2W-05

通信パケットの記録からの Web を介する攻撃の再現

奥田　裕樹†　　福田　洋治‡　　井口　信和‡

近畿大学大学院総合理工学研究科†　　近畿大学理工学部情報学科‡

1. はじめに

組織内の端末が Web を介しマルウェアに感染して，情報の漏洩や金銭の要求，不正な遠隔操作が行われるなどの，インシデントの報告が増加の一途を辿っている．インシデント対応では，根絶と復旧，再発予防の観点で，当時起こった事柄を正確に把握することが求められる．しかしながら，端末で履歴が記録されていない，または消去・攪乱されると，その起こった事柄の全容を把握できない場合がある [1]．

これまで著者らは，インシデント対応における調査活動を支援するためのフォレンジック支援システムを開発してきた [2]．著者らのシステムは，通信パケットの記録から Web サイトを復元し再現端末からこれにアクセスし Web を介した攻撃を再現して，起こった事柄を観測できる．

本稿では，著者らのシステムにより再現できる Web を介した攻撃を明らかにするための実験を行い，その結果について述べる．

2. システムの概要

著者らのシステムは，図 1 のように，疑似 Web サイトと誘導 DNS サーバから構成されており，復元した Web サイトに対し，仮想環境上の Web ブラウザからアクセスすることでアクセス時の Web ブラウザの挙動がそのまま再現される．

再現対象となる通信パケットの記録からリクエストとそれに対応するレスポンスを抽出し，その対応を入出力表として保持する．この表を基に受信したリクエストに対応するレスポンスをアクセス元の Web ブラウザに対し返送することによって Web ページを復元する．

抽出したリクエストのホスト名と疑似 Web サイトの IP アドレスを対応付け，A レコードとし誘導 DNS サーバに登録する．この誘導 DNS サーバが仮想環境からの名前解決を行うことで通常のアクセスを疑似 Web サイトに誘導する．これにより，通常の Web 利用と変わらずに当時アクセスされた Web ページとその挙動が再現できる．

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して使用することを想定している．これにより，実際にマルウェアが感染した場合においてもホスト OS への影響を防ぎ，様々な環境の構築や Web クライアントからの試行を容易にする．

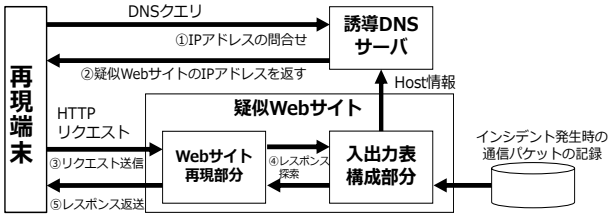

図 1 システムの構成と動作

著者らのシステムは通信パケットの記録から，個々の HTTP セッションを抽出し当時の Web サイトの挙動が再現でき（要件 1），Web クライアントを操作しアクセスすることで当時の Web ページやファイルが実際に閲覧（リダイレクトにも対応），ダウンロードできる（要件 2）．また，仮想化技術を用いることで Web クライアントの種類やアドオン，OS などの環境を容易に変更することができ，繰り返し初期状態に戻してアクセスを試行することができる（要件 3）．

3. 実験

先に挙げた要件を満たす著者らのシステムは，仮想環境上の端末にて，Web ブラウザから復元した Web サイトにアクセスさせることで，Web を介した誘導型攻撃を再現し，エクスプロイトの影響やマルウェアの挙動を観測できる調査支援の環境を提供する．端末に対して Web を介して行われる誘導型攻撃は，表 1 に挙げるような攻撃，使用する技術のパターンに分けられ [3]，著者らのシステムにより攻撃を再現できるかを確認する実験を行う．

この実験では，先に挙げた端末に対する Web を

表 1 調査を行う攻撃の種類

攻撃	使用する技術
DBD攻撃 水飲み場型攻撃	JavaScript
	iFrame
	locationタグ
XSS	Stored XSS
ClickJack攻撃	frame
	iFrame
標的型メール攻撃	URLのクリック
フィッシング攻撃	URLのクリック

Reproduction of Attacks via Web by Using Captured Packets
† Yuki OKUDA, Graduate School of Science and Engineering Research, Kindai University
‡ Youji FUKUTA and Iguchi NOBUKAZU, Faculty of Science and Engineering, Kindai University

介した攻撃を，Metasploit を用いて行い，端末にて Wireshark でその時の通信パケットを観測，pcap 形式で記録して，著者らのシステムでその時と同じ攻撃を再現できるかどうかを試す．著者らのシステムは，PC（CPU:Intel Core i7 3.3GHz, OS:Windows10 Pro 64bit, Memory:16GB ） 上 に Virtual Box を使用して再現端末（OS:Windows7 32bit SP1 English, Web ブラウザ:Internet Explorer 8）と，誘導 DNS サーバ Unbound Ver.1.4.22 と疑似 Web サイト用のホスト（OS:Ubuntu 14.04 LTS）を配置し，閉じたネットワーク上で動作させる．実験開始から Internet Explorer の挙動がなくなり，Process Monitor や Wireshark などで特異な挙動が見られなくなるまでの通信パケットの記録や，Process Monitor の記録から，調査対象の攻撃が正しく再現されたかを判断する．

DBD 攻撃の実験として，それぞれの技術を用いてリダイレクトを複数回行い，バックドアプログラムをダウンロードさせるものを用意した．再現した際の通信パケットの記録から，用意した攻撃と同一のリダイレクト回数と同一の HTTP リクエストが送信されていることが確認できた（図 2）．この結果から，DBD 攻撃について再現できたと考えられる．

XSS の実験として，Stored XSS を用意した．攻撃者が DB に悪意のあるスクリプトを登録し，利用者が Web ページを表示する際にそのスクリプトを読み込むことで攻撃が行われるものである．攻撃の再現において，DB から呼び出されるものが変化し攻撃当時と異なるリクエストが行われた場合，本システムはレスポンスを返せず，攻撃が再現できなかった．結果から，内容が変化する Web ページを利用した攻撃について本システムは再現できない場合があることがわかった．

ClickJack 攻撃の実験として，2 種類のタグを用いて Web ページ上に透過した Web ページを重畳表示させ，利用者の意図しない透過された上層の Web ページのリンクをクリックさせるものを用意した．この攻撃を再現した結果，リンクをクリックすると攻撃用の Web ページへのリクエストの送信を確認した．この結果から，ClickJack 攻撃について再現できたと考えられる．

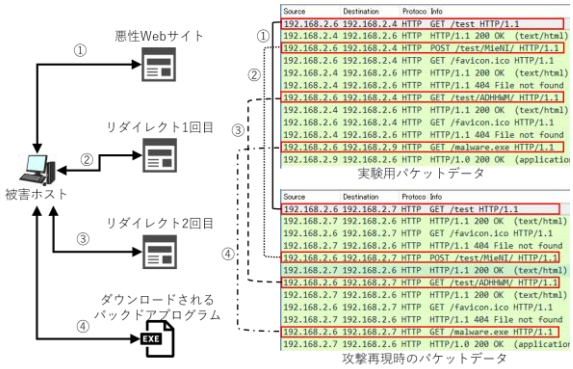

図 2 DBD 攻撃についての実験とその結果

標的型メール攻撃とフィッシング攻撃の実験について，双方ともにメールに URL リンクが張り付けられており，そのリンクをクリックすることによって攻撃が行われるものを用意した．リンクをクリックすると用意した Web ページが表示され，バックグラウンドでバックドアプログラムがダウンロード，実行される．この攻撃を再現した結果，Web ページの表示とバックドアプログラムのダウンロードが正しく行われることを確認した．この結果から，本システムは URL リンクを用いるメールを利用した攻撃について再現できたと考えられる．

実験の結果から，今回実験を行った Web を介した誘導型攻撃について，本システムを用いることで再現できると考えられる．しかし，クライアントサイドスクリプトでコンテンツを呼び出す場合において，当時と異なる内容を表示させる場合，本システムは対応できず攻撃を再現できなかった．この場合，当時とは異なるリクエストが送信されたと考えられる．本システムは入出力表にあるリクエストと一致しないリクエストを受信した場合，レスポンスを返せない．そのため，再現する Web ページから発生したリクエストに対し，入出力表に含まれるリクエストで対応させる必要があると考える．

4. まとめ

著者らのシステムは，通信パケットの記録から Web サイトを復元し，仮想環境上の端末からこれにアクセスし，Web を介した攻撃を再現して，起こった事柄を観測できる．

本稿では，著者らのシステムにより再現できる，端末に対して Web を介して行われる誘導型攻撃を明らかにするため，各種の攻撃の通信パケットの記録を，Metasploit を用いて作成して，攻撃を再現できるかを確認する実験を行った．

実験から，今回実験した Web を介する攻撃についてリクエストが攻撃当時と同じであれば本システムで再現できることがわかった．

参考文献

1) Jason T. Luttgens, Matthew Pepe, Kevin Mandia：Incident Response & Computer Forensics, Third Edition, NIKKEI BP. INC.(April 2016).
2) 奥田裕樹, 福田洋治, 白石義明, 井口信和:ドライブ・バイ・ダウンロード攻撃によるインシデントを再現するフォレンジック支援システム, 電子情報通信学会技術研究報告(ICSS), Vol.117, No.125, pp.81-86(2017).
3) Patil,D.R. and Patil, J.B.: Survey on malicious web pages detection techniques, SERSC Australia, Vol.8, No.5, pp.195-206(2015).