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

Taint-based Analysis Techniques against Evasive Malware
解析回避機能を持つマルウェアの解析手法：
テイント伝播によるアプローチ

申　請　者

川古谷	裕平
Yuhei	KAWAKOYA

2019 年 2 月

今日のサイバーセキュリティ脅威はいわゆる「マルウェア」(malware)によってもたらされるケースが多い。マルウェアとは悪意のあるソフトウェアの総称であり、ウィルス、ワーム、スパイウェア等、ユーザに大小様々な被害をもたらす。マルウェアには金銭的な被害をもたらすものが存在する。例えば被害者が用いる端末のデータを攻撃者の鍵を用いて暗号化し、暗号化されたデータを復号化する鍵の送信を対価として金銭を要求する「ランサムウェア」、あるいは被害者の端末上で秘密裏に暗号通貨のマイニングを行う「クリプトマイナー」、ユーザの端末に感染し、オンラインバンキングサービスで不正送金を行う「バンキングマルウェア」などが知られている。

こうしたマルウェアがもたらす被害を食い止める有効な手段は、マルウェアを解析し、その特徴や挙動を深く理解することである。特徴がわかれば、類似したマルウェアを迅速に検知することができる。挙動がわかれば、マルウェアの動作目的、被害範囲や手口、および外部との通信手段などの情報を得ることができる。マルウェア解析手法は、「動的解析」と「静的解析」に大別され、それぞれに短所と長所があるため、両者をハイブリッドで用いることが多い。どちらの解析においても Application Programming Interface（API）コールの情報が中心的な役割を果たす。API から得られる情報はマルウェアの挙動を特徴づけるため、解析上有用なデータである。実際、商用のマルウェア解析製品においても API を用いるケースは多い。

一方、マルウェアの作成者の視点からすると、マルウェア解析を妨害するようにマルウェアを作成する動機がある。解析が困難であればあるほど、そのマルウェアの寿命が伸びると期待されるからである。したがって、マルウェア作成者は API 情報を解析者から巧妙に隠蔽することを試みる。具体的には動的解析においては API モニタの回避、静的解析においては実行ファイルがインポートする API 情報の隠蔽により、マルウェア解析を回避する手法を実現している。

本論文は、このようなマルウェアの解析回避機構に焦点を当てる。解析回避に対する対抗策として「テイント解析」を利用することにより、隠蔽されていた API 情報を追跡することを可能とする技術を開発する。テイント解析はデータフローの解析技術の一つであり、テイントタグと呼ばれる属性情報をプログラムの実行環境上の値に付与し、その値が環境上を移動する毎にタグを伝播し、データフローを追跡する手法である。

第 1 章では、本研究の背景と目標、ならびに以降の章構成に沿って成果の概要を示している。

第 2 章では、マルウェアが利用可能な解析回避手法の全体像と、これらに対する既存研究を説明するとともに、本研究との関連を説明している。

第 3 章では、第 2 章で示した既存の動的解析と静的解析手法の問題点を立証することを目的としている。すなわち、攻撃的セキュリティの手法を用い

てマルウェア解析を妨害する手法を開発した。具体的には、Windows OS が管理するデータ領域で、ロードした DLL の情報が残らないように、DLL を実行可能にするプログラムローダを開発した。開発した解析妨害手法を用いると、セキュリティ解析の現場で普及している動的・静的解析ツールでは解析が困難であることを立証した。なお、このような攻撃手法は後に示す方法によって対策が可能である。

第 4 章では、動的解析における API モニタにテイント解析を適用する手法を提案している。テイント解析は通常、データフロー解析に利用されるが、本論文ではテイント解析をコード実行の追跡に利用することに特徴がある。各 API のコードに異なるテイントタグを付与し、現在実行されている命令、および次に実行される命令のそれぞれに設定されているタグ間の遷移パターンに着目し、それらが監視対象 API か否かを見分ける手法を提案している。インターネットから収集した大量のマルウェア検体を、提案手法を用いて解析し、その有効性を評価した結果を報告している。

第 5 章では、静的解析実行時に必要となる API の名前解決を、テイントタグを用いて実現する手法を提案している。はじめに各々の API に固有な値を割り当てたテイントタグを作成し、動的解析時にそれらのタグを伝播させる。動的解析終了後にメモリダンプを取得する際に、前記の伝播したテイントタグの情報も合わせて取得する。そのような情報を使って IAT 再構築を行うことにより、API の名前解決を実現できる。提案手法を実データを用いて評価し、解析妨害手法に影響を受けることなく API の名前解決が可能であることを示している。

第 6 章は、本論文のまとめである。全体の内容を概観した上で、1 章で指摘した問題―マルウェア解析回避機構の対策―を実現したことを示す。すなわち、本論文の主要なアイディアである、テイント解析をコード実行の追跡に利用するアイデアとその応用により、従来のアプローチでは解析が困難であったマルウェアの動作を解析可能にした。また、本論文で提案した手法とその制約事項について論じ、この分野における将来の研究課題と、それらにアプローチするための道筋を明確にしている。

以上を要するに、本論文は今日における多様で巧妙なマルウェア解析回避手法を整理・分類し、それらの解析回避手法に対して有効な対抗手段として「テイント解析」技術を用いたアプローチを提案した。具体的にはマルウェアの動的解析、および静的解析のそれぞれにおいて、テイントタグを用いることにより、監視対象となる API を正しく追跡する手法の提案、ならびにそれらの有効性評価を実施した。マルウェアがもたらす脅威を撲滅するためのセキュリティ対策としてきわめて実用的な成果である。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。

2019 年 2 月

審査員

主査　早稲田大学教授　　博士（情報科学）（早稲田大学）　　森　達哉

早稲田大学教授　　博士（情報科学）（早稲田大学）　鷲崎　弘宜

早稲田大学教授　　Ph.D.（Computer Science）
（カリフォルニア大学バークレー校）　寺内　多智弘

筑波大学准教授　　博士（理学）（東京大学）　　大山　恵弘
