HOKKAIDO UNIVERSITY

Title	A study on detection and blocking of DNS-based botnet communication [an abstract of dissertation and a summary of dissertation review]
Author(s)	一瀬, 光
Degree Grantor	北海道大学
Degree Name	博士(情報科学)
Dissertation Number	甲第14122号
Issue Date	2020-03-25
Doc URL	https://hdl.handle.net/2115/78224
Rights(URL)	https://creativecommons.org/licenses/by/4.0/
Type	doctoral thesis
File Information	Hikaru_Ichise_review.pdf, 審査の要旨

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

学位論文審査の要旨

博士の専攻分野の名称　博士 (情報科学)　　氏名　一瀬 光

審査担当者　主　査　准教授　飯田 勝吉
副　査　教　授　髙井 昌彰
副　査　教　授　南 弘征
副　査　教　授　棟朝 雅晴

学位論文題名

A study on detection and blocking of DNS-based botnet communication
（DNS ボットネット通信の検知及び遮断に関する研究）

近年、インターネットでは多数の重大セキュリティインシデントが起きている。多くのセキュリティインシデントにはボットと呼ばれる不正プログラムが用いられている。ボットとは、C&C サーバと呼ばれる不正サーバと緊密な連絡をとり、その指示に従い DoS 攻撃やスパムメール送信などの他者を攻撃するマルウェアのことである。通常 C&C サーバは非常に多数のボット感染 PC を配下に置くため、その影響力は大きく対策は急務と言える。対策には C&C サーバ側とボット側の対策があり, どちらも重要である。特に大学キャンパスネットワークなどの組織ネットワークの管理者にとっては、組織内 PC のボット感染を早期に発見する必要がある。

そこで本研究では、C&C サーバとボット感染 PC 間の通信 (以下、ボットネット通信と記載) を分析し、それによりボット感染 PC の早期発見及び隔離を目指している。具体的には、多くの最新のボットが利用する DNS という通信方式を想定し、不正 DNS 通信の検出を行っている。多くの不正プログラムが DNS 不正通信を用いて、DoS 攻撃やスパムメール送信などで多少を攻撃しているため、DNS を用いたボットネット通信検出の基幹技術の確立は組織ネットワークの防衛の重要な課題である。

DNS を用いたボットネット通信の検出には、DNS トンネリングを行う Feederbot や Morto の分析やハニーポットによる検知手法などの既存研究が存在する。しかし、それらの既存研究では様々な DNS 不正通信の方式に対応することができず、またリアルタイムに隔離するシステムは確立されていない。

つまり不正 DNS 通信を検出するためには、(1) 正当な DNS 通信と不正なそれを区別する基準の確立と、(2) 基準に基づきリアルタイムに検出や遮断をするシステムを実現することの 2 つの課題が存在する。本研究では最初に課題 (1) に取り組み、次にそこで得られた基準を用いて課題 (2) に取り組んでいる。

まず、課題 (1) に関しては、大学のキャンパスネットワークのトラヒックログを用いて二つの方式、リゾルバ経由方式と外部クエリー方式のそれぞれを分析している。リゾルバ経由方式の分析に関しては、ボットネット通信で広く用いられている TXT レコードの DNS フルリゾルバのクエリーとレスポンスの履歴を分析している。TXT レコードには最大 4000 バイトの自由な情報を記載することができるため、不正通信に利用されやすい。しかし、TXT レコードを用いた正当な通信にも用いられているため、すべての TXT レコードを遮断すると実用上の問題が発生する。そこでリゾ

ルバ上の TXT レコードのクエリーとレスポンスの履歴を調査し、RFC などに記載されている正答な利用方法に該当するものを識別し、利用方法がわからない履歴を抽出している。さらに、抽出した履歴を調査したところ、その IP アドレスの約 30% が悪性であり、また、その数は極めて少ないと論じている。そのため、TXT レコードのクエリーとレスポンスの履歴を調査し、利用方法がわからない履歴があったときに、その履歴を詳細に確認することで、少ない手間で不正通信が発見できると論じている。外部クエリー方式に関しては、正当な通信には先行して NS レコードの問い合わせが行われるため、NS レコードの問い合わせがないのに外部クエリーが発生した場合、不正通信の可能性が高いと予想している。その予想に基づき、NS レコードの問い合わせを伴わない外部クエリーを分析した結果、直接外部クエリーの宛先 IP アドレスの約 8% が、間接外部クエリーのそれの約 22% が悪性であると記している。つまり、NS レコードの問い合わせを伴わない直接および間接外部クエリーには不正なものが多く混入しているため、そのような外部クエリーを発見するシステムを実現することで、ボットネット通信の検出や遮断の可能性があると論じている。

次に、課題 (2) に取り組むため、NS レコードの問い合わせを伴わない外部クエリーをリアルタイムに発見し遮断するシステムの設計、実装、評価を行っている。具体的には、NS レコードの問い合わせを伴わない外部クエリーかどうかを発見するために、NS レコードと glue A レコードをすべて取得し、NS 履歴データベースを作成している。その上で、NS 履歴データベースに基づき、外部クエリーの通信遮断制御を行う。通信遮断制御を行う方式として、OpenFlow 技術を用い、コントローラと呼ばれる装置上に NS 履歴データベースと連動して外部クエリーの通信遮断制御を行なうシステムを実装している。実際の通信履歴を用いた評価では、False Positive 率が平均で 10% 未満となることを明らかにしている。

これを要するに、著者は、最新のボットで広く用いられている DNS によるボットネット通信を検出、遮断するための DNS トラヒックの分析やシステム研究を包括的に取り扱っており、組織ネットワーク防衛の基幹技術開発の貢献に大なるものがある。よって、著者は北海道大学博士 (情報科学) の学位を授与される資格があるものと認める。