セカンドアプリ内包型 Android マルウェアの検知

磯原 隆将† 川端 秀明† 竹森 敬祐† 窪田 歩† 可児 潤也‡ 上松 晴信‡ 西垣 正勝‡

†KDDI 研究所
356-8502 埼玉県ふじみ野市大原 2-1-1-5
{ta-isohara, kawabata, takemori, kubota}@kddilabs.jp

‡静岡大学
432-8011 静岡県浜松市中区城北 3-5-1
{cs08028, cs07003}@s.inf.shizuoka.ac.jp, nisigaki@inf.shizuoka.ac.jp

あらまし Androidアプリは，実行ファイルや画像ファイル等をZIP形式で圧縮したファイルとして配布される．昨今，正規アプリを解凍して悪性アプリを追加し，これを再圧縮して作成されるAndroidマルウェアが増えている．このように，正規アプリに追加される悪性アプリをセカンドアプリと呼ぶことにする．セカンドアプリを追加する際，マルウェア対策ソフトによる検知を逃れるために，ファイル名や拡張子が偽装される．そこで本研究では，解凍後のフォルダに含まれるファイルの属性に注目してセカンドアプリを検出する手法を提案する．提案手法は，本来ZIPファイルにAndroidアプリが含まれないことに注目したセカンドアプリ検出手法であり，Android特有のマルウェアに対する普遍的な検出手法としての有効性を示す．

Detection Technique of Android Malware with Second Application

Takamasa Isohara† Hideaki Kawabata† Keisuke Takemori† Ayumu Kubota†
Jyunna Kani‡ Harunobu Agematsu‡ Masakatu Nishigaki‡

†KDDI R&D Laboratories
2-1-15 Ohara, Fujimino, Saitama 356-8502, JAPAN
{ta-isohara, kawabata, takemori, kubota}@kddilabs.jp
‡Shizuoka University
3-5-1 Johoku, Naka-ku, Hamamatsu, Shizuoka 432-8011, JAPAN
{cs08028, cs07003}@s.inf.shizuoka.ac.jp, nisigaki@inf.shizuoka.ac.jp

Abstract Android application is distributed as a zip formatted file that contains execution and resource files. Android malware is built by injecting a malicious android application into a legitimate application package. File name and/or extension of malicious application are obfuscated in order to avoid anti-malware tools. In this paper, we propose a detection technique of Android malware included another application, which focuses attributes of files within an application package. Our idea is designed on an assumption that a legitimate application does not contain another application. We implement the detection system and evaluate the detection ratio to indicate a validity of Android malware detection.

1 はじめに

Android プラットフォームは，アプリの公開にあたって事前審査を必要としないため，世界中の開発者が作成した多くのアプリを自由に利用できる．一方で，情報漏洩や高額 SMS 送信等を行うマルウェアが出現している．特に，正規アプリに悪意の Android アプリ（これを「セカンドアプリ」と呼ぶことにする）を内包するマルウェアは，従来のマルウェアに比べて作成が容易であること，セカンドアプリを変更するだけで多数の亜種を作成可能であることから，猛威をふるっている[1-3]．

マルウェアから端末を保護する手段として，マルウェア対策ソフトの導入[4, 5]や，アプリの事前審査の実施がある．しかし，多数の亜種の出現に対して，マルウェア対策ソフトのパターンファイルの更新が間に合わずに感染すること，事前審査における見逃しが発生することが懸念されている．これに対して，セカンドアプリ固有の特徴に依存しない，異常検知に基づく対策手法が有効と考えられる．

そこで本研究では，異常検知手法に基づき，正規アプリに内包されるセカンドアプリを的確に検知する，セカンドアプリ内包型 Android マルウェア検知手法を提案する．これは，ファイルの属性に注目する手法であり，検査対象のアプリの内部に，Android アプリとしての特徴を有するファイルを発見した場合に，検査対象アプリをマルウェア感染アプリと判定する手法である．提案手法は，Android アプリに共通の特徴に注目するため，ファイル名や拡張子を変更したセカンドアプリを内包する多数の亜種に対しても，未知のマルウェアを的確に検知することが可能である．プロトタイプシステムを実装し，マーケットプレイスや一般の Web サイトから収集したアプリを用いて検知率評価を行った．評価結果より，提案手法がセカンドアプリ内包型 Android マルウェアを的確に検知することを示す．

以下，2 章でセカンドアプリ内包型 Android マルウェアの特徴，生成手法，および感染時の挙動を説明する．3 章でファイル属性に注目したマルウェア検知手法について述べ，4 章でプロトタイプシステムによる検知率評価の結果を報告する．5 章で関連技術を説明し，最後に 6 章でまとめる．

2 セカンドアプリ内包型 Android マルウェアの特徴と挙動

本節では，セカンドアプリ内包型 Android マルウェアの特徴と感染時の挙動について説明する．

2.1 トロイの木馬型 Android マルウェアの定義と分類

Android アプリは，アプリの設定を記述するマニフェストファイル，実行ファイル，および画像・音声・データベース等の各種リソースファイル一式を ZIP 形式で圧縮し，アプリ開発者が署名を施したファイルである．拡張子が「.apk」であることから，APK ファイルと呼ばれることもある．

マニフェストファイルは，実行モジュールの情報，アプリに付与した権限の情報などが記述されており，AndoridManifest.xml という固有のファイル名を持つ．実行ファイルは，Java のソースコードを，Android プラットフォームのアプリ実行用仮想マシンである Dalvik 向けに変換した，DEX（Dalvik Execution）形式と呼ばれるファイルであり，classes.dex という固有のファイル名を持つ．

Android アプリは，ZIP ファイルを解凍してコンテンツを追加し，再圧縮と再署名を行った場合もアプリは正常に動作する．また，実行ファイルは，逆コンパイルツールを用いてソースコードを生成し，これに任意のコードを追加して，再度 DEX ファイルを生成する場合も，9 割程度が正常に動作することが報告されている[6]．

このように，Android アプリの改造が容易であることから，正規アプリに見せかけて悪意のコードを含む，トロイの木馬型 Android マルウェアが多く出現している．トロイの木馬型 Android マルウェアは，実行ファイルに悪意のコードを追加す

るタイプと，これに加えて，APK ファイルに悪意の Android アプリを追加するタイプが知られている．特に後者のタイプは，悪意の Android アプリの種類を変更することで，多数の亜種を容易に生成できるため，マルウェア対策ソフトや事前審査における見逃しが懸念され，的確な検知手法が必要となる．本論文では，正規アプリに追加する Android アプリをセカンドアプリと呼ぶこととして，これを内包するマルウェアをセカンドアプリ内包型 Android マルウェアと定義する．

2.2 セカンドアプリ内包型 Android マルウェアの作成手法

図 1にセカンドアプリ内包型 Android マルウェアの作成手法を示す．マルウェア作成者は，APKファイルに，セカンドアプリとroot権限を奪取するエクスプロイトコードを追加する．また，DEX ファイルとマニフェストファイルに悪性コードを追加し，再圧縮と再署名を施して APK ファイルを再生成する．

このとき，マルウェア作成者は，セカンドアプリの存在を隠蔽するため，セカンドアプリの名前や拡張子を変更する．拡張子については，実行時に.apk に戻す処理を正規アプリに組み込むことで，正常に動作する．

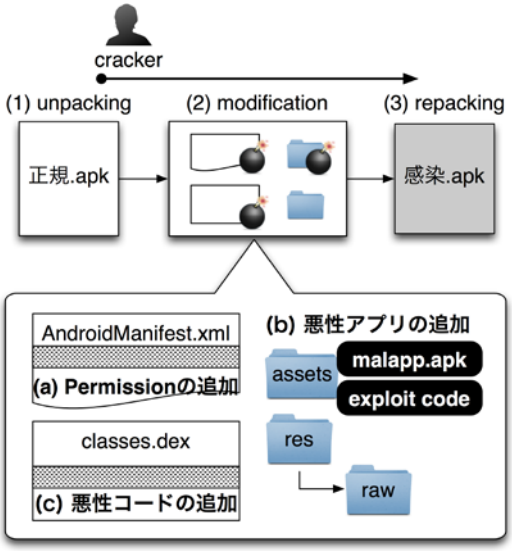

図 1 マルウェア作成の事例

2.3 セカンドアプリ内包型 Android マルウェア感染時の挙動

セカンドアプリ内包型 Android マルウェアの感染時の挙動の一例を図 2に示し，要点を以下に述べる．

A) マルウェアへの感染

ユーザは，マーケットプレイスや一般の Web サイトで公開されるセカンドアプリ内包型 Android マルウェアを取得して端末にインストールすることで感染する．

B) マルウェアの発症

感染したアプリの起動に伴って DEX ファイルに追加された悪性コードが実行される．悪性コードは，APK ファイルに含まれるエクスプロイトコードを実行して，端末の root 権限を取得する．つづいて，root 権限を用いて，セカンドアプリをインストールする．ここで，APK ファイルを，/data/app または/system/app 以下に配置することで，端末ユーザによる承諾を伴わずにアプリのインストールを完了できることから，root 権限を悪用したサイレントインストールが行われる．

3 ファイル属性に注目したセカンドアプリ検知

正規 Android アプリでは，内部に別の APK ファイルを含めることは起こり得ない．したがって，

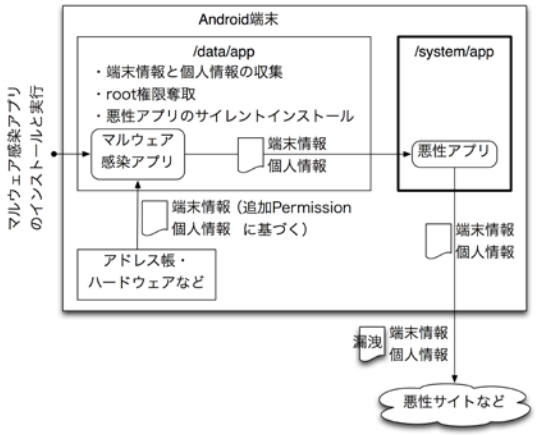

図 2 マルウェア感染時の挙動の例

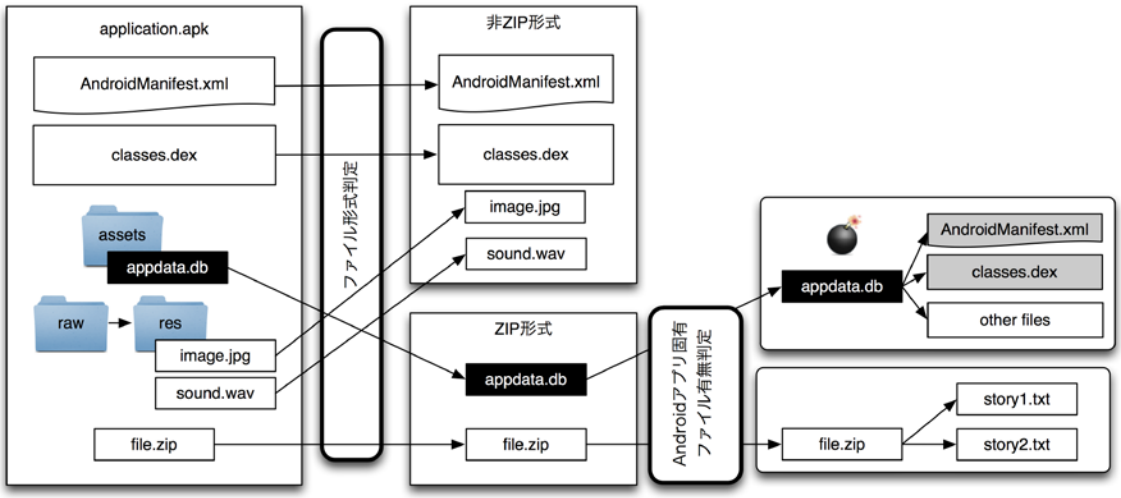

図 3 セカンドアプリ内包型 Android マルウェア検知の処理手順

APK ファイルの内部に含まれる別の APK ファイルの検査を行うことで，セカンドアプリ内包型マルウェアを検知することが可能となる．Android アプリは，1)ファイル形式が ZIP であること，2)内部に AndroidManifest.xml と classes.dex という名称のファイルを含むこと，の 2 つを特徴とする．以下，APK ファイルのコンテンツに，これら 2 つの特徴を有するファイルを発見した場合，該当の APK ファイルはセカンドアプリ内包型 Android マルウェアであると判定する手法について説明する．

3.1 ファイル形式判定

APK パッケージに含まれるファイルのうち，ZIP 形式のファイルを発見する処理である．本処理では，ファイルのヘッダー情報を参照し，ZIP ファイルを発見する．なお，セカンドアプリを複数回圧縮して存在を隠蔽する攻撃を考慮して，圧縮形式のファイルは，再帰的に解凍処理を行う．ここで ZIP 形式のファイルと判定されたものを「Android アプリ固有ファイル有無判定」処理の対象として，それ以外のファイルは，「Android アプリ固有ファイル有無判定」処理を行わない．

3.2 Android アプリ固有ファイル有無判定

3.1 節の処理で ZIP 形式と判定されたファイルについて，ファイル名が AndroidManifest.xml および classes.dex の 2 ファイルの有無を確認する．具体的には，ZIP ファイルを解凍し，パッケージに含まれるファイルの名称を検査する．

本処理において，2 つのファイルが確認される場合に，検査対象のファイルをセカンドアプリと判定する．いずれか一方のファイルのみ確認される場合は，Android アプリとして不完全であるとみなし，セカンドアプリと判定しない．

3.3 マルウェア判定の条件

3.1 節，3.2 節の処理結果より，ファイル名称が AndroidManifest.xml および classes.dex のファイルを含む ZIP 形式のファイルを保有する場合，検証対象のアプリをセカンドアプリ内包型 Android マルウェアと判定する．

4 検知率評価

提案手法を用いたマルウェア検知のプロトタイプシステムを実装し，サンプルを用いて検知率を評価した．以下，検知結果とマルウェアの形態に関する考察を述べる．

4.1 検知結果

検知率を評価するため，Android Market[7]か

表 1 マルウェアの形態

タイプ	検知数	APK ファイル内に内包されるエクスプロイトコードの配置場所と名称	セカンドアプリとして検知されたファイルの配置場所と名称
DroidDream	5	assets/exploid assets/rageagainstthecage	assets/sqlite.db
BaseBridge	3	res/raw/rageagainstthecage	res/raw/anserverb
N/A	1	res/raw/exploid	res/raw/superuser_cd res/raw/superuser_ef
DroidKungFu	1	assets/gjsvro assets/ratc	assets/legacy
DroidKungFu	1	assets/gjsvro assets/ratc	assets/legacy assets/alipay_plugin222_0223.apk
N/A	1	assets/gingerbreak.png	assets/superuser.png
N/A	1	res/raw/rageagainstthecage	res/raw/superuser.apk

ら取得した 587 アプリと，一般 Web サイト[8]からマルウェア検体として取得した 13 アプリの，計 600 アプリをサンプルとして使用した．

評価の結果，Android Market から入手した 2 アプリと，一般 Web サイトから入手した 12 アプリがマルウェア感染アプリと判定された．Android Market から入手した 2 アプリのうち，1 アプリは，エクスプロイトコードを含まず，また，セカンドアプリ自身についても，APK ファイルへの署名が不完全であったため，Android アプリとして正しく動作しないものであった．これは，開発上の不備により不完全な APK ファイルを混入したままリリースしてしまったと推測される．もう一方の 1 アプリと一般 Web サイトから入手した 12 アプリの計 13 アプリは，エクスプロイトコードとセカンドアプリを内包することから，明確にマルウェアと判定できるアプリであった．

4.2 マルウェアの形態に関する考察

明確にマルウェアと判定できる 13 アプリについて，エクスプロイトコードおよびセカンドアプリとして検知されたファイルの配置場所と名称に注目して形態の分類を行った．分類結果を表 1 に整理する．なお，検知結果のうち，マルウェア対策ソフトベンダー等によってマルウェアの定義と命名がなされているものについては，定義名称を「タイプ」欄に記した．

表 1より，エクスプロイトコード・セカンドアプリとして検知されたファイルともに，任意のファイルを配置するために用いられる/assets，/res/raw のいずれかのディレクトリにのみ配置されていた．また，セカンドアプリとして検知された 8 種類のファイルのうち，6 種類がファイル名や拡張子の隠蔽を行っていた．その内訳は，assets/sqlite.db が 5 件，res/raw/anserverb が 3 件，assets/legacy が 2 件，assets/supreuser.png，res/raw/superuser_cd，res/raw/superuser_ef がそれぞれ 1 件であった．assets/alipay_plugin222_0223.apk は拡張子を偽装していないが，セカンドアプリ検知の判定条件に一致したため検知された．また，res/raw/superuser.apk は，apk ファイルを GZIP 形式で圧縮したファイルであり，一度 GZIP 圧縮を解凍することで，Android アプリとして実行可能な APK ファイルが抽出された．これは，多重の圧縮を行うことで，セカンドアプリの隠蔽を意図したと想定される．なお，提案手法はセカンドアプリを暗号化した場合，ファイル形式判定において ZIP ファイルを発見できないために見逃しが生じるが，今回の 600 サンプルについて調査した結果においては，セカンドアプリを暗号化して内包したマルウェアは発見されなかった．

5　関連研究

Android 端末におけるマルウェア対策として，マルウェア対策ソフト[4]やリスク診断ソフト[5]がある．

マルウェア対策ソフトは，マルウェアのファイル名やハッシュ値等をシグネチャとしてブラックリスト登録し，Android 端末にインストールされたアプリやそのコンテンツに，リストの登録内容と一致するファイルを発見した場合に，該当のアプリやファイルをマルウェアとして検知する方式である．しかし，多数の亜種の出現に対して，マルウェア対策ソフトのパターンファイルの更新が間に合わずに感染する恐れがある．

また，リスク診断ソフトは，端末にインストールされたアプリのパーミッション情報を収集し，情報漏洩等の危険性を有するアプリについて，警告を表示する．しかし，パーミッションはネットワーク通信やデバイスの利用など，おおまかな粒度で権限を定義しているため，パーミッションに基づくリスク分析は，精度が低いことが課題となる．

6　おわりに

本研究では，Android 端末を対象としたトロイの木馬型マルウェアのうち，APK ファイル内部に第 2 の Android アプリを内包するアプリを，セカンドアプリ内包型 Android マルウェアと定義して，これを検知する手法を提案した．提案手法は，APK ファイル内に，1）ZIP 形式のファイルであること，2）内部に AndroidManifest.xml と classed.dex という名称のファイルを含むこと，の全ての条件を満たすファイルが発見される場合に，これを含む APK ファイルを，セカンドアプリ内包型 Android マルウェアと判定する．プロトタイプシステムを実装して，Android Market と一般 Web サイトから収集した合計 600 のアプリについて検査を行った結果，14 アプリがマルウェアと判定され，うち，13 アプリが，エクスプロイトコードとセカンドアプリを含むために，明確にセカンドアプリ内包型 Android マルウェアと判定できるものであった．提案手法は，アプリの事前審査等に用いることで，未知のマルウェアを的確に検知できる．

参考文献

[1] Threat Description: Trojan:AndroidOS/Fakeplayer.A, http://www.f-secure.com/v-descs/trojan_androidos_fakeplayer_a.shtml.

[2] The Official Lookout Blog | Update: Security Alert: DroidDream Malware Found in Official Android Market, http://blog.mylookout.com/2011/03/security-alert-malware-found-in-official-android-market-droiddream/.

[3] One Year Of Android Malware (Full List) Blog di Paolo Passeri, https://paulsparrows.wordpress.com/2011/08/11/one-year-of-android-malware-full-list/.

[4] Mobile Security Personal Edition for Android Smartphones and Android Tablets - Trend Micro USA, http://us.trendmicro.com/us/products/personal/mobile-security-for-android/.

[5] tSpyChecker, http://www.taosoftware.co.jp/android/spychecker/.

[6] William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri. A Study of Android Application Security, Proceedings of the 20th USENIX Security Symposium, August, 2011. San Francisco, CA.

[7] Android Market, https://market.android.com/.

[8] contagion, http://contagiodump.blogspot.com/.