様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 １５ 日現在

機関番号：３５４０９
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１９７

研究課題名（和文）Wiki と良性ボットを使った悪性ボットネット対策システム

研究課題名（英文）An Anti-Malicious Botnet　System Using Wiki software and a Beneficial Botnet

研究代表者
山之上　卓（YAMANOUE, Takashi）

福山大学・工学部・教授

研究者番号：００１９１３７０

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：P2P通信機能やドメイン生成アルゴリズム(DGA)機能を持つような悪性ボットネットに対応するための、良性ボットネットに関する研究を行い、試験的なシステムを開発した。このようなボットネットに対応するため、我々の過去の良性ボットを使った良性ボットネットの開発を行っている。P2P通信機能を持った悪性ボットネットは１台の侵入検知システムでは検知することが困難である。我々の良性ボットネットは良性ボットの協調動作により、P2P通信を検知する能力を持つ。この良性ボットネットはDGAを使った通信を検知する能力も持つ。今後出現するであろう新しい悪性ボットの技術に対応する潜在能力も持っている。

研究成果の学術的意義や社会的意義
標的型攻撃などによって組織内に侵入したボットによる重大な情報漏えい事件があいついで発生している。一度発生した情報漏えい事件は社会に大きな影響を与える場合があり，これを解決するには膨大な時間と労力と出費が必要となるだけでなく，完全な解決は不可能な場合もある。ボットを検知することは，組織の存続にかかわる重要な活動である。また，最近のボットはウィルス対策ソフトでは検出できない場合が多い。従って，そのボットが行う通信を監視すること以外の方法でこのようなボットを検知するのは難しい。本研究はこのような悪性ボットネットによる被害を小さくしようとするものである。

研究成果の概要（英文）：A beneficial botnet, which tries to cope with technology of malicious botnets such as peer to peer networking and Domain Generation Algorithm (DGA), has been investigated and its prototype system has been developed. In order to cope with such botnets' technology, we are developing a beneficial botnet as an anti-bot measure, using our previous beneficial bot. The beneficial botnet is a group of beneficial bots. The peer to peer (P2P) communication of malicious botnet is hard to detect by a single Intrusion Detection System (IDS). Our beneficial botnet has the ability to detect P2P communication, using collaboration of our beneficial bots. The beneficial bot could detect communication of the pseudo botnet which mimics malicious botnet communication. Our beneficial botnet may also detect communication using DGA. Furthermore, our beneficial botnet has ability to cope with new technology of new botnets, because our beneficial botnet has the ability to evolve, as same as malicious botnets.

研究分野：情報学

キーワード：ネットワークセキュリティ　ボット　P2P　DGA　分散システム　ボットネット　Wiki

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

１．研究開始当初の背景

標的型攻撃などによって組織内に侵入したボットによる重大な情報漏えい事件があいついで発生している。一度発生した情報漏えい事件は社会に大きな影響を与える場合があり，これを解決するには膨大な時間と労力と出費が必要となるだけでなく，完全な解決は不可能な場合もある。ボットを検知することは，組織の存続にかかわる重要な活動である。

標的型攻撃ではメールなどにより，組織内の利用者のパソコンにボットが侵入する。標的型攻撃で使われるメールは人間の心理をうまく利用しており，これを開かないようにすることは困難である。また，最近のボットはウィルス対策ソフトでは検出できない場合が多い。従って，そのボットが行う通信を監視すること以外の方法でこのようなボットを検知するのは難しい。

しかしながら従来の基幹ネットワークの監視では大量のトラフィックの陰にかくれて，ボットの通信の検出が困難な場合がある。基幹ネットワークの監視でボットの通信が検出された場合でも，利用者側 LAN と基幹ネットワークの間に NAT を行う機器が設置されていると，ボットに侵入されたパソコンの特定が困難になる。

これに対し，組織内ネットワークで監視の邪魔になっていた NAT にボットの活動を検知する機能を付けることにより，大量のトラフィックに埋もれることなく，LAN 内および LAN とその外の通信をきめ細かく監視することが可能になる。LAN 内のボットに感染したパソコンを特定することも容易になる。

ボットの侵入は，組織内および組織間の，自明ではない通信の相関を取ることにより検知できる場合がある。組織内および組織間でセキュリティ担当者が連携し，監視データを共有することにより，ボットおよびボットネット対策をより強力に行うことが可能になる。

我々は，Wiki を使って，NAT 等で保護された LAN 内通信を LAN の外から監視し，緊急時には，基幹ネットワークの設定変更等を行うことなく，疑わしい通信を遮断したり，制御したりすることを可能にするシステム（良性ボット）や，Wiki に書かれたプログラムによって，複数の Web ページのデータを集計するシステムの研究と開発を行っている。これらのシステムを改良・拡張して組み合わせることにより，上で述べたようなボットの監視の仕組みで使う機器を容易に開発可能である。

２．研究の目的

Wiki と，Wiki で遠隔操作可能な多数のネットワーク機器(良性ボット)を連携させて，有害なボットネットやそれによって遠隔操作されているボットを検出するシステム（良性ボットネットシステム）に関する研究を行う。必要に応じて,有害なボットネットの機能の一部を，遠隔操作により麻痺させることも可能にする。良性ボットは NAT やルータの機能も持ち，利用者が使う LAN と，WAN や組織の基幹ネットワークの間に，この良性ボットを設置する。これにより従来の集中的な監視方法では入手困難だった情報入手を容易にする。Wiki を使うことにより管理者グループの連携も強化する。図 1 に当初計画した良性ボットネットシステムの概要を示す。

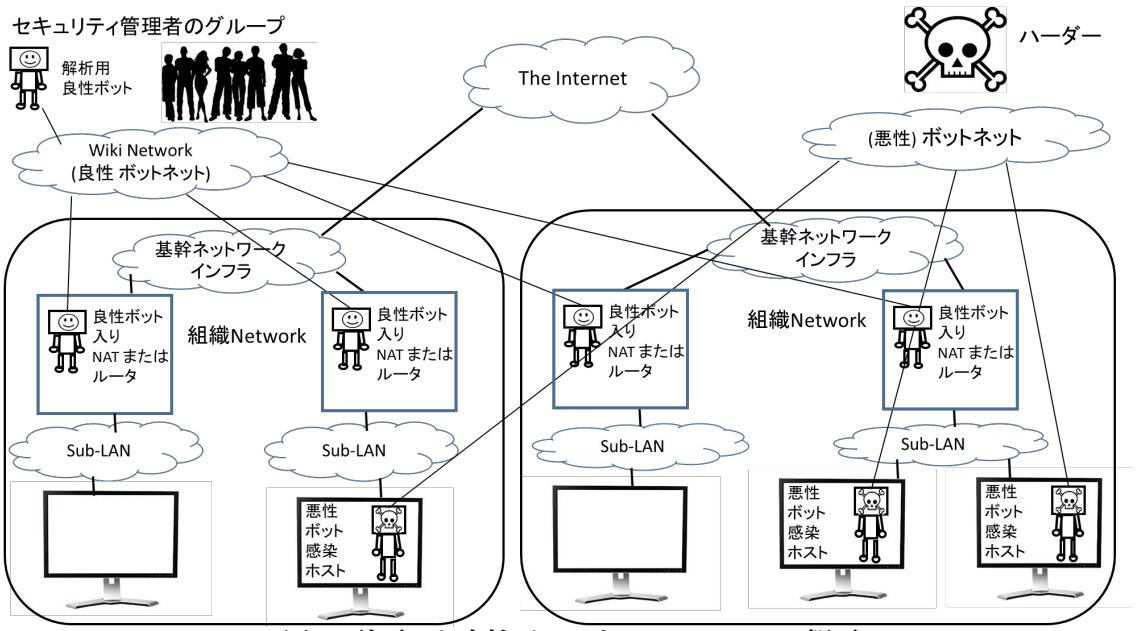

図 1. 計画した良性ボットネットシステムの概要

３．研究の方法

我々の Wiki を使った各種システムを拡張・改良することにより「良性ボットネット」で利用する機器を開発する。これと共に，本研究に関連する他所の関連研究を調査し，我々の研究に役立つ知見を入手する。これらの機器と知見を元に，良性ボットネットの試作を行い，評価

を行って，国内外の学会等で発表を行う．この発表の質疑応答などで得られた知見を元に，システムの改良を行う．この手順を何度も繰り返して，より良いシステムを開発する。

４．研究成果

2016 年度：

我々が研究開発している良性ボットシステムの元になるプログラムで、統計分析パッケージ R が利用できるようになった⑪．良性 Bot の制御は従来、Wiki ページで行っていたが、Twitter でコマンドを送信することにより、良性 Bot の制御を行うことができるようになった．

2016 年 6 月にアメリカ合衆国アトランタで開催された IEEE COMPSAC2017 に参加して、本研究に関連する情報の収集を行った．2016 年 11 月にはアメリカ合衆国デンバーで開催された ACM SIGUCCS 2017 に参加し、本研究に関連した論文発表を行うと同時に、関連研究の情報収集を行った⑫．

2017 年度:

昨年度から引き続き良性 Botnet の構成要素である良性 Bot の開発を行い，その経過と，改良した Bot の応用例に関し，⑩⑨⑧の発表を行った．

この他，2017 年 7 月にイタリアのトリノで開催された IEEE COMPSAC に参加し，関連研究の資料収集や情報セキュリティの研究者との情報交換を行った．

また，良性ボットネットシステムの試作を行い，その評価を行う為に，偽 Botnet を作成して，良性ボットネットの評価を行った．

2018 年度:

研究期間にほぼ計画通り,良性ボットネットの開発を行った．悪性ボットと同様の振る舞いをする，安全な偽ボットを作成することにより，良性ボットネットの評価を行うことができた①③。

この研究成果をまとめて，最終年度には④の発表を行うことができた．また，この研究に利用する良性ボットの研究開発に関し，最終年度に②⑤の発表も行った。

図 2 に偽ボットのネットワークの活動を検知する良性ボットネットシステムの実験を行った時の構成を示す。

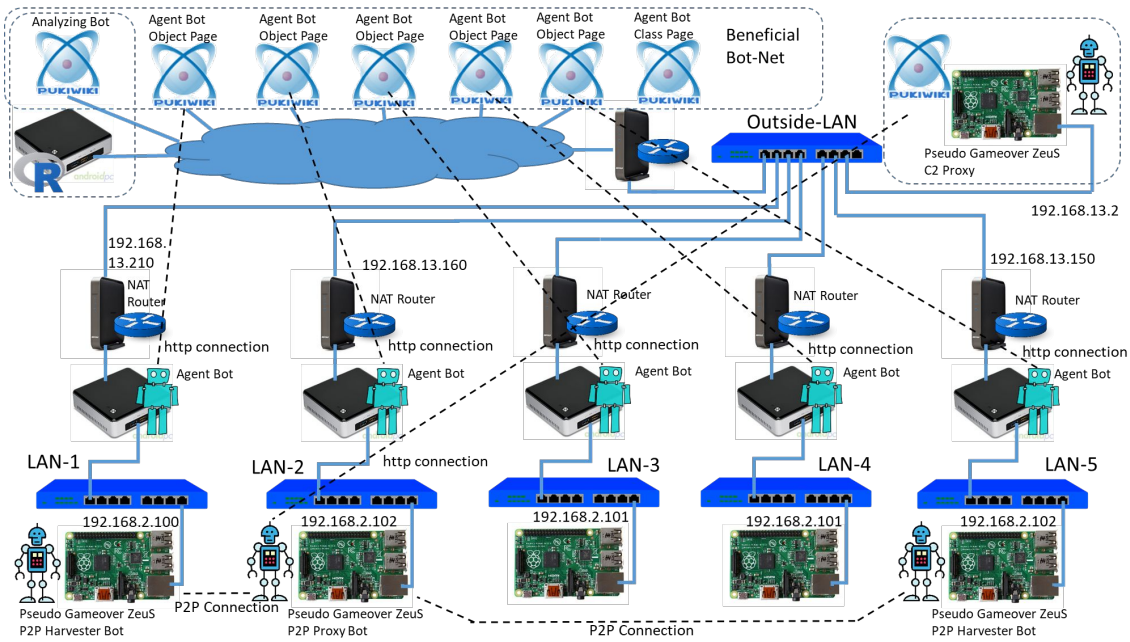

図 2．偽ボットのネットワークの活動を検知する良性ボットネットシステムの実験

５．主な発表論文等

〔雑誌論文〕（計　　0 件）

〔学会発表〕（計　　13 件）

① 山之上　卓, 長副誉司, "悪性 Botnet 包囲網の Bot による WannaCry のようなマルウェアの活動検知の試み", 情報処理学会　研究報告インターネットと運用技術（IOT）, 2019-IOT-44(5),1-8 (2019-02-28) , 2188-8787. 査読なし

② Takashi Yamanoue, "Bot Computing and its Application to Solve Minimal Path Problems", 情報処理学会プログラミング研究会第 122 回研究発表会 (2019-1). 査読なし

③ 山之上 卓, "インターネット上の Wiki ページにより NAT 背後のセンサ端末の設定変更や制御が可能な IoT システムによるサーバとサーバ室の監視", 情報処理学会シンポジウム, インターネットと運用技術シンポジウム 2016 論文集, 情報処理学会シンポジウムシリーズ No. 2018, pp. 62-69, (2018-12), 査読あり

④ Takashi Yamanoue, "A Botnet Detecting Infrastructure Using a Beneficial Botnet," SIGUCCS '18 Proceedings of the 2018 ACM on SIGUCCS Annual Conference, pp. 35-42, Orland, Florida, USA, Oct.,2018. 査読あり

⑤ Takashi Yamanoue, Daichi Yokoyama, Ryoya Umeda, Shota Morita, Takashi Ozeki and Noboru Nakamichi, "An IoT System with Remote Re-configurable Wireless Sensor Network Nodes and Its Application to Measure Activity of a Class", 7th International Conference on E-Service and Knowledge Management (ESKM 2018), Yonago, Japan., (2018). 査読あり

⑥ 山之上　卓, "悪性 Botnet 包囲網における P2P 通信検知の試み", 情報処理学会 研究報告インターネットと運用技術（IOT）,2018-IOT-42(3),1-8 (2018-06-21) , 2188-8787. 査読なし.

⑦ 村上　順也, 山之上　卓, "悪性 Botnet 包囲網における DGA 検知の試み", 情報処理学会研究報告インターネットと運用技術（IOT）,2018-IOT-42(4),1-8 (2018-06-21) , 2188-8787. 査読なし

⑧ Takashi Yamanoue, "Monitoring Servers, With a Little Help from my Bots", SIGUCCS '17 Proceedings of the 2017 ACM on SIGUCCS Annual Conference, pp. 173-180, Seattle, Washington, USA, Oct.,2017. 査読あり

⑨ 横山大知・梅田凌弥・山之上　卓・森田翔太・尾関孝史・中道　上 "IoT システムを利用したグループ学習の活発度の計測実験" 信学技報, vol. 117, no. 209, ET2017-37, pp. 35-40, 2017 年 9 月. 査読なし

⑩ 山之上卓, 羅牧野 "センサネットワークのセンサ端末群をインターネット上の Wiki ページで制御する IoT システムの試作", 研究報告インターネットと運用技術（IOT）,2017-IOT-36(12),1-8 (2017-02-24) , 2188-8787. 査読なし

⑪ 平田篤, 藤田健吾, 伊勢本和広, 山之上卓, "Wiki ページに書かれた R 言語のプログラムによるデータ解析を可能にした Bot の試作",インターネットと運用技術シンポジウム 2016 論文集, 情報処理学会シンポジウムシリーズ No. 2016, pp. 91-97, (2016-12). 査読あり

⑫ Takashi Yamanoue, Noboru Nakamichi, and Kunihiko Kaneko, "Enhancing Campus Cyber Security through a Class with Combination of Computer Ethics Videos and Logical Thinking" SIGUCCS '16 Proceedings of the 2016 ACM on SIGUCCS Annual Conference, pp. 117-123, Nov.,2016. 査読あり.

⑬ 山之上卓, "Bot と Wiki を使った試験的な並列プログラミング" 情報処理学会, 研究報告インターネットと運用技術（IOT）, vol. 2016-IOT-34, No.2, pp.1-12,2016-06-25. 査読なし.

〔図書〕（計　　0 件）

〔産業財産権〕
○出願状況（計　　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年：
国内外の別：

○取得状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕

ホームページ等
http://www.yama-lab.org/~yamanoue/wiki/index.php?BotCapturingNet

６．研究組織

(1)研究分担者

研究分担者氏名：

ローマ字氏名：

所属研究機関名：

部局名：

職名：

研究者番号（8 桁）：

(2)研究協力者

研究協力者氏名：

ローマ字氏名：