2W-04

クライアント環境で動作するセンサを利用したドライブ・バイ・ダウンロード攻撃の検出手法の提案

吉田 豊† 中村 嘉隆† 高橋 修†
†公立はこだて未来大学 システム情報科学部

1 はじめに

ドライブバイダウンロード攻撃は，Webのユーザに対して，不正な手段によってマルウェアのダウンロード・実行を行わせるものである．この攻撃は，Webのユーザが攻撃者によって改ざんされたWebサイトにアクセスすることによって引き起こされる．改ざんされたサイトには，攻撃者の用意した攻撃用サイトへのリダイレクト処理が含まれており，ユーザは気が付かない間に攻撃サイトへとアクセスすることとなる．攻撃サイトでは，ユーザの使用するOS，ブラウザ，ブラウザのプラグイン等の脆弱性に対する攻撃が行わる．最終的に，ユーザはマルウェアの配布サイトへと誘導されて，不正なプログラムをダウンロードさせられる．

近年のドライブバイダウンロード攻撃では，様々な技術を用いて，攻撃の隠蔽が行われており，攻撃の発見・調査が困難な状況となっている．そこで，本研究では，クライアント環境で動作するセンサを利用することによって，攻撃を行うサイトの情報を素早く収集するための手法を提案する．

2 関連研究

既知の悪性Webサイトの情報を利用し，新たな悪性Webサイトを探索するEVILSEEDというシステムがある[1]．一般に，悪性Webサイトを探索するシステムは，Web空間にランダムアクセスを行うクローラ，クローラで得られたページをフィルタリングするフィルタ，より詳細な分析を行い最終的な良性・悪性の判定を行うオラクルから構成されている．EVILSEEDは，オラクルによって悪性と判断されたページの情報を利用することによって，未知の悪性サイトかもしれないページを取得しフィルタにかける．フィルタリングされ，オラクルで悪性と判定されたものは，再びEVILSEEDシステムで利用される．このように，悪性サイトと判断された情報を再帰的に利用することによって，単純なランダムアクセスによるクローリングよりも効率の良い探索が可能となる．

クライアントのブラウジング情報を収集し，大規模な分析センタによってそれらの情報を分析することによって，悪性サイトの脅威からクライアントを守るドライブバイダウンロード攻撃対策フレームワークがある[2][3][4]．このシステムでは，クライアントの通信を常に収集し，リアルタイムに悪性な通信が行われていないかを確認している．そのため，分析センタによって，悪性と判断されたページの読込を停止するということも可能となっており，クライアントの安全なブラウジングを確保できる．しかし，このフレームワークはクライアントの通信を全て監視する必要があるため，分析センタの負荷が非常に大きくなってしまうという難点がある．また，クライントの通信内容が全て分析センタに送信されるためプライバシーの問題も生じる．

3 提案手法

本稿では，クライアント環境で動作し，訪れたサイトが悪性・良性かの簡易判定を行うセンサを利用することによって，悪性サイトの情報を素早く収集する手法を提案する．クライアント環境において，ユーザが訪れるサイトが良性・悪性かを判断するものをセンサと呼ぶ．

提案手法の概要を図1に示す．センサは，訪れたページが悪性だと判断すると，そのページの情報をデータベースへと送信する．センサは，悪性Webサイトの情報を収集するという観点から，見落としを極力少なくする必要がある．そのため，正規サイトを誤って悪性サイトと判定してしまうこともあるが，既存の手法のように通信の遮断を行うことはないので，ユーザはセンサを意識せずにブラウジング可能である．センサによって収集された情報は，ドライブバイダウンロード攻撃を動的に解析することが可能なクライアントハニーポットや，JavaScriptのコード解析などのより詳細な調査に利用することができる．

提案手法では，悪性サイトの検知後，データベースへのデータの送信のみを行うため，提案手法だけではマルウェアの感染を防ぐことはできない．しかし，既存の攻撃に対する防御手法と併用することによって，悪性サイトのデータ収集と攻撃の防御を同時に行うことが可能となる．

An Approach to Detect Drive-by Download Attacks by Using Sensor Plug-in Working in Client Environment
Yutaka Yoshida†, Yoshitaka Nakamura† Osamu Takahashi†
† School of Systems Information Science, Future University Hakodate

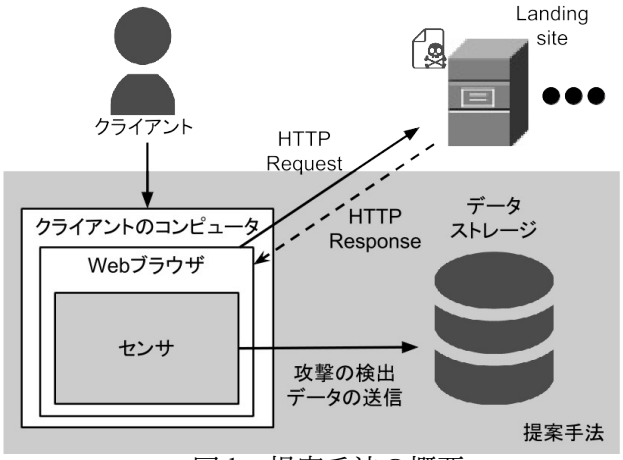

図 1．提案手法の概要

3.1 検出に用いる特徴

ドライブバイダウンロード攻撃を検出するために，最も基本的な特徴である通信遷移の情報を利用する．通信遷移には，Web ページのリンクの深さ，Web ページのリンクの広がりという 2 つの指標がある[5]．リンクの深さとは，あるページを読み込んだ際に，そのページから呼び出されるファイルの段数である．リンクの広がりとは，異なるドメインへの遷移数である．ドライブバイダウンロード攻撃では，最終的にマルウェアをダウンロードさせる危険なリクエストがある．そのような通信で利用される Content-Type を pdf，x-shockwave-flash，octet-stream，x-msdownload，x-download，x-msdos-program とする．

3.2 検出アルゴリズム

ユーザ操作による通信を起点として，Web ページのリンクの深さと広がりを測定する．それぞれの初期値は 0 とする．リンクの深さが 3 以上で危険なリクエストが発生した場合，もしくは，リンクの広がりが 1 以上で危険なリクエストが発生した場合には，ドライブバイダウンロード攻撃が起こったと判定する．

4 実験と考察

提案手法の有効性を示すために，HTTP による通信をキャプチャしたものを利用して，検知率・誤検知率を測定する．評価の指標として，正規サイト，悪性サイトそれぞれの偽陽性，偽陰性を用いる．

4.1 実験用通信データ

良性のデータとして，Alexa のトップ 1000000 からランダムにアクセスしたものを利用する[6]．悪性データとして，NTT セキュリティプラットフォーム研究所が提供する D3M2014 データセットを利用する[7]．

4.2 実験結果と考察

実験結果を図 1 に示す．提案手法における，悪性サイトの検知率は 100%であった．そして，正規サイトを悪性サイトと誤検知する割合は 1%であった．この結果から，提案手法を利用することによって，悪性サイトを完全に検知しながらも，正規サイトの誤検知を少なくすることが可能となった．誤検知が少なくなった要因として，マルウェアのダウンロードが行われるようなリクエストを攻撃の検出に用いたことが挙げられる．

表 2．正規・悪性サイトの検知率

	悪性サイト	正規サイト
有効 URL 数	56	100
検知数	56	1
誤検知率	0%	1%

5 おわりに

本稿では，ドライブバイダウンロード攻撃を行うサイトの情報を収集することを目的として，クライアント環境で悪性サイトかどうかの簡易判定を行い，悪性サイトの情報を収集する手法を提案した．また，実験によってクライアント環境下でのドライブバイダウンロード攻撃判定の有効性を示した．現在，マルウェアのダウンロードが行われた場合のみ判定可能であるため，今後は，ダウンロードが行われない場合であっても，悪性らしいと判定できるような手法を提案したいと考えている．

参考文献

[1] L. Invernizzi，S. Benvenuti，M. Cova，P. Milani Comparetti， C. Kruegel， G. Vigna“EvilSeed： A Guided Approach to Finding Malicious Web Pages，”Proceedings of the 2012 IEEE Symposium on Security and Privacy（SP’12），pp. 428-442，2012.

[2] 笠間 貴弘，井上 大介，衛藤 将史，中里 純二，中尾 康二，“ドライブ・バイ・ダウンロード攻撃対策フレームワークの提案，” コンピュータセキュリティシンポジウム 2011 論文集，vol. 2011，no．3，pp．780-785，2011.

[3] 松中 隆志，山田 明，窪田 歩，“Drive-by Download 攻撃対策フレームワーク実現に向けたリンク構造解析による Web サイトの分析，” 情処研報，vol．2015，no．48，pp．1-8，2015.

[4] T．Matsunaka，A．Kubota，and T．Kasama，“An Approach to Detect Drive-By Download by Observing the Web Page Transition Behaviors，” 2014 Ninth Asia Jt．Conf．Inf．Secur．，pp．19-25，2014.

[5] 安藤 槙悟，寺田 真敏，菊池 浩明，and 趙晋輝，“通信の遷移に着目した不正リダイレクトの検出による悪性 Web サイト検知システムの提案，” 情処研報，vol．2011，no．32，pp．1-6，2011.

[6] “Alexa - Actionable Analytics for the web”，http://www.alexa.com/

[7] 秋山満昭，神薗雅紀，松木隆宏，畑田充弘，“マルウェア対策のための研究用データセット ~MWS Datasets2014~，” 情処研報，vol. 2014，no. 19，pp. 1-7，2014.