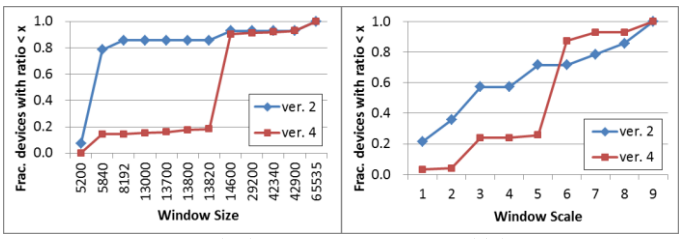

図 1：Window サイズ（左）と Window スケール（右）の累積分布関数

表 1：閾値によるバージョン別端末数の比率

	wsize ≤ 8192	wscale < 6	wsize > 8192	wscale ≥ 6
Version 2	0.86	0.71	0.14	0.26
Version 4	0.14	0.29	0.86	0.74

3. Android 端末による通信の抽出

スキャン活動を行う Android マルウェアのバージョン別の分布を分析するため，先行実験[3]で用いた手法（図 2）により，ダークネットトラヒックデータから Android 端末による通信を抽出した．データは，MWS Datasets 2014[2]より提供された NICTER Darknet Dataset 2014 の 2014 年 1 月 1 日から 2014 年 12 月 31 日までを活用した．

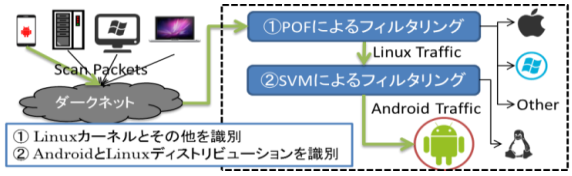

図 2：Android 端末による通信の抽出法の概要

4. ダークネットトラヒックデータの分析

ダークネットトラヒックデータから抽出した Android 端末による通信の分析を行った．図 3 に，ダークネットにおける Android 通信の，Window サイズおよび Window スケールの，ホスト数の累積分布関数を示す．Window サイズは，殆どが 5400 から 5840 の間で増加し，Window スケールは，1 および 2 で大きく増加していることが分かった．表 1 と同様に，Window サイズの閾値を 8192，Window スケールの閾値を 6 に設定した．その結果，約 98%のホストの Window サイズが 8192 以下であり，約 99%のホストの Window スケールが 6 未満であることが判明した．表 1 の結果と合わて考察すると，Window サイズ 8192 以下または Window スケール 6 未満である端末は，2 系が大半であり，ダークネットにおける Androi 端末からのスキャン通信の殆どは，古い Android 端末によるものであることが推察できる．Android OS のバージョン 2 系におけるセキュリティは不十分であり，ユーザに対して新しい端末への移行を強く働きかけるなど，対策を講じる際の一つの判断材料として，この結果を活用できる可能性がある．

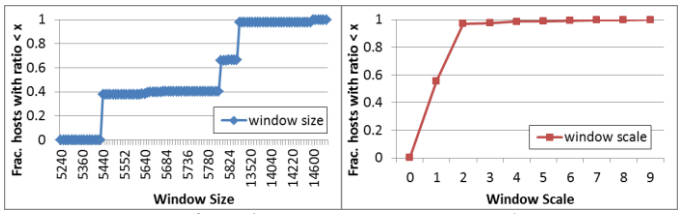

図 3：ダークネットにおける Android 通信の Window サイズ（左）と Window スケール（右）の累積分布関数

5. おわりに

本稿では，パケットのヘッダ情報の比較を行い，スキャン活動を行う Android マルウェアのバージョン別の分布を分析した．その結果，殆どが Android OS のバージョン 2 系の端末からと推測される通信であることが判明した．

参考文献

[1] Dashboards | Android Developers, https://developer.android.com/about/dashboards/
[2] 鈴木 貴之 他，“ダークネットにおける Android 端末の通信分析，” コンピュータセキュリティシンポジウム 2014 論文集，pp.314-312, 2014-10.
[3] 鈴木 男人 他，“Wi-Fi を経由した Android マルウェアのスキャン分析，” 電子情報通信学会 東京支部学生会 研究発表会，2014-02.（発表予定）
[4] 秋山 満昭 他，“マルウェア対策のための研究用データセット MWS Datasets 2014，“ 情報処理学会研究報告 コンピュータセキュリティ(CSEC), Vol.2014-CSEC-66, No.19, pp.1-7, 2014.