早稲田大学大学院 基幹理工学研究科

博士論文審査報告書

論　文　題　目

Internet Communications Data Profiling for Detection of Evolving Cyber Attacks

進化するサイバー攻撃の検知のための インターネット通信データプロファイリング

申　請　者

Daiki	CHIBA
千葉	大紀

情報理工・情報通信専攻　情報システム工学研究

2017 年 7 月

インターネット上の重要情報を狙うサイバー攻撃が増加している。多くのサイバー攻撃は端末が悪意のあるソフトウェア（マルウェア）に感染することから始まる。端末がマルウェアに感染するとサイバー攻撃に悪用されてしまう。サイバー攻撃を抑制するためにはマルウェア対策が必須である。

マルウェアへの対策にはホスト上での対策とネットワーク上での対策がある。ホスト上での対策の代表例はアンチウィルスソフトである。アンチウィルスソフトは既知のマルウェアを解析してシグネチャを生成する。シグネチャと検査対象のファイルを照合してマルウェアを検知する。このファイルベースの対策の弱点は新種のマルウェアに対応するために次々にシグネチャを生成する必要がある。

ネットワーク上の対策の代表例はブラックリストを用いる通信ベースの対策である。通信ベースの対策では、悪性通信の宛先（ドメイン名、URL）や悪性通信のパターンを監視して、感染を誘発する悪性通信を検知する。マルウェアに感染したとき、あるいは感染後には悪性通信が発生する。ファイルベースの対策が困難な場合でも通信ベースでの対策が有効になる。

本論文は、マルウェア対策のためのインターネット上の通信データの新しい解析法を提案する。本論文は従来のマルウェア対策を妨げている４つの基本的な課題を明らかにして､第２章から第５章で各課題の解決手法を検討する｡本論文は、サイバー攻撃対策技術を飛躍的に前進させることを目的にしている。提案手法の有効性を検証するために実際のサイバー攻撃に用いられたデータを利用して実用性を評価する。

第１章では、本研究の背景と目標を述べている。

通信ベースのマルウェア対策を実行する際には、悪性通信の宛先や悪性通信のパターンの特徴を次の手順で把握する。（１）攻撃を観測するための囮（おとり）となるハニーポットで、端末が感染する時の悪性通信やマルウェア検体を記録する。（２）マルウェア検体を動的解析技術により実際に動作させて､感染した端末が発生する悪性通信を捕捉する。（３)得られた各種のデータに対して適切なデータ解析手法を適用して悪性通信の宛先および悪性通信パターンの特徴を生成する。

適切なデータ解析手法を用いて、ハニーポット技術や動的解析技術だけでは直接に検知できない新種の悪性通信の推定と特定を行うことが重要である。攻撃者は解析技術に追随して対策を回避する仕組みを考案する。従来のデータ解析手法を利用するだけでは対策が不十分となる新種の悪性通信が出現する。

第２章では､Webサイトの IPアドレスの特性を用いて悪性サイトを検知する方法を提案している。攻撃者は複数の悪性サイトを連携させて攻撃を実行する。例えば、ドライブバイダウンロード攻撃でユーザをマルウェア感染させる際に、複数の悪性サイトを中継させた後に最終的にマルウェアをダウンロードさせる。このように一連の攻撃が複数かつ多様な悪性サイトで構成される場合には、悪性サ

イトのドメイン名やURLの通信宛先を個別に扱う従来のデータ解析手法では検知できない場合がある。本章では悪性サイトのIPアドレスの特性をプロファイリングして悪性サイトを検知する新たなデータ解析手法を提案している。ここでは、悪性サイトのIPアドレスの領域がURLやドメイン名に比べて安定的であるという性質を利用する。この性質を活用して機械学習による軽量かつスケーラブルな悪性サイトの検知機構を開発した。実データを用いて提案手法の評価を行い、従来手法では検知できない新規の悪性サイトを正しく特定可能であることを示した。

第3章では、悪性ドメイン名の時系列変動パターンを利用する悪性ドメイン名の検知法を提案している。攻撃者は悪性ドメイン名を次々と新たに生成して変化し続けて解析技術を回避する。悪性ドメイン名が変化し続ける場合には、ある時点でドメイン名の評価を行う従来のデータ解析手法では十分に追随できない。第3章では将来に悪用されるドメイン名を検知するためのデータ解析手法を提案している。主要なアイデアは、悪性ドメイン名の時系列変動パターンをプロファイリングすることである。ドメイン名の時系列変動パターンとは、ドメイン名が人気ドメイン名リストや悪性ドメイン名リストに掲載される、あるいは削除される変化のことである。本手法では，能動的にドメイン名に関するDNS通信ログを収集して、ドメイン名の時系列変動パターンを特定する。その結果を解析して、あるドメイン名が将来サイバー攻撃に悪用されうるものかどうかを判定する。大規模な実データを用いた評価を行い、提案手法によるデータ解析が従来手法では特定できない悪性なドメイン名を高い精度で発見できることを明らかにした。

第4章では、悪性ドメイン名の運用特性に基づく最適な対策の決定法を提案している。攻撃者は、特性の異なるドメイン名を用いて悪性通信を構成する。例えば、攻撃者が正規サービスを悪用した悪性ドメイン名を利用すると、対策側は正規サービスを妨害しないように対策用の情報を精緻に生成する必要がある。一方、攻撃者が攻撃専用に悪性ドメイン名を用意する場合には、対策側はドメイン名を単位として対策用の情報を生成して即座に適用するべきである。このように悪性ドメイン名の特性に応じて実施するべき対策が異なる。従来のデータ解析法では単一の対策を想定しているために最適な対策を提示することができない。第4章では悪性ドメイン名の特性に応じて最も効果的な対策を選択するためのデータ解析手法を提案している。主要なアイデアは、対策を実施する際に考慮するべき悪性ドメイン名の特性をカテゴリとしてプロファイリングし、各カテゴリに対応する対策を選択することにある。具体的には、提案手法は悪性ドメイン名に対して実施するべき対策方法、対策場所、対策粒度を客観的に決定して対策用情報を出力する。実際の攻撃で利用された大規模なドメイン名データセットを利用して評価を行い、提案手法で生成した対策用情報を利用すれば、正規サービスを妨害せずに本来の攻撃のみを効果的に防ぐことができることを示した。

第５章では、再利用される攻撃基盤の特性を利用する悪性通信の検知法を提案している。攻撃者は、悪性通信を良性通信と区別しにくいように設計して、容易に検知されないように工夫を凝らす。具体的には、攻撃者はマルウェア感染の際に発生する悪性通信を、ユーザが日常的に発生させる良性通信と類似させることで対策を回避する。このような良性通信に類似する悪性通信に対して、従来のデータ解析手法を用いると良性通信を誤って悪性と判定する誤検知が多発して、悪性通信の正確な特定が妨害される。第５章では誤検知を削減しながら悪性通信を正確に特定するためのプロファイリングを提案している。提案手法は、攻撃者が利用するマルウェア検体やコマンドアンドコントロール通信などの攻撃基盤は毎回新規に設計されるものではなく、一部が再利用されながら設計されているという性質を利用する。具体的には、マルウェア感染端末が送出する悪性 HTTP リクエストの内容から同一の攻撃基盤を再利用することに起因する不変箇所を特定し、その不変箇所を利用してマルウェア感染端末を検知する方法を提案している。検知するための対策用情報（テンプレート）を自動生成するシステムを開発して、提案手法を大規模な実ネットワークで検証を行い、従来手法と比較して誤検知を大幅に削減しながら感染端末の検知率を向上できることを示した。

第６章では結論を述べている。

以上を要するに、本論文は従来のマルウェア対策において悪性通信の特定を妨げている４つの基本的な課題を明らかにして、各課題を解決する新たなデータ解析手法を提案している。実データを用いた評価により提案手法の有効性を確認している。提案手法は進化するサイバー攻撃の特性を捉えて設計された実用的な手法であり、インターネットにおけるサイバー攻撃対策を大幅に向上することができる。本論文の成果は、よりセキュアなインターネット環境を実現するために有用である。よって、本論文は博士（工学）早稲田大学の学位論文として価値あるものと認める。

2017 年 7 月

審査委員

主査　早稲田大学教授　　工学博士（東京大学）　　後藤　滋樹

早稲田大学教授　　博士（工学）（北海道大学）　内田　真人

早稲田大学准教授　　博士（情報科学）（早稲田大学）森　達哉