別紙様式第８

論文の内容の要旨

申請者　防衛大学校　トラン　コン　マン

論文題目

A Research on Detection and Classification of Automated HTTP Communication
(HTTP 自動通信の検出と分類に関する研究)

近年、様々なアプリケーションの実装基盤として HTTP が用いられるようになってきた。利用者が必要とするサービスのほとんどがウェブ上で提供されるため、HTTP はインターネット上で最も多用されるプロトコルと認知されている。このため多くのネットワーク環境において、HTTP 通信は制限されることなく自由に利用できる。HTTP は、個別の要求と応答のみが定義されており、会話的な相互通信を行わないため､アプリケーションが連続的かつ会話的な非同期通信を必要とする場合は、クライアントは能動的かつ自動的にサーバへ接続要求を送信し続ける必要がある。この論文では、このような通信を行うソフトウェアを自動化ソフトウェア(autoware)、生成された通信を自動化トラフィックと呼ぶ。

自動化トラフィックには、OS の更新などの良性のもの、ボットネットの C&C 通信などの悪性のもの、およびアドウェアなどのグレーのものがある。ユーザのコンピュータやネットワークに危害を与えるのはマルウェアだけでなく、アドウェアなどのグレーウェアの可能性もある。一部のアドウェアは、ユーザのウェブアクセスの習慣や設定を監視し、その情報をターゲット広告を目的とした第三者に送信する。この自動化の結果として、ウェブアクセスの通信はユーザのウェブ操作とは無関係に生起することになる。正当なユーザーは、未知のトラフィックや制御されていないトラフィックのためにインターネット上でランザクションを行うため､常にリスクに直面している｡近年、サイバー犯罪者は、不正なアドウェア、スパイウェア、ボットなどの悪意のある HTTP オートウェアを拡散させるための通信媒体としてウェブを活用するようになってきている。

このような問題への従来の対策のひとつとして、アンチウィルス（AV）製品は、コンテンツおよびシグネチャベースのマルウェア検出技術を用いてアプリケーションの良性または悪性を判定する。しかし、近年のさまざまな調査の結果、シグネチャベースの手法を使用して検出されないマルウェアが数多く存在し、主要な AV エンジンは最近のマルウェアのわずか 30～70％しか検出できていないことが明らかとなった。本研究では、コンテンツベースの検出手法における問題に対処するため、ネットワークトラフィックの分析と分類による手法を用いる。

これまでの HTTP 環境におけるマルウェア検出は、ボットネットを対象としたものが多い。このような検出法は、一般的なマルウェアを対象としているため、正当なソフトウェアに類似した様々なアドウェアなどのグレーウェアを識別することができない。したがって､HTTP 自動通信を分析し、それらのアクティビティを検出および分類する必要がある。そこで本研究では、自動通信の振る舞いの特徴量を観測、分析することにより、ホストベースおよびネットワークベースでの HTTP 自動通信を検出、分類する手法を提案する。

ホストベースの検出アプリケーションモデルは、メモリとリソースの制限を伴う単一の PC に適用できる利点がある。ホストベースのシステムを導入することにより、マルウェア感染の可能性のあるトラフィックを低減できるため、ネットワーク全体のリスク軽減に役立つ。このアプリケーションモデルは、ユーザがネットワークトラフィックを監視して、不審なトラフィックをフィルタリングすることができる。

ネットワークレベルの検出手法は、特定の URL ではなく、特定の目的のための URL グループに着目する。この分析結果は、ネットワークやシステムの管理者がユーザにはほとんど知られていない HTTP 自動トラフィックを検知することができる。その結果から、HTTP オートウェアによって引き起こされる内部脅威を早期に検知することができる。

様々な種類のオートウェアの通信が混合した実ネットワークトラフィックを用いて実験を行った結果、高い識別精度が得られ、手法の有効性を確認した。また、提案手法を実環境に実装する場合のアプリケーションモデルについても考察、提案している。

今後の課題は誤警報を減らすことと達成されている結果を広げることである。ネットワークベースの手法において、クラスタ化されなかった疑わしい URL を通常の URL と識別するために、付加特徴量について検討する必要がある。また、いくつかのソフトウェアはセキュアチャネルを使用する傾向があるため、悪意のある HTTPS 通信の検出について検討する必要がある。