US009800609B2

(12) **United States Patent**
**Liao**

(10) **Patent No.: US 9,800,609 B2**
(45) **Date of Patent: Oct. 24, 2017**

(54) **METHOD, DEVICE AND SYSTEM FOR DETECTING MALWARE IN A MOBILE TERMINAL**

(71) Applicant: **Tencent Technology (Shenzhen) Co., Ltd.**, Shenzhen, Guangdong (CN)

(72) Inventor: **Chongliang Liao**, Guangdong (CN)

(73) Assignee: **Tencent Technology (Shenzhen) Company Limited**, Shenzhen, P.R. (CN)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 8 days.

(21) Appl. No.: **14/622,074**

(22) Filed: **Feb. 13, 2015**

(65) **Prior Publication Data**

US 2015/0163232 A1 Jun. 11, 2015

**Related U.S. Application Data**

(63) Continuation of application No. PCT/CN2014/080793, filed on Jun. 26, 2014.

(30) **Foreign Application Priority Data**

Jul. 30, 2013 (CN) ..... 2013 1 03261916

(51) **Int. Cl.**

| | |
|---|---|
| ***H04L 29/06*** | (2006.01) |
| ***G06F 21/56*** | (2013.01) |
| ***G06F 9/445*** | (2006.01) |

(52) **U.S. Cl.**

CPC ..... ***H04L 63/145*** (2013.01); ***G06F 8/61*** (2013.01); ***G06F 21/563*** (2013.01); ***G06F 21/567*** (2013.01); *G06F 2221/2115* (2013.01)

(58) **Field of Classification Search**

CPC ..... G06F 8/61; G06F 21/56–21/568; G06F 2221/2115; H04L 63/1416; H04L 63/1441–63/145

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,281,399 B1 10/2012 Chen et al.
2009/0282483 A1* 11/2009 Bennett ..... H04L 63/1416 726/23

(Continued)

FOREIGN PATENT DOCUMENTS

CN 102123396 A 7/2011
CN 102663281 A 9/2012

(Continued)

OTHER PUBLICATIONS

Yajin Zhou, Zhi Wang, Wu Zhou, and Xuxian Jiang (Zhou et al.) "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets", 19th Annual Symposium on Network and Distributed System Security (NDSS Symposium 2012). <http://www.internetsociety.org/sites/default/files/07_5.pdf>. Published: Feb. 7, 2012.*

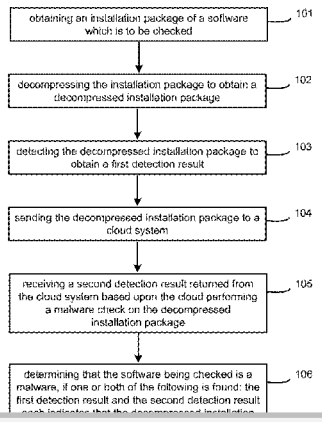
(Continued)

*Primary Examiner* — Kevin Bechtel
(74) *Attorney, Agent, or Firm* — Brinks Gilson & Lione

(57) **ABSTRACT**

A method, device and system for detecting malware in a mobile terminal are disclosed. The method includes at least the following operations: obtaining an installation package of a software which is to be checked; decompressing the installation package to obtain a decompressed installation package; detecting the decompressed installation package to obtain a first detection result; sending the decompressed installation package to a cloud system; receiving a second detection result returned from the cloud system based upon the cloud performing a malware check on the decompressed installation package; determining that the software being checked is a malware, if one or both of the following is found: the first detection result and the second detection result each indicates that the decompressed installation package is abnormal.

**15 Claims, 4 Drawing Sheets**



(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 2010/0333203 | A1* | 12/2010 | Tsviatkou | G06F 21/566 726/23 |
| 2011/0145920 | A1 | 6/2011 | Mahaffey et al. | |
| 2012/0330801 | A1* | 12/2012 | McDougal | G06F 21/577 705/32 |
| 2013/0263266 | A1* | 10/2013 | Bojaxhi | H04L 63/145 726/23 |

FOREIGN PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| CN | 102663286 | A | 9/2012 |
| CN | 102779257 | A | 11/2012 |
| CN | 103400076 | A | 11/2013 |

OTHER PUBLICATIONS

International Preliminary Report on Patentability and Written Opinion received in PCT Application No. PCT/CN2014/080793 dated Feb. 2, 2016.

International Search Report received in PCT Application No. PCT/CN2014/080793 dated Sep. 26, 2014.

Fang, "Malware Implementation and Detection on Android," *Thesis Submitted to Nanjing University of Posts and Telecommunications for the Degree of Master of Engineering*, Jun. 15, 2013.

Wenjun et al., "A Detection Method and System Implementation for Android Malware," *Journal of Xi'an Jiaotong University*, vol. 47:10, Oct. 2013.

First Office Action received in Chinese Application No. 201310326191.6 dated Jul. 1, 2015.

* cited by examiner

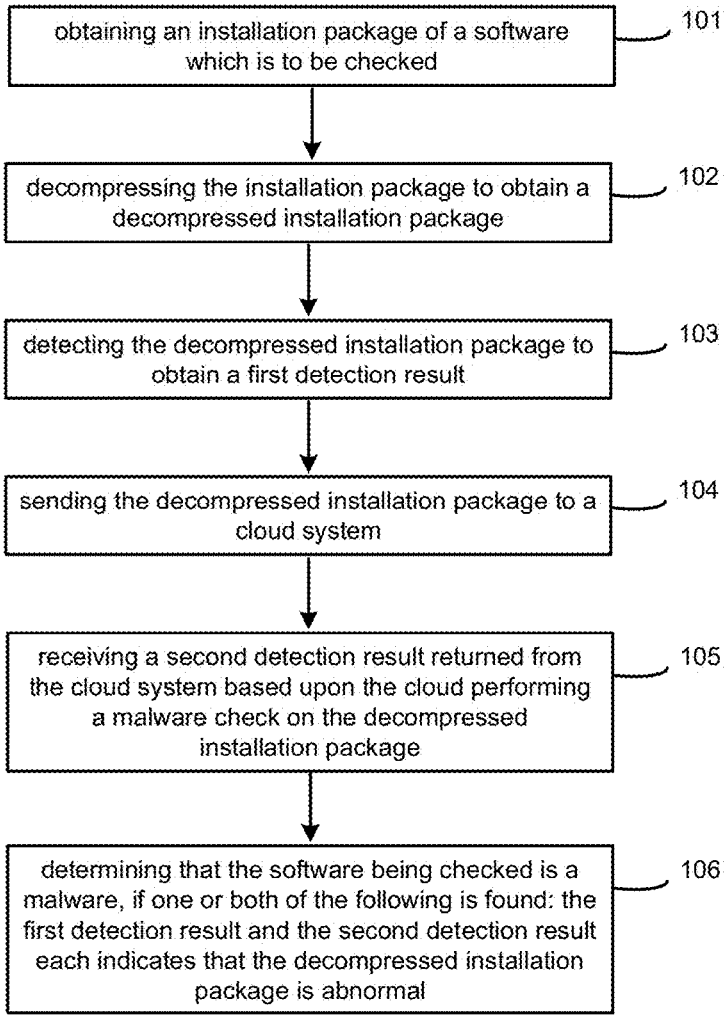



Figure 1

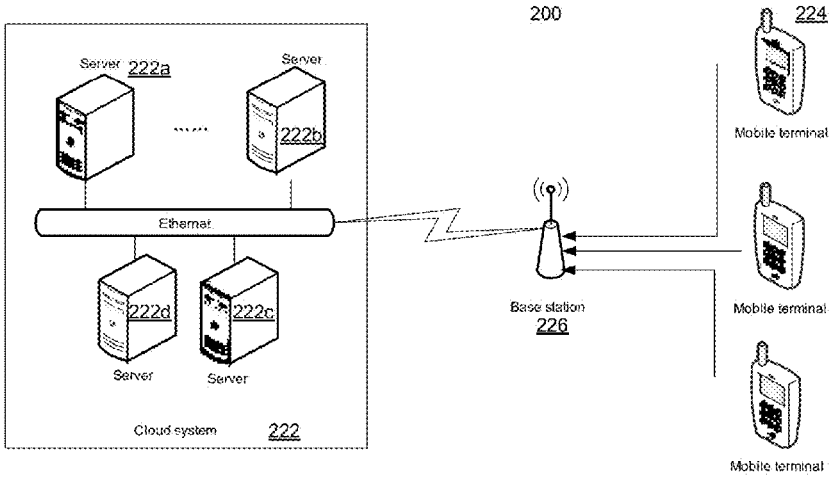



Figure 2a

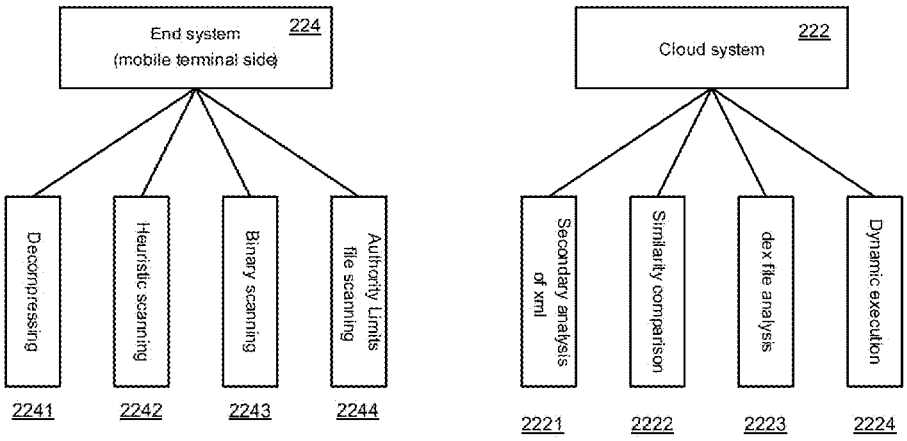



Figure 2b

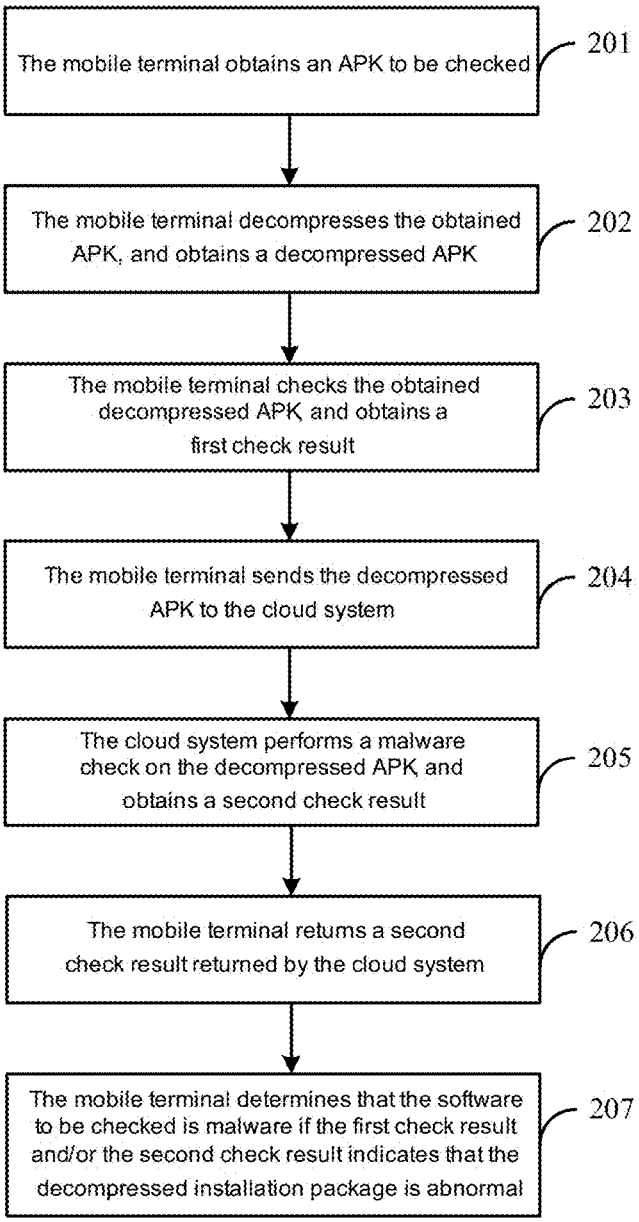



Figure 2c

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.