Drive-by Download 攻撃検知手法の継続的評価と Exploit Kit に対する考察

小林 峻[†1]　寺田 成吾[†1]　瀬戸口 武研[†1]　道根 慶治[†1]　山下 康一[†1]

概要：我々は，ネットワーク通信を監視し，正規アプリケーションには見られない特有の通信挙動を示すことに着目することで，攻撃者およびマルウェアに察知されることなく Drive-by Download 攻撃（以下，DbD 攻撃）による感染端末を検出する手法を提案した．しかし年々高度化が進むサイバー攻撃の分野においては，対策手法が有効であるか継続して評価していく必要がある．そこで本稿では，最近の DbD 攻撃を含むトラフィックデータを用いて，あらためて本検知手法の評価を行ない，その評価結果を基に攻撃手法についてネットワークトラフィックの観点から分析し，攻撃者の利用する Exploit Kit に関する巧妙な偽装技術の知見を示した．

キーワード：MWS, Drive-by Download 攻撃, Exploit Kit, ネットワーク通信

Continuous Evaluation of Drive-by Download Detection Method and A Study on Exploit Kits

Takashi Kobayashi[†1]　Seigo Terada[†1]　Mugen Setoguchi[†1]
Keiji Michine[†1]　Kouichi Yamashita[†1]

Abstract: We proposed the method detects devices infected by Drive-by Download attacks (DbD attacks) by observing on a network traffic without being noticed by attacker or malware. It focus on DbD attacks has specific network traffic behaviors are different from formal applications. However, in view of evolving cyber-attacks trend, we should continue validation of the method efficiency. In this paper, therefore, we evaluated the effectiveness by using recent traffic data has some flow of DbD attacks. We analyzed the evaluation from the point of view of network traffic and showed imitative technique with exploit kits used by attackers.

Keywords: MWS, Drive-by Download Attack, Exploit Kit, Network Communication

1. はじめに

昨今，サイバー攻撃の被害件数は年々増加の一途をたどっている．攻撃手法やマルウェアも日々高度化しており，これらの進化する脅威に対応できる検知・対策技術が求められている．マルウェアの感染経路には様々なものがあるが，Web を経由して感染させる攻撃手法として，Drive-by Download 攻撃（以下，DbD 攻撃）がある．DbD 攻撃は，標的とする組織や個人が閲覧する Web サイトや Web 広告を介して，端末内アプリケーションの脆弱性を攻撃し，マルウェアを利用者の端末へ秘密裏にダウンロードさせる攻撃手法である．また，マルウェア侵入の検知技術にも様々なものがあるが，近年のマルウェアには検知機能を回避する仕組みを備えているものも多い. そのため DbD 攻撃においては，マルウェアそのものではなく，攻撃の特徴に着目して検知する手法が研究されている．[1][2][3][4]

我々の研究では，攻撃者およびマルウェアの活動をネットワーク通信の観点で 8 つのフェーズに整理した”攻撃者行動遷移モデル”を定義し, 監視する端末の通信を各フェーズに当てはめ, フェーズの遷移を分析することで DbD 攻撃を検知する手法を提案し，その有効性を示してきた．[5]しかし，サイバー攻撃の高度化という背景を鑑みると，検知技術の有効性を継続的に評価し，技術の改良や新しい対策技術を考案していくことが重要である．そこで本稿では，DbD 攻撃手法の変化および動向について，検知手法の改良や新しい対策の考案につながる新しい知見を示すことを目的とする．まず，DbD 攻撃手法の変化を確認するために，本検知手法を最近の攻撃トラフィックデータによって評価した結果を示す．そして，評価結果を基にトラフィックデータを調査し，個々の通信特徴の変化，および攻撃全体の特徴をまとめ，DbD 攻撃に使われる Exploit Kit の高度化に関する知見を示す.

2. 関連研究

HTTP 通信の遷移に注目した DbD 攻撃検知に関する研究としては, 北野ら[1]や工藤ら[2]によってネットワーク機器やセキュリティ機器のログから，攻撃特徴の遷移を分析して検知する手法が提案されている. 松中ら[3]や佐藤ら[4]は, Web ページのリンクやリダイレクトによるページ遷移に着

†1 株式会社 PFU
PFU LIMITED

目して悪性サイトを検出する手法を提案している．また，DbD 攻撃にかかわる悪性コンテンツについて詳細な分析を行なった研究としては，今野ら[7]による悪性 PDF ファイルの考察，Ford ら[6]による SWF ファイルの静的および動的解析による悪性判定手法の提案などがある．これらに対し，我々はネットワーク通信を直接観測し，HTTP のコンテンツを検査対象とするが，コンテンツが悪性であるかどうかを検査しない，検知精度と軽量さを両立させた手法を提案した．[5]

検知技術の継続的な評価を行なった研究としては，益子ら[8]による，北野ら[1]の手法について Exploit Kit の時系列的な特徴の変化を分析し，改良方法を検討した研究がある．

3. 検知手法

本章では，本稿で評価を行なう DbD 攻撃検知手法[5]の概要を説明する．

3.1 攻撃者行動遷移モデル

まず，本手法で定義する，“攻撃者行動遷移モデル”を説明する．本モデルは，攻撃者とマルウェアの活動をネットワーク通信の観点で 8 つのフェーズに整理（表 1）し，さらにそれぞれのフェーズから別のフェーズへの遷移を整理（図 1）したものである．

表 1 攻撃者およびマルウェアのフェーズ

番号	内容
Phase1 (P1)	ソフトウェアの脆弱性を悪用し，マルウェアのダウンロードとインストールを試みる．
Phase2 (P2)	ネットワーク環境の探索．グローバル IP アドレスの確認や近隣端末の探索など．
Phase3 (P3)	感染可能な端末へのマルウェアのコピーやリモート実行による感染．
Phase4 (P4)	実行形式ファイルをダウンロードし，マルウェアの機能追加やツールの追加を行う．
Phase5 (P5)	遠隔操作を行うために接続可能な C&C サーバを検索する．
Phase6 (P6)	C&C 通信で遠隔操作が行われる．感染端末の生存確認も含まれる．
Phase7 (P7)	侵害した組織で収集した機密情報などを外部へ持ち出す．
Phase8 (P8)	DDoS 攻撃などを行うためのボットとして，攻撃活動に参加させる．

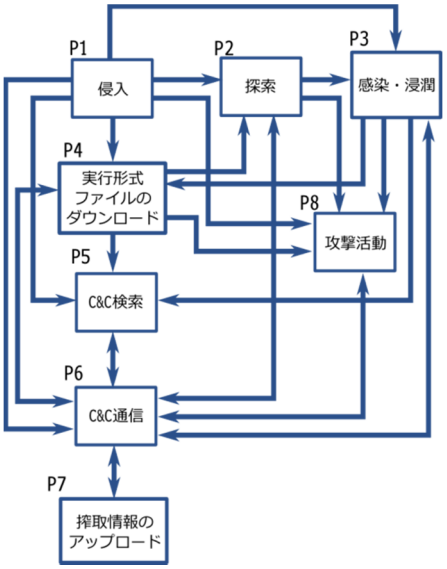

図 1 攻撃者行動遷移モデル

本モデルは，いままで“マルウェア活動遷移モデル”と称していたが，マルウェア個別の活動だけでなく攻撃者の行動にも着目しているため，より広義の“攻撃者行動遷移モデル”と改めた．

3.2 本モデルを用いた DbD 攻撃の検知

DbD 攻撃は以下の図 2 に示す流れで実行される．

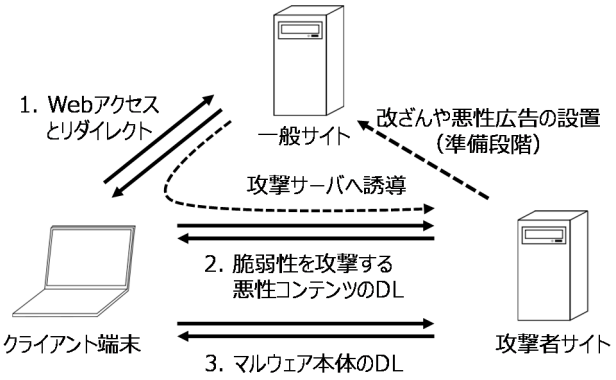

図 2 DbD 攻撃の流れ

準備段階

一般サイトの改ざんや悪性広告の配信によって，攻撃者のサーバへ誘導するリンクやスクリプトを挿入する．

1. Web アクセスとリダイレクト

標的ユーザーが上記準備段階で改ざんされた一般サイトにアクセスすると，攻撃者の挿入したコンテンツによって，攻撃者のサーバへ誘導される．

2. 悪性コンテンツのダウンロード

攻撃者のサーバから標的ユーザーが利用するアプリケーションの脆弱性を攻撃する悪性コンテンツがダウンロードされる．

3. マルウェア本体のダウンロード

悪性コンテンツによる攻撃が成功すると，マルウェアが自動的にダウンロードされる．

本モデルを用いた DbD 攻撃の検知は, ネットワーク上で端末の行なう通信をリアルタイムで監視し，“2. 悪性コンテンツのダウンロード”の攻撃活動を Phase1，“3. マルウェア本体のダウンロード”の攻撃活動を Phase4 へ当てはめ, この相関を分析してフェーズの遷移を検出することによって実現される.

3.3 通信とフェーズの識別

まず Phase1 は, 攻撃対象となる脆弱性をもつ端末内アプリケーションによる通信である．そのため，脆弱性が狙われることが多い Java[a], Silverlight[b], Flash[c], PDF, JavaScript[d]の通信を悪性コンテンツ候補として検査対象としている．これらの悪性コンテンツ候補を識別する検査では，HTTP の GET リクエストに含まれる URI のファイル拡張子(.jar, .swf など）やリクエストヘッダー（User-Agent ヘッダーや x-flash-version ヘッダーなど)，を監視し，レスポンスに含まれる Content-Type ヘッダーとボディ部に含まれるファイルのマジックナンバーを検査して悪性コンテンツ候補のダウンロードを識別する.

次に，Phase4 はマルウェア本体をダウンロードする通信である．本手法では，ファイルそのものの悪性検査は行なわないため，実行形式のファイルであることが推測されるダウンロード通信を Phase4 として識別している. 実行形式ファイルを識別する方法は，Phase1 での検査箇所に加え，Content-Disposition ヘッダーや ZIP 等のアーカイブ内に含まれるファイルの拡張子（.exe, .dll など）を検査して識別する．さらに，Content-Type ヘッダーとボディ部のコンテンツの整合性検査を行なうことで，ヘッダーが偽装されたファイルや難読化されたバイナリファイルについても，怪しいファイルのダウンロードであるとみなし，Phase4 として識別する.

3.4 フェーズ間遷移の相関分析

本手法において, Phase1 から Phase4 への遷移は, 表 2 に示す相関条件に基づいた分析を行なうことで検知している. 表で示す“TCP コネクション”は，Phase1，Phase4 の通信が行なわれる接続先サーバとの TCP コネクション状態の条件である．また，“HTTP 通信の割り込み”は，Phase1 と Phase4 の通信が異なるコネクションで行なわれた場合において, Phase1 と Phase4 の間に少数の割り込みを許容する条件である.

表 2 Phase1-Phase4 の相関条件

相関条件	TCP コネクション	HTTP 通信の割り込み
CA1	同一	—
CA2	異なる	なし
CA3	異なる	GET メソッド
CA4	異なる	POST メソッド

3.5 本手法の特徴

本手法は，個々のコンテンツやマルウェア本体の悪性な特徴ではなく，攻撃活動によって生じる通信特徴の遷移に着目している．そのため，攻撃手法が変化しない限り有効な手法であると考えられる．また，HTTP メッセージのボディ部も検査対象としており，攻撃者が容易に偽装可能なヘッダー情報を用いる検知手法に比べ，回避されにくい.

4. 評価

本章では，D3M[9]や Threatglass[10]のデータセットを用いて評価を実施してきた本検知手法が，それ以降に行なわれた DbD 攻撃に対してどの程度有効であるか, また本検知手法で検知できなくなった攻撃手法の変化を確認するため, 新しいデータセットを利用して実施した評価結果を示す.

4.1 データセット

評価に利用するデータセットは，Malware-Traffic-Analysis.net[11]（以下，MTA）で公開されているキャプチャファイル（.pcap）を利用した．MTA は，2013 年から継続的にマルウェアや Exploit Kit のトラフィックデータとブログを公開しているサイトであり，Exploit Kit の特徴を研究するデータセットとしても利用されている[12]．今回は，2015 年 1 月から 2016 年 6 月 10 日までに公開されたもので，主要な Exploit Kit (EK)である Angler EK, Nuclear EK, Rig EK, Neutrino EK, Magnitude EK, Fiesta EK のキャプチャファイル全 448 個を抽出した．さらに， DbD 攻撃の全容が含まれていないと考えられるものや，分析時にノイズとなる以下の条件に該当するデータはあらかじめ除外し, 422 個のキャプチャファイルを評価に利用した.

【除外したキャプチャファイルの条件】

- ファイル名に“payload”または“fail”を含む（18 個）
- ファイル名に複数の EK 名を含む（4 個）
- ファイルサイズが 100KB 未満（4 個）

a Java は，Oracle Corporation 及びその子会社，関連会社の米国及びその他の国における登録商標です.
b Silverlight は，米国 Microsoft Corporation の，米国，日本およびその他の国における登録商標または商標です.
c Flash は，Adobe Systems Incorporated（アドビ システムズ社）の米国ならびに他の国における商標または登録商標です.
d JavaScript は，Oracle Corporation 及びその子会社，関連会社の米国及びその他の国における登録商標です.

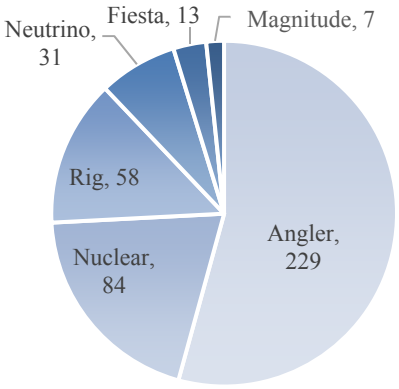

図 3　対象とした Exploit Kit とその割合

今回対象とした Exploit Kit 以外には，Sweert-Orange EK, Blackhole EK, KaiXin EK のキャプチャファイルが含まれていた．しかし，いずれも数が少なく傾向がつかみにくいため評価データには含めないこととした．

4.2　評価方法

本検知手法は，ネットワーク通信をモニタリングし，リアルタイムで解析するプログラムとして実装されている．しかし，多くのキャプチャファイルを評価する場合，トラフィックを再生するために多大な時間がかかるため，効率的な評価ができない．そこで，解析プログラムにキャプチャファイルを直接読み込む改造を行ない，タイムスタンプを基準に処理するプログラムを作成した．このプログラムに，評価するキャプチャファイルを順番に処理させ，それぞれのファイルに対し DbD 攻撃を検知できたかどうか，評価を実施した．また，ベースとする解析プログラムは 2015 年 11 月時点のものを使用し，改良後の評価についても同様の方法で再評価を行なった．

4.3　評価結果

処理させたキャプチャファイルを 1 月から 3 ヶ月ごとの区間で区切り，評価結果を表 3 にまとめた．検知できていないファイルには，キャプチャ品質が悪いものや攻撃通信の一部しか記録されていないものも多く残っている．これらについては一定の条件で除外することが難しいが，検知する必要はないものであり，よって検知率を 100%にすることはできない．今回の評価では，Angler EK 以外の Exploit Kit について検知率の極端な変化は見られなかったが，Angler EK では 2016 年 4 月以降に大きな低下がみられた．この評価結果から Angler EK の攻撃手法に大きな変化があったことが推測できる．

5.　分析

本章では，4 章で得られた評価結果をもとに，検知できなくなった Angler EK のキャプチャファイルと，その攻撃手法の変化について分析した結果，および改良後の評価結果を示す．また，分析する上で必要な SWF ファイルの構造についても簡単に解説する．

5.1　Angler EK の攻撃シーケンスの分析

Angler EK の代表的な攻撃は，図 4 に示したように，ま

表 3　MTA データセットを用いた評価結果

Exploit Kit		2015年				2016年		全期間合計
		1～3月	4～6月	7～9月	10～12月	1～3月	4～6月	
Angler EK	データ数	4	21	35	28	88	53	229
	検知数	4	16	34	26	86	3	169
	検知率	100.0%	76.2%	97.1%	92.9%	97.7%	5.7%	73.8%
Nuclear EK	データ数	12	8	40	17	7	0	84
	検知数	12	8	37	16	6	0	79
	検知率	100.0%	100.0%	92.5%	94.1%	85.7%	-	94.0%
Rig EK	データ数	2	2	6	25	11	12	58
	検知数	2	2	6	22	9	12	53
	検知率	100.0%	100.0%	100.0%	88.0%	81.8%	100.0%	91.4%
Neutrino EK	データ数	2	3	9	4	1	12	31
	検知数	2	3	9	4	1	11	30
	検知率	100.0%	100.0%	100.0%	100.0%	100.0%	91.7%	96.8%
Fiesta EK	データ数	5	7	1	0	0	0	13
	検知数	5	7	1	0	0	0	13
	検知率	100.0%	100.0%	100.0%	-	-	-	100.0%
Magnitude EK	データ数	3	1	3	0	0	0	7
	検知数	3	1	3	0	0	0	7
	検知率	100.0%	100.0%	100.0%	-	-	-	100.0%
6EK合計	データ数	28	42	94	74	107	77	422
	検知数	28	37	90	68	102	26	351
	検知率	100.0%	88.1%	95.7%	91.9%	95.3%	33.8%	83.2%

ず標的ユーザーが攻撃者に改ざんされた一般サイトや，悪性なリダイレクトコードを含む広告を表示することによって，攻撃者のサーバへ誘導される．すると，攻撃者のサーバから脆弱性を攻撃する通信（図中①）が GET メソッドによって行なわれ，それによって引き起こされた通信（図中②）で利用者端末にマルウェアがダウンロードされる．

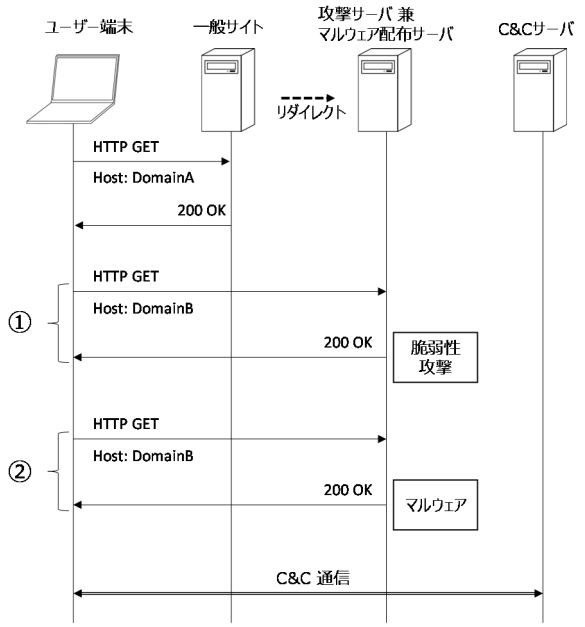

図 4 Angler EK の攻撃シーケンス

先に述べたように本検知手法では，脆弱性攻撃に関するダウンロード通信を Phase1，マルウェア本体のダウンロード通信を Phase4 として識別することによって，その遷移を検出して DbD 攻撃を検知する．しかし，今回検知できなかったパターンでは，いままでの検査方法で Phase4 として識別可能な通信が含まれていないことが原因であることがわかった．

そこで，実際に検知できなかったキャプチャファイルを見ていくと，2 つの SWF ファイルがダウンロードされていることがわかった．1 個目の SWF ファイルのダウンロードは，Flash Player の脆弱性を攻撃すると考えられる通信であり，Phase1 と識別されるべきものである．しかし，2 個目の SWF ファイルについては，ダウンロードの直後から，C&C 通信と考えられる通信が発生しているため，SWF ファイルに偽装したマルウェア本体のダウンロード通信であることが示唆される．本通信は，HTTP メッセージの各種ヘッダーや SWF ファイルの特徴から Phase1 として識別されるが，攻撃者の活動に当てはめると，本来は Phase4 として識別される通信である．

本手法においては，脆弱性攻撃とマルウェア本体のダウンロード，それぞれの役割を区別できれば，再び検知できるようになるはずである．そのため，これらの SWF ファイルの特徴について分析を行なった．

5.2 SWF ファイルの構造

まず SWF ファイルの構造について整理する．本研究では，コンテンツそのものの悪性には着目しないため，表層的な部分のみ解説する．SWF は Adobe 社によって仕様が公開されたファイルフォーマットであり，ファイルの全体構造は，図 X に示すようにヘッダーに複数のタグが連なったブロック構造となっている．[13]

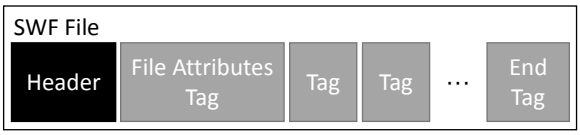

図 5 SWF ファイルの全体構造

また，先頭に位置するヘッダーには，表に示すようにシグネチャとバージョンおよびファイルサイズが格納されている．このシグネチャの先頭文字の種類によって，後方に格納されるデータの圧縮形式を示しており，ZLIB 形式と LZMA 形式での圧縮をサポートしている．圧縮が行なわれる場合，ファイルサイズを示す FileLength フィールドには，圧縮前および展開後のファイルサイズが格納され，ヘッダーの 8 バイト目以降のデータが圧縮される．

表 4 SWF ファイルのヘッダー構造

Signature（3byte）	FWS(0x465753)：非圧縮形式 CWS(0x435753)：ZLIB 形式 ZWS(0x5a5753)：LZMA 形式
Version（1byte）	符号なし 8bit 整数
FileLength（4byte）	符号なし 32bit 整数 （リトルエンディアン）
フレーム情報（可変長）	※圧縮される場合はこのデータから圧縮される

5.3 SWF ファイルの分析

キャプチャファイルから得られた 2 つの SWF ファイルについて，ファイルフォーマットに従い表層的な分析を行なった．先にダウンロードされた小さい SWF ファイルを“swf-1”，後にダウンロードされた大きい SWF ファイルを“swf-2”として，ヘッダーから得られる情報を表にまとめた．両者とも ZLIB 形式で圧縮されたデータである．swf-2 については Version が 6 と swf-1 に比べ古いが，ZLIB 形式をサポートしているバージョンは 6 以降であるため，SWF ファイルのヘッダーから得られる情報に異常は見られなかった．

表 5 SWF ヘッダーから得られる情報

	swf-1	swf-2
Signature（圧縮形式）	CWS(ZLIB)	CWS(ZLIB)
Version	13	6
FileLength (byte)	45,150	1,020

さらに，SWF ヘッダーの 8 バイト目以降について ZLIB を利用して展開を試みると，SWF ヘッダーの FileLength フィールドに記載されたサイズとなるデータを得ることができた．しかし，swf-2 については，ZLIB では展開できない余分なデータが存在し，HTTP で実際に転送されたデータと比べると，展開可能だったデータはずっと小さいことがわかる. 今回はこれ以上に詳細な分析は行なっていないが，先に述べたとおり swf-2 のダウンロードの後には，C&C 通信と見られるトラフィックが発生している. そのため, swf-2 は先頭にダミーの SWF ファイルが連結された，マルウェア本体である可能性が高いと考えられる．

表 6 データ長の比較（単位：byte）

	swf-1	swf-2
HTTP Content-Length	40,825	205,482
SWF FileLength	45,150	1,020
(Uncompressed header)	8	8
ZLIB decompressed size	45,142	1,012
ZLIB unused data size	0	204,825

swf-2 のような単純に結合されたデータにおいては，実際のファイルサイズや，データの境目等に着目することによって，付加されたデータを識別し，異常な SWF ファイルを区別することが可能である．

5.4 リクエストヘッダーの変化

マルウェア本体の SWF ファイルへの偽装のほかに，マルウェア本体をダウンロードする HTTP リクエストにも変化があった．キャプチャファイルを過去に遡って調べてみると，2016 年 1 月前後に取得された Angler EK のトラフィックデータからヘッダーの特徴に変化が生じている. また，本検知手法では 2016 年 1 月前後での検知率に差がないことから，リクエストヘッダーの特徴の変化による影響は受けていないことがわかる．

```
GET /same.asmx?apply=&able=iYw&add=h8i4kiQB&later=
Connection: Keep-Alive
Accept-Language: en-EN
Host: s[redacted].com
```

図 6 2015 年 12 月のリクエストデータ

```
GET /police.jsf?she=Lggj&case=&experience=k_uKQ&sou
Connection: Keep-Alive
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Referer: http://www.r[redacted]d.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Tride
Host: [redacted]g.com
```

図 7 2016 年 1 月のリクエストデータ

これまで脆弱性攻撃後に発生する通信では，User-Agent や Referer など，マルウェアのダウンロードに関係のないヘッダーは付加されてこなかった. そのため, Exploit Kit の特徴的な通信パターンとしてよく利用されてきた．[3][4]

しかし，攻撃者が発生させる通信は，正常な通信と見分けるのが難しくなっており，あらためて分析してみると，攻撃通信を見分けるポイントが以前よりずっと少なくなっていることがわかる．

5.5 改良後の再評価

これまでに述べてきた SWF ファイルを識別するための修正を加えたプログラムを作成し，同様のデータを用いて再評価を行なった．評価結果を表 7 に示す．

この修正により低下した検知率は以前と同等のレベルまで回復した．一方で，検知したときの相関条件の変化について注目すると，検知率が低下した Angler EK については，評価期間全体にわたって，ほとんどを CA2 の条件で検知している．つまり，個々の通信パターンに比べ，フェーズの遷移にかかわる相関条件は変化しにくい特徴であることがわかる．また，攻撃フェーズの遷移に着目した攻撃者行動遷移モデルは，DbD 攻撃の通信パターンの変化に対しても有効であることが示された．

表 7 改良後の評価結果と各相関条件

Angler EK		2015年				2016年		全期間合計
		1～3月	4～6月	7～9月	10～12月	1～3月	4～6月	
データ数		4	21	35	28	88	53	229
検知数	CA1	0	0	0	0	0	0	0
	CA2	4	15	32	26	83	50	210
	CA3	0	1	3	0	0	0	4
	CA4	0	0	0	0	2	1	3
	合計	4	16	35	26	85	51	217
検知率		100.0%	76.2%	100.0%	92.9%	96.6%	96.2%	94.8%

6. まとめ

本稿で得られた知見を以下にまとめる．

- 攻撃者行動遷移モデルを利用した 2015 年 11 月時点の DbD 攻撃検知手法が，以降に観測された攻撃を検知できるか評価し，その結果を示した．
- ネットワーク通信の観点で，最近の Exploit Kit および DbD 攻撃手法の高度化について，Angler EK を例に具体的な変化を示した．
- Exploit Kit による個々の通信パターンが変化しても，DbD 攻撃の手法に大きな変化はなく，攻撃者行動遷移モデルを用いた検知手法が有効であることを示した．

今後については，ネットワーク観点での攻撃手法の変化について，引き続き調査を行なっていくとともに，攻撃者行動遷移モデルにおける他のフェーズの評価なども行なっていく予定である．

参考文献

[1] 北野美紗，大谷尚通，宮本久仁男. Drive-by-Download 攻撃における通信の定性的特徴とその遷移を捉えた検知方式. コンピュータセキュリティシンポジウム 2013 論文集, p.595-602.

[2] 工藤聖，トラン・コン・マン，中村康弘. HTTP リクエストシーケンスに注目した不正リダイレクトの検出. コンピュータセキュリティシンポジウム 2015 論文集, p.221-225.

[3] 松中隆志，窪田歩，星澤裕二. Drive-by Download 攻撃対策フレームワークにおける Web アクセスログを用いた Web リンク構造の解析による悪性サイト検出手法の提案. コンピュータセキュリティシンポジウム 2014 論文集, p.559-566.

[4] 佐藤祐磨，中村嘉隆，高橋修. 通信遷移と URL の属性情報を用いた悪性リダイレクト防止手法. コンピュータセキュリティシンポジウム 2015 論文集, p.8-15.

[5] 寺田成吾，小林峻，小出和弘，羽藤逸文，瀬戸口武研，道根慶治，山下康一. ネットワーク通信の相関性に基づく Drive-by Download 攻撃検知手法. コンピュータセキュリティシンポジウム 2015 論文集, p.1-7.

[6] Ford Sean, Cova Marco, Kruegel Christopher, Vigna Giovanni. “Analyzing and Detecting Malicious Flash Advertisements” Proceedings of the 2009 Annual Computer Security Applications Conference, p.363-372.

[7] 今野由也，角田裕. Drive-by-Download 攻撃における悪性 PDF の特徴に関する考察. コンピュータセキュリティシンポジウム 2014 論文集, p.25-31.

[8] 益子博貴，重田真義，大谷尚道. Exploit Kit の変化への適応を目的としたサイバー攻撃検知システムの改良. コンピュータセキュリティシンポジウム 2015 論文集, p.24-31.

[9] 神薗雅紀，秋山満昭，笠間貴弘，村上純一，畑田充弘，寺田真敏. マルウェア対策のための研究用データセット～MWS Datasets 2015～. 情報処理学会 研究報告コンピュータセキュリティ(CSEC) Vol. 2015-CSEC-70, No6.

[10] Barracuda Labs, “Barracuda Labs Threatglass” Barracuda Networks, Inc. http://www.threatglass.com/ (2016/7/25)

[11] “Malware-Traffic-Analysis.net” http://www.malware-traffic-analysis.net/about.html (2016/7/25)

[12] 佐藤祐磨，中村嘉隆，高橋修. エクスプロイトキットで利用される文字列特徴を用いた悪性 URL 検出手法の提案. 情報処理学会研究報告, Vol.2016-CSEC-72, No.25.

[13] Adobe Systems Inc. “SWF File Format Specification (version 19)” http://www.adobe.com/devnet/swf/ (2016/7/25)