平成23年度　卒 業 論 文

邦文題目

Android端末をターゲットとしたボットによる被害防止策の提案

英文題目

Proposal of Measures to Prevent Damage from Bots on Android terminals

情報工学科

(学籍番号: 080425210)

渡邊研究室

戸田　尚希

提出日: 平成24年2月9日

名城大学理工学部

内容要旨

近年，Android 端末をターゲットとしたボットの登場により，ボット対策が重要な課題となりつつある．ボットは，ユーザの意図しないメール送信，特定のサーバへの端末情報の送信，DDoS 攻撃への加担などの被害をもたらす．

本稿では，ボットの完全な感染防止は困難であることから感染した Android 端末がもたらす 2 次被害の防止について検討した．ボット被害がネットワークへの送信により発生すること，キー入力操作はボットには出来ない操作であることに着目し，送信前にキー入力操作があったかどうかをチェックし，通信制御やユーザへの警告を行うことで Android 端末のボットによる被害を防止する．

Abstract

Recently, the advent of bots that target the terminal Android, A bot countermeasure become an important issue. Bots bring about sending mail is not intended by the user, sending the personal information to a server terminal, and complicity to DDoS attack.

In this paper, because a prevention of a complete bot infections is difficult, considered about prevention of secondary damage by Android terminals. We focus that damage of bot occur to sending packet to network and bot can't keystroke, so check to see if there was prior to sending keystrokes, a warning to the user and the communication control to prevent damage by bot of Android terminal.

目 次

第1章　はじめに

インターネットの発展に伴い，ウイルスの被害が大きな問題となっている．ボットは悪質化したウイルスの一種で，ボット感染端末はボットネットと呼ばれるネットワークを構築する特徴を持つ．近年では，ボットネットによるスパムメールの送信やDDoS（Distributed Denial of Service）攻撃，情報の奪取など様々な問題が蔓延している．ボットはオープンソースとなっているため，新種・亜種が数多く存在する．このため，ボット対策としては新種・亜種のボットに対応する必要がある．しかし，現状は新種・亜種のボットが出回った後に対策が打たれているように，ボット対策は常に後手に回らざるを得ないのが現状である．ボットは攻撃者（Herder）の指示があるまで待機するため，ボット感染端末のユーザが感染に気付きにくいという問題点がある．また，ボットは複数の指令サーバと通信を行う．仮に1つの指令サーバを停止できたとしても他のサーバを介して命令を送り続けることが出来る．このため，ボット対策をサーバに対して施すことは難しいとされている．

近年ではスマートフォンの普及に伴い，Android端末をターゲットとしたボットが登場している．今後のスマートフォンのさらなる普及を考えると，Android端末をターゲットとしたボット対策は重要な課題であると考えられる．しかし，ボットの感染を完全に防ぐことは難しい．そこでボットの感染は避けられないことを想定し，2次被害を防止する方法について検討した．

本稿では，Android端末でキー／ボタン操作等のユーザが行う特徴的な操作に着目し，ユーザによる操作かボットによる操作かを判断して，ボットによる操作と判断された場合にユーザへの警告の後，送信パケットの破棄を行うことによる，Android端末におけるボットによる被害を防止する方法を提案する．

以降，2章で既存のボット対策と関連研究について述べる．3章ではAndroidで動作するボットの一例について述べる．4章では，提案方式について述べる．5章でまとめる．

第2章　既存のボット対策と関連研究

2.1　ボットネットとは

図 2.1 にボットネットの概要を示す．ボットネットとは，コンピュータウイルスの一種であるボットが構成する，指令サーバを中心とするネットワークのことをいう．指令サーバとしては，チャットを行う際に利用される IRC（Internet Relay Chat）サーバが利用されることが多い．

Herder は，複数の IRC サーバに接続しており，IRC サーバを介してボット感染端末に対して命令を送る．ボット感染端末は Herder の命令を受け取り，他端末に対してスパムメールを送信したり，Web サーバに対して DDoS 攻撃を行うなど，ユーザが知らない間に加害者になってしまう可能性がある．また，Herder は悪意のある第 3 者から依頼を受けてボットネットによる攻撃活動を行うことがある．そのため，特定の Herder による攻撃活動を抑えても，別の Herder に攻撃活動を依頼されてしまうのでボットネットによる被害状況は縮小しない．

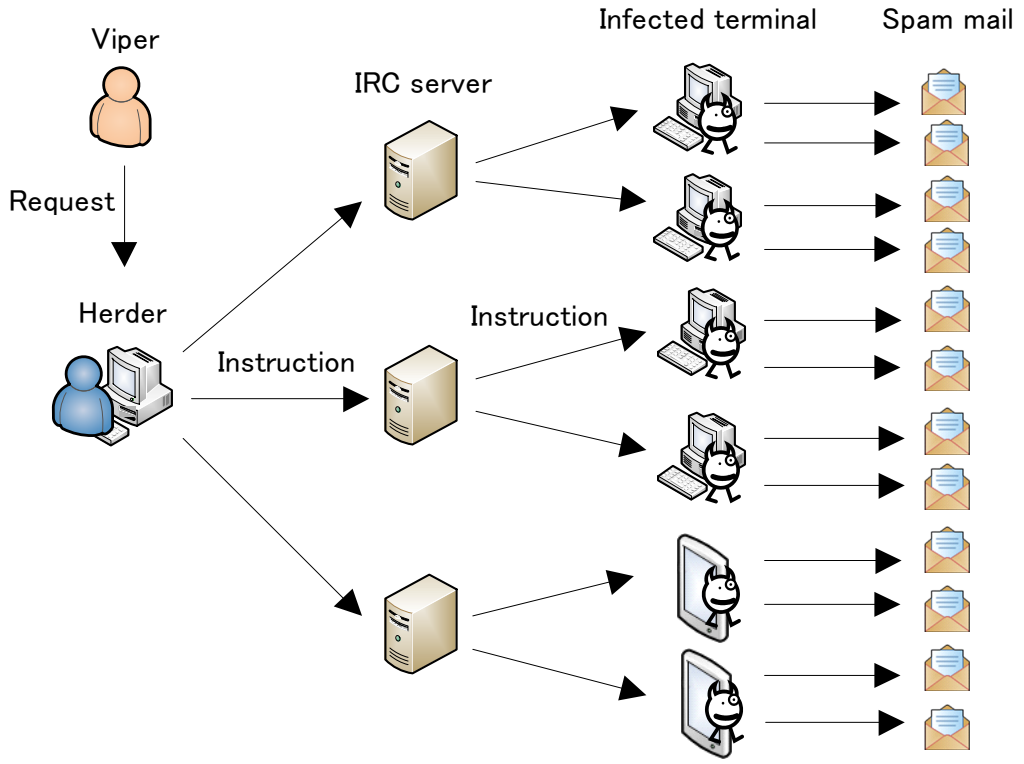

図 2.1　ボットネットの概要

2.2 Android 端末をターゲットとしたボット対策

既存のボット対策として，以下のような方法がある．

1. セキュリティ対策ソフトを導入する．
2. 信頼できないサイトからアプリケーションは取得しない．
3. Android 端末側で提供元不明のアプリケーションをインストールしない設定をする．
4. アプリケーションインストール時のアクセス許可に注目し，必要以上にアプリケーションにアクセス権限を与えていないか確認する．

1. における対策は，ボットを含むウイルスの検知・駆除に有効である．対策ソフトとしてはノートン，マカフィー，ウイルスバスター等のアンチウイルスソフトがある．しかし，アンチウイルスソフトのウイルス検出方法はウイルス定義ファイルを利用したパターンマッチングが主流である．このため，ウイルス定義ファイルに定義されてない新種や亜種といったウイルスは即座に検出することが出来ないという問題点がある．

2.，3. における対策は，正規アプリケーションにボットが内包された海賊版アプリケーションのインストールを防ぐことが出来る点で有効である．しかし，2.，3. における対策はユーザ自身が意識して行う対策であり，システムとしてボットの感染を完全に防ぐ訳ではない．

4. における対策は，ボットによる必要以上のアクセス許可要求に気付くことが出来ればボットを感染の段階で防ぐことが出来る点で有効である．Android 端末においてアプリケーションをインストールする際には必ずアプリケーションが利用したい権限の一覧を表示し，ユーザに対して同意を求める画面が表示される．ボットがアプリケーションに内包されている場合，ユーザに不要なアクセス権限の承認を求めている場合がある．しかし，一般のユーザが表示されるアクセス許可から，これからインストールするアプリケーションが不正なアプリケーションかどうかを判断することは極めて困難である．

このように既存のボット対策は，ほとんどがボットの感染を防ぐための対策であるが，新種や亜種が容易に出回るボットに対応して感染を完全に防ぐことは難しいのが実状である．

2.3 ヒューリスティック検知

未知のウイルス対策として，ヒューリスティック検知がある．ヒューリスティック検知とは，パターンマッチングによるウイルス検出とは異なり，通常なプログラムでは行わないシステム領域や DLL の書き換え等のウイルスに特徴的な挙動の有無を調べてウイルスを検出する手法である．しかし，この方法は未知のウイルスを確実に発見できるわけではなく，ウイルスではないものをウイルスとして誤認してしまう可能性もある．

第3章　Android端末で動作するボット

Android 端末で動作するボットは PC の場合と同様に，複数の感染した Android 端末同士でボットネットを構成し，Herder の命令に従って様々な被害を引き起こす．

図 3.1 に Android 端末で動作するボットの概要を示す．ダウンロードサイトからボットが内包されたアプリケーションをインストールすることによって Android 端末はボットに感染する．Android 端末に感染したボットはバックグラウンドで動作し，Herder により指定されたサーバに定期的にアクセスして Herder からの命令を待ち受ける．サーバは，Herder からの命令をボットに感染した全ての Android 端末に送信するために，チャットの機能を持つ IRC サーバが主に利用される．サーバ経由で Herder からの命令を受けたボットは，その命令に従って Android 端末の位置情報などの保存されている個人情報を Herder に対して送信する．他にも，他端末へのスパムメールの送信や，特定の Web サーバに対して DDoS 攻撃を行う等，ユーザの知らない間に加害者にされてしまう可能性がある．また，ボットの活動によりバッテリの消耗が激しくなる等の被害を受ける可能性がある．

Herder は複数のサーバに接続しているため，仮に 1 つのサーバを停止出来たとしても他のサーバを介して命令を送り続けることが出来る．このため，ボット対策をサーバに対して施すことは，難しいとされている．

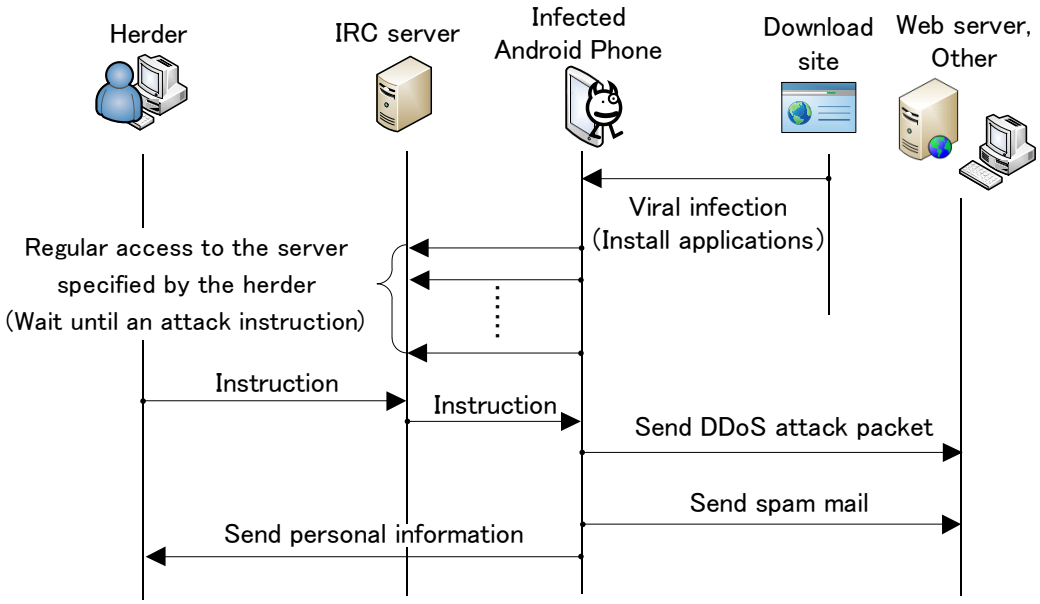

図 3.1　Android 端末で動作するボットの動作概要

第4章　提案方式

4.1　ボットとユーザ操作の違い

ボットによる操作とユーザが行う操作には以下のような違いが存在する．メール送信時の送信ボタンを押す操作，Web 閲覧時のブラウザボタンを押す操作，検索時の入力操作がボットにはできないユーザ特有の操作である．従って，Android 端末がネットワークにアクセスする際，直前にこれらの操作があったか確認することにより，正常な送信とボットによる送信を区別できる．

4.2　動作概要

図 4.1 に提案方式のフローチャートを示す．

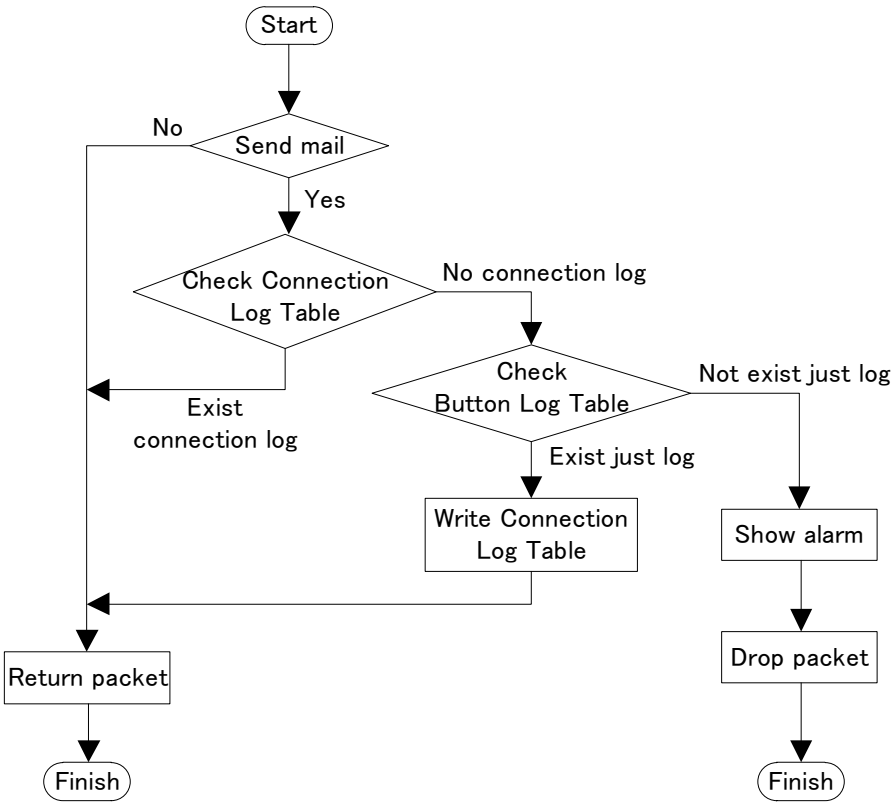

図 4.1　提案方式のフローチャート

提案方式では，監視プログラムの操作監視モジュールによって常にアプリケーションのキー／ボタン操作を監視して，キー／ボタン操作を時間情報としてボタン監視テーブルにログとして残す．キー／ボタン操作はボットが絶対に関与できないフッキング方法として，カーネル内でフックすることを想定している．

監視プログラムは全ての送信パケットをフックする．そして，パケット監視モジュールはコネクション履歴テーブルを参照する．コネクション履歴テーブルに書き込まれるパケット情報は，フックされたパケットの送信元 IP アドレス，宛先 IP アドレス，送信元ポート番号，宛先ポート番号から構成される．

フックされたパケットのパケット情報がコネクション履歴テーブルに存在すればパケットを戻し，通常動作としてネットワークへ送信する．フックされたパケットのパケット情報がコネクション履歴テーブルに存在しなければ，ボタン履歴テーブルを参照し，直前のキー／ボタン操作があるかを確認する．初期状態では，コネクション履歴テーブルには何も書かれていないので，無条件でボタン履歴テーブルを参照することになる．

直前にキー／ボタン操作が行われていた場合，コネクション履歴テーブルにフックされたパケット情報を書き込み，パケットを戻して通常動作としてネットワークへ送信する．以降に続く同じパケット情報をもつパケットは，パケット監視モジュールがコネクション履歴テーブルを参照すると既に自身のパケット情報と同じものがコネクション履歴テーブルに記録されているので，続きのパケットであると判断してボタン履歴テーブルの参照を行わずにネットワークへパケットを送信する．

直前にキー／ボタン操作が行われていない場合，ユーザに送信パケットを破棄する旨のアラームを提示して，ボットによる操作としてパケットを破棄する．

4.3　実装方法

図 4.2 に監視プログラムのモジュール構成について示す．監視プログラムの操作監視モジュールとパケット監視モジュールの 2 つをバックグラウンドで動作するようにしてカーネル空間で実装する．操作監視モジュールはキー／ボタン操作を時間情報としてボタン履歴テーブルに記録する．Netfilter は全てのパケットをフックする．パケット監視モジュールはコネクション履歴テーブルやボタン履歴テーブルを参照し，送信パケットが正規パケットであるか不正パケットであるかを判断し，ボットによる操作と判断された場合にパケットの破棄を行う．

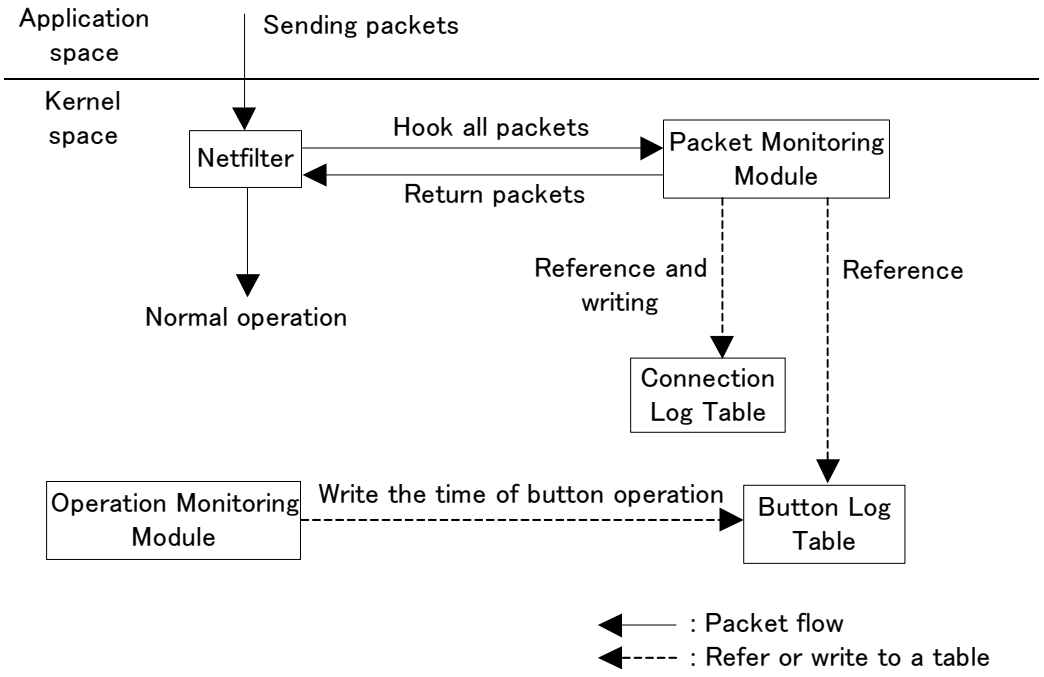

図 4.2　提案方式のモジュール構成

第5章　まとめ

Android 端末におけるボット対策として，Android 端末でユーザが行う特徴的な操作を考察した．メール送信やネットワークアクセス時の直前にボタン操作がない場合は対象パケットを破棄することにより，ボットによる 2 次被害を防止する方法を提案した．今後は，Linux カーネルを主に調査することで，ボタン操作の有無の検出方法を検討し，この方法の有効性を確認するための実装を行う．

謝辞

本研究にあたり，多大なる御指導と御教授を賜りました，渡邊晃教授には心から感謝いたします.

また，本研究を進めるにあたり，御意見ならびに御助言を受け賜りました，鈴木秀和助教に心から感謝いたします.

最後に，本研究を進めるにあたり，数々の有益な御助言や御討論を賜りました，渡邊研究室，鈴木研究室の諸氏に感謝します.

参考文献

[1] 戸田尚希，鈴木秀和，渡邊　晃：”Android 端末をターゲットとしたボットによる被害防止策の検討”，平成 23 年度電気関係学会東海支部連合大会論文集，F1-4，2011

[2] 平田祐二，鈴木秀和，渡邊　晃：”ボットによる不正メールの送信を防止するための検討”，平成 20 年度電気関係学会東海支部連合大会論文集，講演番号 O-077，2008

[3] 間宮領一，鈴木秀和，渡邊　晃：”ボットネットによるスパムメール送信防止方法の検討”，平成 19 年度電気関係学会東海支部連合大会論文集，講演番号 O-373，2007

[4] 三根健司，鈴木秀和，渡邊　晃：”Windows API の監視による未知ウイルス検出手法の検討”，平成 19 年度電気関係学会東海支部連合大会論文集，講演番号 O-372，2007

研究業績

学術論文

なし

研究会・大会等

1. 戸田尚希，鈴木秀和，渡邊晃，”Android 端末をターゲットとしたボットによる被害防止策の検討”，平成 23 年度電気関係学会東海支部連合大会論文集，F1-4，2011.
2. 戸田尚希，鈴木秀和，渡邊晃，” Android 端末をターゲットとしたボットによる被害防止策の提案”，情報処理学会第 74 回全国大会講演論文集，6Z-5，2012.

付 録A　ハニーポット

ハニーポットは，ハッカーやクラッカーの侵入方法やコンピュータウイルスの振る舞いなどを研究するためにインターネット上に設置された脆弱性のあるサーバやネットワーク機器の事を言う．ハニーポットは，脆弱性のあるサーバやネットワークを監視し，攻撃者の攻撃の手口や侵入方法といった行動の研究や，新種や亜種のウイルスをいち早く捕獲して分析する事が出来る．

ハニーポットに対して不正なアクセスを試みようとする際には，解放されているポート番号を確認するポートスキャンが行われる．ポートスキャンの中では，SYN スキャンと呼ばれる方法がある．SYN スキャンは，ハニーポットに対して SYN パケットを標的ポートに送信する．そして，ハニーポットから SYN/ACK を受信した場合のポートは開放状態にあることを示し，RST/ACK を受信した場合のポートは閉鎖状態にあることを示す．このような方法でハニーポットにおける開放ポートを探り，そのポートを利用した不正な活動が行われる．