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_abstract.pdf, 論文内容の要旨

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

学 位 論 文 内 容 の 要 旨

博士の専攻分野の名称　博士（情報科学）　氏名　一瀬 光

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）

昨今、次世代インターネットではより高い QoS のサービスを提供する一方で、それに伴いより高度で、影響度の大きな、多くのセキュリティインシデントが発生している。そのようなセキュリティ攻撃の中には、ボットと呼ばれる不正プログラムを利用するものがあり、深刻な問題になっている。ボットとは DDoS 攻撃やスパムメールの送信等、多様な攻撃を行う前段階において、メールの添付ファイル、Web 閲覧、USB 等により普及される悪性のプログラムである。このボットに感染した PC をボット感染 PC と呼ぶ。ボット感染 PC は C&C サーバと呼ばれるサーバから多様な攻撃の命令を受信し、その命令に従って、一斉に他者を攻撃する。ボットネット通信とは C&C サーバとその配下にある多数の PC 等から構成される論理的なネットワークである。ネットワーク管理者にとってボット感染 PC を組織内に置かないことが重要であり、急務である。本論文では最新のボットネット通信である DNS クエリーを利用したボットネット通信に着目し、自動的に検知・遮断するシステムについて論じている。

第 1 章では、研究の背景、つまり、ボットネット通信の脅威について概観し、それらの研究の課題をあげ、本研究の目的を論じている。ボットネット通信の既存研究では (1)DNS TXT レコードに関する正当な利用方法と不明確な利用方法との分析が行われておらず、(2) 組織内の DNS フルリゾルバを経由しないボットネット通信 (以後、直接クエリーのボットネット通信) の分析が行われておらず、(3) 直接クエリーのボットネット通信の自動的検知・遮断が実現されていない。そのためこれらを解決することが本論文の目的であると述べるとともに、解決方法の概要を説明している。

第 2 章では、ボットネットの詳細、DNS プロトコル、DNS を利用したボットネットの挙動について述べ、既存研究を紹介し、解決すべき課題を概説している。

第 3 章では課題 (1)、(2) の解決方法について論じている。実際の DNS トラフィックを分析することによって DNS を利用したボットネット通信の対策システムについて検討している。具体的には、東京工業大学から約 3 ヶ月の DNS トラフィックを取得し、3 種類のボットネット通信に着目し、DNS トラフィックの分析を行っている。その 3 種類のボットネット通信とは組織内の DNS フルリゾルバを必ず経由する手法、一度組織内の DNS フルリゾルバを経由した後、二度と DNS フルリゾルバを経由しない (以下、間接外部クエリー) 手法、そして一度も組織の DNS フルリゾルバを経由しない (以下、直接外部クエリー) 手法であると説明されている。DNS トラフィックを分析した結果、組織内の DNS フルリゾルバを必ず経由する分析では不明確な利用方法に分類された宛先 IP アドレスのうち約 30% が悪性であることを示している。また、間接外部クエリーの分析では毎日約 22% の宛先 IP アドレスが、直接外部クエリーでは毎日約 8% が悪性であることを示している。これらの分析をさらに進めた結果、直接外部クエリーは事前に NS レコードを取得しないことを明らかにしている。そこで、直接外部クエリーのボットネット通信についての対策システムとして事前に NS レコードとそれに対応する glue A レコードを全てデータベース化することにより、

検知システムの実現が可能であると論じている。
第 4 章では課題 (3) の解決方法について論じている。第 3 章において提案したボットネット通信の対策システムに基づいた実装を行なっている。仮想化環境上において東京工業大学から取得した DNS トラフィックを使用し、NS レコードと glue A レコードを全て取得し、NS 履歴データベースを作成している。その NS 履歴データベースを直接外部クエリーを判定する機能として利用し、遮断方法として、SDN 技術を使用することによってスイッチを制御している。本技術を実装することによって NS 履歴データベースに登録されていない宛先 IP アドレスを持つ DNS クエリーについては悪性であると判定し、スイッチで DNS クエリーを遮断することで課題の解決を図っている。
次に、システム評価実験を行なっている。実装したシステムの評価を行うために、仮想環境上で 2 つの実験を行なっている。実験 1 では機能評価として、クライアントからスイッチに送信される DNS クエリーの宛先 IP アドレスが NS 履歴データベースに登録されているかを判定し、適切にシステムが挙動しているかを確認している。その結果、NS 履歴データベースに登録されている場合には正当な DNS クエリーとして通過させて、登録されていない場合は遮断している。実験 2 では性能評価として、通常時の DNS の名前解決の速度と提案手法のシステムの名前解決の速度を測っている。その結果、提案手法は通常時の手法と比べて、5% 未満の遅延増加があったが、実用上許容可能であると述べている。次に、実装したシステムの誤検知率を分析している。東京工業大学で取得した DNS トラフィックを使用し、DNS クエリーの宛先 IP アドレスを抽出している。それとは別に、その DNS トラフィックを使用し、NS 履歴データベースも作成している。その DNS クエリーの宛先 IP アドレスと NS 履歴データベースに登録されている IP アドレスとを照合し、比較している。その結果、DNS クエリーの宛先 IP アドレスが NS 履歴データベースに登録されている IP アドレスに比べて約 10% 多いことを示している。この値は誤検知率であり、学習時間を設けることでこの値を下げることができることを示し、本システムの有用性・有効性を確認している。
第 5 章では本研究の成果と今後の課題をまとめている。