2W-07

通信パケットのログを利用した マルウェア感染インシデント再現システムの開発

奥田　裕樹†　　福田　洋治†　　井口　信和†

近畿大学理工学部情報学科†

1. はじめに

情報システム運用において，マルウェア感染に基づく情報漏洩や不正遠隔操作，利用不能行為などのセキュリティインシデント(以下，インシデント)への迅速な対応が課題となっている．インシデントを検知した際，関連する事象を正確に把握する必要がある．しかし，当該機器で事象が記録されていない，または消去・攪乱されるとインシデントの全容把握が困難になる[1)]．

本研究では，端末にマルウェアを送る主要な手段の1つである Drive by Download 攻撃を含むインシデントを想定し，マルウェアの感染と活動の調査を支援するシステム(以下，本システム)を開発する．本システムは，インシデント発生時の通信パケットのログから Drive by Download 攻撃に関連する悪性 Web サイトへのリクエストとそのレスポンス，Web クライアントの動作を再現する．

悪性 Web サイトは作られてから姿を消すまでの期間が短く，端末に設置されたマルウェアが活動後に消失，または攻撃者が痕跡を消去・攪乱すると，事後の調査が困難になる．インシデント対応の初動や調査の場面で本システムを用いることで Drive by Download 攻撃によるマルウェア感染の過程が再現できる．これをインシデントが観測・記録できる環境で実施することでマルウェア感染の過程と活動の痕跡の収集と記録を支援する．

2. マルウェア感染インシデント再現システム

本研究では，平時からネットワーク機器や端末において取得・記録している通信パケットのログを利用して悪性 Web サイトを復元し，事後に Web クライアント端末で起こった事象を再現・把握するシステムの開発を行う．本システムは，Web を介したマルウェア感染インシデント発生後，通信パケットのログから Web サイトとの通信を再現し，マルウェア感染の可能性のある Web サイトを復元する．

システムの要件は，以下のとおりである．

要件 1　…　通信パケットから個々の HTTP セッションを抽出して，当時の悪性 Web サイトの動き(アクセス先 URL，リクエストに対して，レスポンスを返す動き)が再現できる．

要件 2　…　Web クライアントを操作して，当時の悪性 Web サイトの URL にアクセスすると，実際に Web ページやファイルをダウンロード，閲覧(リダイレクトにも対応)することができる．

要件 3　…　Web クライアントの種類，アドオン，動作させる OS 等の環境は，変更が容易で，繰り返し，初期状態に戻して，再現した悪性 Web サイトにアクセスを試すことができる．

上の要件1～3を満たす，本システムの構成，動作を図1に示す．

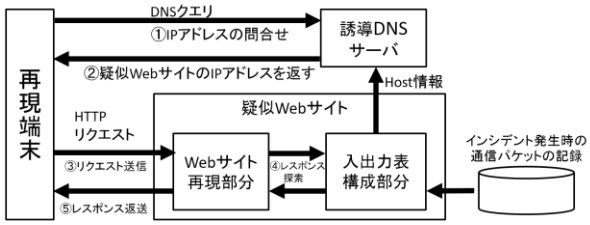

図1　システムの構成と動作

疑似 Web サイトは，入出力表構成部分と Web サイト再現部分からなる．入出力表構成部分は，PCAP 形式で与えられる通信パケットのログから，Web サイトに対する HTTP リクエストとそのレスポンスを表(以下，入出力表)にし，管理する．

入出力構成部分の表作成の流れを以下に示す．

1. 通信パケットのログから TCP のフローを抽出
2. 抽出した TCP フローから HTTP リクエストを取得
3. HTTP リクエストに対応するレスポンスを収集
4. リクエストとレスポンスの入出力表を作成，アクセス先ホストの表を作成

Web サイト再現部分は，Web クライアントからの HTTP リクエストに対し入出力表を基にレスポンスを返し，Web サイトの挙動を再現する．また，複数同時のアクセスに対応するため，Socket 通信を用いた並行サーバ方式を採用した．

Web サイト再現部分の動作の流れを以下に示す．

1. Web クライアントから HTTP の接続を受ける
2. HTTP リクエストを解析，リクエストキーを作る
3. 入出力表を参照し，リクエストキーを検索する
4. 見つかった場合，対応するレスポンスを返す
　見つからない場合，エラー404を返す

疑似 Web サイトは，通信パケットのログから HTTP セッションを抽出，HTTP リクエストとそのレスポンスの表を作成，管理する．その後，Web クライアントからのアクセスを受け付け，入出力表を基に HTTP リクエストに対するレスポンスを返す．

Development of malware infection incident reproduction system using log of communication packet
Yuki OKUDA, Youji FUKUTA, and Nobukazu IGUCHI,
School of Science and Engineering, Kindai University

これにより，要件1に対応する．

誘導DNSサーバは疑似Webサイトの IPアドレスと復元する Web サイトのホスト名の対応を A レコードとして持つ．再現端末からのアクセスに伴う名前解決時にこの誘導 DNS サーバを参照させることで疑似 Web サイトにアクセスを誘導する．これにより，要件2に対応する．

再現端末は，仮想化技術を用いて被害の可能性がある端末と同じソフトウェア環境を構築する使用を想定している．仮想化技術で端末を構築することによって，実際にマルウェアが感染した場合でも，ホスト OS への影響を防ぎ，様々な環境を構築，Web クライアントからの試行を容易にできる．これにより，要件3に対応する．

再現端末では，WiresharkやProcess Monitorなど，インシデントを観測・記録するためのツールを動作させる．再現端末から Web クライアントを用いて疑似 Web サイトにアクセスし，マルウェア感染時の挙動が再現されることで，改めて痕跡の観測・記録ができる．

3. システムの試作と動作確認

PC(CPU: Intel core i7 3.3GHz ，Main memory: 16GB, OS: Windows 10 Pro 64bit)上に，Virtual Box を用いて疑似 Web サイト，誘導 DNS サーバ用のゲスト OS（Ubuntu 14.04)と再現端末のゲスト OS（Windows 7 32bit SP1, Internet Explorer 11）を導入した．

実験に使用する通信パケットのログは MDL[2]にある悪性 Web サイトに Web クローラを用いてアクセスを行いその通信を Wireshark で記録したものを複数用意した．本システムで，用意した通信パケットのログを使用し入出力表を作成，再現端末の Web クライアントからアクセスし，再現対象の悪性 Web サイトが閲覧できることを確認した．

実際に再現を行った様子を図 2 に示す．左半分が実験に使用した通信パケットのログの内容を Wireshark で表示したものである．右半分は，用意した再現端末から Web クライアントを使用して悪性 Web サイトが再現された様子である．本実験は再現端末にプライマリ DNS として誘導 DNS サーバを指定し，悪性 Web サイトへアクセスを行った．図2の右半分に示す通り，アクセスを行った Web サイトが再現できていることがわかる．通信の再現については，再現対象とする通信パケットのログと再現時に行われた通信の内容とを比較することで確認した．本実験を通して，HTTP 通信について正しく再現できることが確認できた．

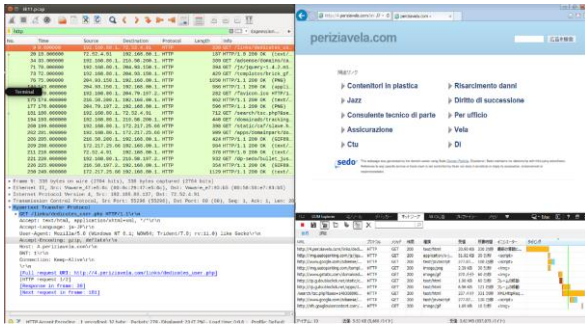

図 2　通信パケットのログと再現した Web ページの例

（左：Wireshark で PCAP ファイルを表示したもの

右：IE11 で表示した悪性 Web サイト）

4. 関連研究

社内ネットワークなどを再現した環境で実際のマルウェアなどを発生させその挙動をホストおよびネットワークの両面から分析し，対処方法を体験できる，攻撃再現環境の技術が開発されている[3]．

攻撃対象ごとにマルウェアの検体が異なり，動的解析のために攻撃対象を含む環境情報も再現しないとマルウェアの活動の全体が把握できないことから高詳細な攻撃対象環境を模倣した環境の構築と動的解析を自動化するシステムが提案されている[4]．

本研究で扱うシステムは，インシデントの初動対応または調査の場面で，入手した通信パケットのログから，マルウェア感染の過程を再現して，当時，得られなかった，インシデントに関連する事象や OS やアプリケーションの振る舞いの履歴を収集して，解析を支援することに注目している．

5. まとめ

本研究では，マルウェアの感染と活動の調査の支援を目的とし，通信パケットのログから悪性 Web サイトを復元，Web クライアントの挙動を再現して，事後の調査を支援するシステムを開発した．

MDL にある悪性 Web サイトの一つに Web クライアントがアクセスしたときの通信パケットの記録を用意し，その記録から，悪性 Web サイトを復元して実際に Web クライアントからアクセスさせ，挙動が再現されることを確認した．

現在，リンク先やリダイレクト先，ダウンロード元のホストを，そのまま IP アドレスを用いて指定している場合，誘導 DNS サーバでは対応できないため，今後，レスポンスのデータを適宜書き換える処理を含めることを検討する．また，悪性 Web サイトを介したマルウェア感染事例を整理して，本システムによって Web サイトの振る舞いの再現が可能な範囲を明確にすることが挙げられる．

5. 参考文献

1) Jason T. Luttgens，Matthew Pepe，Kevin Mandia：Incident Response & Computer Forensics，Third Edition，NIKKEI BP. INC.(April 2016)
2) “Malware Domain List”, <https://www.malwaredomainlist.com/>
3) 三輪 信介，門林 雄基，篠田陽一：小規模攻撃再現テストベッドによる動作記録データセットの生成，マルウェア対策研究人材育成ワークショップ（MWS2009）発表資料，A9-2(2009年10月)
4) 安田真悟，三浦良介，高野祐輝，宮地利幸：Alfons：マルウェア解析の為の高詳細な環境構築システム，電子情報通信学会技術研究報告，ICM，114(523)，pp.139-144(2015年3月)