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

Analyzing Hidden Features of Web-based Attacks
Web 感染型攻撃における
潜在的特徴の解析法

申　請　者

Yuta　TAKATA

髙田　雄太

情報理工・情報通信専攻　情報システム工学研究

2018 年 2 月

インターネットの利用が拡大すると同時にサイバー攻撃の脅威が増加している。攻撃者は他人のクライアントをマルウェアに感染させて不正に操作し、情報の窃取や改ざん、破壊活動を行う。多くのインターネットサービスが Web を活用して提供されているため、Web が主要なマルウェア侵入経路となっている。Web を悪用するマルウェア感染攻撃はドライブバイダウンロード攻撃と呼ばれる。

ドライブバイダウンロード攻撃の対策には、ホスト上の対策とネットワーク上の対策がある。ホスト上の対策は、アンチウイルスソフトを用いたマルウェアの検知と除去が代表的である。ネットワーク上の対策は、URL ブラックリストを用いた悪性通信の検知と遮断がある。このような対策技術は、マルウェアや悪性 URL に関して事前に収集した悪性情報に基づいて攻撃を検知する。その悪性情報を収集する方法には、ネットワークトラヒックを受動的に監視する方法および悪性 Web サイトへの能動的なアクセスによる方法がある。いずれの方法も情報収集には有効であるが、受動的な収集方法は観測できる地点が限定されること、さらに通信の内容に立ち入るプライバシーの問題がある。このため能動的な収集方法が広く使われている。

悪性 Web サイトへの能動的なアクセスには、意図的に攻撃を受ける囮（おとり）のクライアントシステム（ハニークライアント）を用いる。ハニークライアントは、攻撃を受ける際に発生するシステム上の種々の変化、および対象とする Web サイトの特徴に基づく機械学習により悪性 Web サイトを検知する。一方で攻撃者は対策技術を回避するように行動する。巧妙な攻撃は、既存のハニークライアントが容易に情報を取得できないように設計される。ハニークライアントが悪性情報を収集できない場合には従来の対策技術が有効に機能しない。

本論文は、巧妙化するドライブバイダウンロード攻撃の有効な対策となるようにハニークライアントの解析性能を向上して、悪性 Web サイトを検知するための情報をより多く収集する方法を提案している。具体的には悪性 Web サイトにおける４つの巧妙化技術に対応している。(1) コンテンツの難読化、(2) 環境依存攻撃、(3) 多段転送、(4) Web サイト改ざん、である。本論文の提案手法を用いると、悪性 Web サイトから得られる情報を従来技術に比べて飛躍的に拡大できる。

第１章は本研究の背景、課題、目標ならびに研究成果の概要を述べている。

第２章では、従来の対策技術ならびに攻撃の巧妙化技術を説明している。対策技術としては、実環境を使用して解析する高対話型ハニークライアントおよびエミュレータを使用する低対話型ハニークライアントの両方を説明している。本論文は低対話型ハニークライアントを高度に拡張して用いている。次にハニークライアントで収集した情報を用いて攻撃を検知する機械学習の技術を説明している。従来から、攻撃コードの構造のような静的な特徴量、あるいは攻撃コードの挙動や多段転送の構造等の動的な特徴量を用いた機械学習により様々な攻撃検知手法が提案されている。

さらに第2章では、攻撃の巧妙化技術としてコンテンツ難読化、環境依存攻撃、多段転送、Web サイト改ざんについて説明している。攻撃者は、悪性 Web サイトに関連する情報を隠蔽するために悪性コンテンツに難読化を施す。さらに多段転送により悪性 URL を頻繁に変更する。また、多段転送の過程で特定の OS やブラウザのみを標的とする環境依存攻撃を仕掛ける。さらに Web サイトの改ざんにより一般の Web サイトを攻撃に加担させる。このような攻撃の巧妙化に対応するためのハニークライアントおよび機械学習技術における課題を説明している。

第3章では、本論文が提案する環境依存攻撃の対策として、特定の環境を攻撃するために構築された URL を抽出する方法を提案している。ドライブバイダウンロード攻撃における多段転送は、攻撃の起点となる入口 URL、クライアントのアクセスを中継する踏台 URL、攻撃コードを含む攻撃 URL、そしてマルウェアを保持するマルウェア配布 URL のように異なる役割を担う複数の URL で構成されている。環境依存攻撃は、この多段転送の過程で JavaScript を用いてブラウザフィンガープリンティングを実行して、クライアントの OS やブラウザ等の環境を識別する。その識別結果に応じて転送先の URL を変更する。ハニークライアントを使用する従来技術は、そのクライアントの環境が攻撃対象に一致しない場合には攻撃 URL やマルウェア配布 URL 等の悪性 URL への転送が行われない。このように悪性 URL へ転送されないハニークライアントでは、攻撃コードやマルウェア等の悪性コンテンツを取得することができず、情報を収集できない。

この課題を解決するために、第3章では JavaScript をプログラムスライシング技術で解析することにより、環境毎に用意された転送コードを特定している。その解析結果から URL を抽出する手法を提案している。この手法は JavaScript の実行網羅性を向上するものである。例えば条件分岐文で本来は実行されないコードからも URL を抽出できる。悪意のある転送コードの多くは難読化が施されている。これに対応するために、URL アクセス時に直接取得できる JavaScript の静的なコードに加えて、難読化解除を経て動的に生成されるコードも解析できるようにブラウザエミュレータを用いて本手法を実装している。本論文では、このように拡充されたブラウザエミュレータがハニークライアントの役割を果たしている。事前に収集した悪性 Web サイトの HTTP 通信データを用いて提案手法の評価を行った結果、従来の方法よりも多くの URL を抽出できることが分かった。

第4章では、多段転送や JavaScript 実行を追跡することにより、改ざんされた Web サイトにおける悪性コンテンツを特定する手法、ならびに複数のクライアントの環境を模擬して攻撃対象を特定する手法を提案している。多段転送に使われる入口 URL は、悪性 URL へ転送するように改ざんされた一般の Web サイトが悪用されることが多く、攻撃を疑わないユーザからのアクセスを奪取する。Web サイト改ざんを無効にするためには、その Web サイト管理者によるインシデント対応が必要不可欠である。この際に従来技術では、改ざんされた Web サイトの URL

の情報がブラックリストとして管理者に通知される。多段転送や環境依存攻撃のような巧妙な攻撃に対しては、URL だけでは情報が不足している。一般の Web サイト上で改ざんされた悪性コンテンツは、元来は無害な Web サイトに含まれるコンテンツである。第 4 章ではハニークライアントを用いて悪性コンテンツを詳細に解析している。ここで得られる改ざんされたコンテンツの特徴および Web サイト改ざんにより発生する転送、攻撃対象のクライアントの環境等の情報を用いて、迅速かつ精緻に攻撃への対応が出来るようになる。

さらに第 4 章では、攻撃者により改ざんされたコンテンツを特定するとともに、当該コンテンツにより攻撃の脅威に晒されるクライアントの環境を特定する手法を提案している。具体的には、ブラウザエミュレータを用いて多段転送や JavaScript の実行を詳細に追跡している。どのコンテンツがどのような URL へ転送するかを特定する機能を実現している。本手法は、複数のクライアントの環境を模擬して Web サイトを解析して、どのようなクライアントの環境が脅威に晒されるのかを特定できる。提案手法を評価するために、前章と同様の実験環境を用いて悪性 Web サイトの HTTP 通信データを収集して評価した結果、提案手法により改ざんされたコンテンツならびに攻撃対象のクライアントの環境情報を効果的に特定できることが実証できている。

第 5 章では結論を述べている。

以上を要するに、本論文は悪性 Web サイトにおける 4 つの攻撃巧妙化技術の特徴を明らかにして、ハニークライアントを用いて巧妙な攻撃を解析する手法を提案して実装している。本論文で提案している技術は、巧妙化するドライブバイダウンロード攻撃が普遍的に持つ特徴を捉える実用的な手法である。本論文では、実ネットワーク上のデータを用いて提案手法を評価して有効性を確認している。本論文の提案技術によるハニークライアントが収集する情報は、アンチウイルスや機械学習等の既存技術による悪性 Web サイトの検知精度向上にも貢献する。本論文の成果は、よりセキュアな Web サイトを構築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。

2018 年 2 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