動的解析による Android マルウェアの解析

吉川無我

2015 年 1 月 9 日

目次

1 はじめに

今日では，スマートフォンが非常に身近な存在であり，その中でも Android 端末は最も世界中で普及している． IDC による，世界中のスマートフォンの OS 別のシェアの調査 [1] においては，Android 端末は 80% 以上のシェアがあると示している． つまり，Android 端末は他の OS の端末，iOS, Windows Phone, Black Berry OS に比べて，より多くのユーザによって使われていることがわかる．Android がオープンソースであることがその理由の 1 つである．様々なメーカーによって開発が行われ，多種多様な製品が世界中で販売されている．

しかし，Android の普及に伴い，Android 端末を標的にした Android アプリのマルウェアによる被害が増えている．先に述べたように，Android はオープンソースであるため，攻撃者は脆弱性を見つけることは他のモバイル端末 OS に比べると容易だ．Cisco の 2014 年のレポート [2] によると，モバイル向けマルウェアの 99.9% が Android を標的にしていると報告している．Y.Zhou, X.Jiang の研究 [3] では，彼らの研究に用いたデータセットの数の増加から，Android マルウェアが急激に増加したことを報告している．具体的には，2011 年の 6 月では 209 個だったのが，同年 10 月には 1260 個にも増加していた．2014 年の 9 月には，ロシアで銀行口座を狙った Android マルウェアを作成したとして，2 名の逮捕者が出ている．これらの事例を見てわかるように，Android 端末を標的にしたマルウェアによる被害は深刻であり，Android 端末のユーザは危険にさられている

code.google.com が提供している既存の Android マルウェアの解析ツールとして androguard [4] , droidbox [5] の 2 つがある．androguard は Android アプリのコード解析を行うことで，アプリ内のクラスごとの関係を示すグラフを作り，危険だと判定した部分のみを赤く表示する．もし，マルウェアが外部から攻撃コードをダウンロードするという攻撃をする場合，静的解析では，対応することはできない．droidbox はエミュレータ上でマルウェアを動かし，データのやりとり，ファイルの読み書き，などを動的に監視することでマルウェアの挙動を解析している．しかし，droidbox はマルウェアが実際に実機でどのような挙動をするかを正確にとらえているとは限らない．なぜならマルウェアがエミュレータ上で動いているのを検知して，挙動を変える可能性もあるからだ．

マルウェアの実際の挙動をより詳細に調べるためには，実機でマルウェアを動かし，その挙動から解析を行う必要がある．そこで本研究では実機における Android マルウェアの動的解析を提案する．マルウェアを実機で動かしながら，ログを得ることで解析を行う．提案手法をマルウェアに適用することで，実行されたメソッド名，クラス名，引数の型名と値を得ることができる．Android アプリは APK ファイルという 1 つのファイルにまとめられて端末にインストールされている．その APK ファイルから Java クラスファイルを取り出して，ログを得たいメソッドを含むクラスの Java クラスファイルを書き換える．Java クラスファイルを書き換えたマルウェアの APK ファイルを実機にインストールして動かすと，動的にログを得ることができる．それを用いてマルウェアの解析を行う．

本提案によりマルウェアを解析できたかを示すためにインターネットのサイト上で入手した 11 個 の Android マルウェアを用いて 2 種類の実験を行った．1 つめの実験では，11 個の検体において，不正なコードを含むと思われるクラスのそれぞれのメソッドの始めにログを出力するようにクラスファイルを変更した．その結果，11 個中 5 個のマルウェアから，不正な挙動を表すログを得ることができた，例えば，SMS の送信や，外部からのコードの入手を示していた．2 つめの実験では，先の 11 個の検体の中の 1 つである，iMatch に対してのみ行った，1 つめの実験で行ったクラスファイルの変更に加えて，あるメソッド内でのメソッド

呼び出しの情報も出力するようにした．この実験の結果として，これの攻撃手段である，SMS 送信のための Android API とそのメソッドを呼び出しているメソッドとそのクラスを特定することができた．

本論文の構成を以下に示す．

2　Android を標的にしたマルウェア

explanation of Android

2.1　悪意ある Android アプリ

2.2　Android アプリの構成

classes.dex の説明もここ

3 関連研究

Dissecting Android Malware

Analyzing Unsafe and Malicious Dynamic Code Loading in Android Applications

others

4 提案

4.1 全体の流れ

4.2 解析手順

4.3 ログコードの挿入箇所

4.3.1 メソッドの先頭にコードを挿入

4.3.2 メソッド呼び出しの’前後でコードを挿入

5　実装？

6 実験

6.1 目的

6.2 実験方法

6.3 実験結果

7　おわりに

7.1　まとめ

7.2　今後の課題

謝辞

参考文献

[1] IDC http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[2] Cisco 2014 Annual Security Report

[3] Yajin Zhou Xuxian jiang "Dissecting Android Malware: Characterization and Evolution" In *IEEE Symposium on Security and Privacy*, 2012

[4] androguard https://code.google.com/p/androguard/

[5] droidbox https://code.google.com/p/droidbox/