

Title	Website Protection Schemes Based on Behavior Analysis of Malware Attackers
Author(s)	Yagi, Takeshi
Citation	大阪大学, 2013, 博士論文
Version Type	VoR
URL	https://hdl.handle.net/11094/51137
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

【26】

氏名	八木 毅（やぎ たけし）
博士の専攻分野の名称	博士（情報科学）
学位記番号	第 25863 号
学位授与年月日	平成25年3月25日
学位授与の要件	学位規則第4条第1項該当 情報科学研究科情報ネットワーク学専攻
学位論文名	Website Protection Schemes Based on Behavior Analysis of Malware Attackers （マルウェア感染攻撃に対する攻撃者の挙動解析に基づいたWebサイト防衛方式）
論文審査委員	（主査） 教授 村田 正幸 （副査） 教授 村上 孝三　教授 中野 博隆　教授 東野 輝夫

論文内容の要旨

本論文では，近年脅威となっているWebサイトへのマルウェア感染攻撃に対して，多種多様な多数の攻撃を高精度に検知する方式を提案する．マルウェア感染攻撃に対しては，既存の攻撃の特徴情報を抽出する方式に加え，その特徴情報に基づいてサーバ上で攻撃を検知するアンチウィルスソフトや，その特徴情報に基づいてネットワーク上で攻撃を検知する攻撃防御装置などが検討されている．ただし，従来の方式では，多種多様化が急激に進むマルウェア感染攻撃を高確率で検知することができなかった．

Webサイトへのマルウェア感染は，Webアプリケーションのぜい弱性に起因して発生する．Webアプリケーション数が急増している近年において攻撃を防御するためには，多様な攻撃を検知できる必要がある．また，多くの攻撃を検知するためには，Webサイトへの特定のアクセスを攻撃と判断するための根拠情報となる既知の攻撃の特徴情報を，最大限収集して保有する必要がある．さらに，高精度に攻撃を検知するためには，検知漏れや誤検知を抑制可能な攻撃検知が必要となる．

従来の方式では，まず，監視対象としている攻撃の特徴情報として，マルウェアファイルの特徴や攻撃者からのHTTPリクエストの特徴を適用していた．しかし，マルウェア亜種の増加やHTTPリクエストの難読化に伴い，監視対象が爆発的に増加しており，効率的な監視が困難となっている．

第二に，従来の方式では，既存の攻撃の特徴情報を抽出する際に，不正な制御が実行された際にのみ攻撃を検知して特徴情報を抽出していた．このため，不正な制御を試行したが成功しなかった攻撃者からのアクセスを特定できず，多くの攻撃の特徴情報を発見できない．

最後に，従来では，攻撃者の挙動を考慮せず，攻撃を監視して適宜制御していた．このため，攻撃の監視が攻撃者に感知され，攻撃に使用される特徴情報が攻撃者により変更され，その結果，攻撃の検知率が低下していた．

そこで，提案方式では，多様な攻撃の検知を実現するために，マルウェア感染時にWebサイトがアクセスする宛先をブラックリスト化する方式を提案する．さらに，収集可能な攻撃の特徴情報を最大化するために，攻撃の宛先URLを制御して攻撃を監視下で成功させる方式を提案する．最後に，攻撃検知率の改善を実現するために，攻撃者の挙動解析に基づくブラックリスト更新方式を提案する．

論文審査の結果の要旨

八木毅君の博士学位論文は、マルウェア感染攻撃防御方式について、理論的な基本的検討のみならず実用化にも直結した内容であり、非常に優れた研究成果をまとめたものである。

本論文では、1章で攻撃の概要が説明され、2章で従来の対策手法が説明されている。3章では、近年のプロバイダ環境に存在する多数のWebサイトをマルウェア感染攻撃から保護するための要求条件と、従来手法の課題が説明されており、4章から6章までで提案手法が説明されている。

4章では、多様な攻撃を防御するために、マルウェア感染時にWebサイトがアクセスする宛先をブラックリスト化する手法を提案している。本手法は、攻撃者からのアクセスの特徴や受信ファイルの特徴をブラックリスト化する手法と比較して、効率的に多くの攻撃を防御することができ、提案手法の有効性は実データを用いて評価されている。

5章では、インターネット上に存在する既存の攻撃からブラックリストに関する情報を最大限収集するために、攻撃を収集するためのおとりシステムにおいて攻撃の宛先URLを制御することで攻撃を監視下で成功させる手法を提案している。従来のおとりシステムと比較して数倍のブラックリスト情報を収集できることを、実データを用いて検証している。

6章では、ブラックリストを防御に用いた際の検知漏れと誤検知を抑制するために、攻撃者の挙動解析に基づくブラックリスト更新手法を提案している。ブラックリストに掲載されたURLが現時点で悪性か否かを検査する最適な周期を数値解析によって算出する手法を、シミュレーションを用いて評価している。

以上の内容は、理論的な面だけでなく、実用的な面でも有効性が認められる。特に実用的な面では、4章に記載の手法に基づいて得られた成果が、NTTコミュニケーションズのSecurity Operation Centerが提供するManaged Security Serviceに実現されており、グローバルなセキュリティビジネスにおいて実際に活用されている。また、5章に記載の手法に基づいて得られた成果は、前記サービスだけでなく、総務省国家プロジェクト「国際連携によるサイバー攻撃予知・即応技術の研究開発」でも活用されているものである。さらに、6章に記載の手法は、サイバー攻撃対策において数値解析を用いている貴重な事例となっている。これらの手法は全て、既に新たなセキュリティサービスの提供に用いられていく計画になっている。なお、これらの成果は、2件の論文と3件の国際会議発表に反映されているとともに、投稿中の2件の論文誌論文にもまとめられており、理論的な面でも有効性は認められている。

このように、本論文は、理論面と実用面で非常に高い成果をまとめているといえる。よって、博士（情報科学）の学位論文として価値のあるものと認める。