検知を目指した不正リダイレクトの分析

寺田 剛陽　　古川 忠延　　東角 芳樹　　鳥居 悟

株式会社富士通研究所 ソフトウェア＆ソリューション研究所

あらまし 本稿ではDrive by Download攻撃におけるWebページへのアクセスの遷移に着目し，そのアクセス履歴の特徴を明らかにした．Webクライアント型ハニーポット(Marionette)により収集された攻撃通信データ(D3M 2010)を元に，マルウェアホストへ不正にリダイレクトされる状況を分析した．また，危険なファイルのダウンロードに至るURL（潜在URL）の判別ロジックを機械学習の決定木学習手法を用いて抽出した結果，Webアクセス遷移の考慮が判別に有効であることが分かった．これらの分析結果は，マルウェアによる被害を事前に軽減する対策を策定するうえで非常に重要である．

Analysis of the malicious redirecting for detection

Takeaki Terada　Tadanobu Furukawa　　Yoshiki Higashikado　　Satoru Torii

Software and Solution Laboratories, Fujitsu Laboratories LTD.

Abstract By focusing on the transition of the access to the Web pages, we clarified the feature of the access history of the *Drive by Download* attack. We analyzed the situation maliciously redirected to the host by using the attack communication data (D3M 2010) collected by client honeypot (Marionette). Moreover, we derived the distinction logic by using decision tree learning. The logic shows the consideration of the Web access transition is effective for the detection of URL (potential URL) that leads to the download of a malicious file. These analysis results are very important for settling on measures to reduce the malware damage beforehand.

1　はじめに

近年のマルウェアは，その感染手口が巧妙になってきている．特に，Web ページを閲覧しただけで自動的にマルウェアがインストールされる Drive by Download 攻撃[1]が大きな脅威となっている．この攻撃は，別の Web ページに移動させる手段としてよく利用されているリダイレクト機能を悪用している．改ざんしてリダイレクトを埋め込まれた一般の Web ページへのアクセスが，悪意のあるサイトへのアクセスに自動的に切替えられて，マルウェアをダウンロードさせる．この切替えは，複数の Web ページを経由して行われることもある．

このような切替え（不正なリダイレクト）状況を明らかにすることで，マルウェアがダウンロードされる前に何らかの対処が行えると考える．

Drive by Download 攻撃における Web ページへのアクセスの遷移に着目し，そのアクセス履歴の特徴を明らかにすることが重要である．マルウェアのダウンロードに至るアクセス遷移と通常の Web アクセスとの区別を可能とすることで，将来的に，事前対処の実現が期待できる．

そこで本論文では，CCC Dataset 2010[2]に含まれている D3M 2010 の攻撃通信データを分析し，得られた不正なリダイレクトの特徴について報告する．

本分析を行うにあたり，我々は，攻撃通信データから HTTP 通信セッションを再構築し，その呼び出し関係から Web ページへのアクセス遷移を明らかにした．さらに，マルウェアのダウンロードに相当する危険なアクセスを抽出し，その HTTP リクエストに至る遷移の特徴を明らかにした．さらには，危険なアクセスの前に呼び出される URL（潜在 URL）の判別ロジックの導出を，機械学習を用いて試みた．

これらの分析結果は，マルウェアによる被害を軽減する事前の対策を策定するうえで，非常に重要である．

2　Drive by Download 攻撃

Drive by Download 攻撃は，主に Web ブラウザを通じて利用者に気づかれないように，不正なプログラムをダウンロードさせるものである．利用者が単に Web ページを閲覧しただけで，Web ブラウザやサードパーティ製アプリケーション等の脆弱性が悪用され，自動的にマルウェアがインストールされる．具体的には，(1)一般の Web ページが何らかの方法で改ざんされ，(2)ユーザが当該ページにアクセスすると，(3)そのアクセスがマルウェアをホストした悪意あるサーバに接続がリダイレクトされ，(4)マルウェアがダウンロードされ感染に至る（図 1）．

リダイレクトする手法としては，HTTP レスポンス(3xx Redirection)や，Web ページ中の iframe タグ，javascript などが使用される．特に，多重にリダイレクトされたり難読化が施されるなど，その手口が巧妙になっている．

マルウェアの感染には，Adobe Reader の脆弱性を悪用する PDF ファイルや、Flash Player の脆弱性を悪用する SWF (Small Web Format)ファイルなどが利用される．Web ブラウザの脆弱性だけでなく，アプリケーション脆弱性も悪用される．

この攻撃手法は，外部からの不正通信をブロックするファイアウォールでは防げず，組織内ネットワークのクライアント PC に感染被害を与えることが可能である．特に，2009 年末から，日本国内の著名サイトが改ざんの被害にあい，不特定多数のユーザに対して大きな感染被害を及ぼしたといわれている．

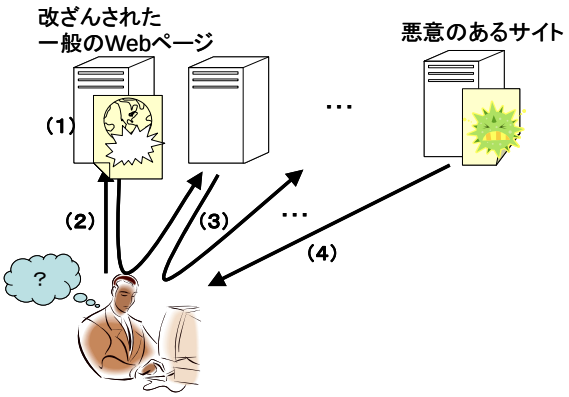

図 1：Drive by Download 攻撃

3　関連研究

Drive by Download 攻撃に関する研究としては，その攻撃手法を収集するためのハニーポット[4][5]に関するものが活発である．

検知・防御に関しては，Web サーバとの HTTP 通信の振る舞いに着目し感染したクライアントを可視化する手法[6]や，クライアント側の脆弱性をつく怪しいメッセージを遮断する手法[7]などがある．

Web ページに着目した検出手法に関しては，アンチウィルスソフトを混乱させる怪しいリンクに着目した手法[8]や，Web ページ中に埋め込まれたタグやスクリプトの特徴に基づく決定木を適用した手法[9]などがある．

いずれも怪しいメッセージや Web ページそのものを検知･防御の対象としている．本研究では，ダウンロードに至る一連の HTTP 通信の遷移に着目し，事前にダウンロードを予測し未然に対処することを目的としている．

4　アプローチ

CCC Dataset 2010 の Web 感染型マルウェアの観測データ群である D3M 2010

に含まれる攻撃通信データを分析した. これはNTT情報流通プラットフォーム研究所により作成された高対話型のWebクライアントハニーポット[5]が収集したものである.

4.1 HTTPセッションの構築

D3M 2010の攻撃通信データから，通信フローを再構築し,接続が継続する一連の通信をひとつのHTTP通信セッション（HTTPリクエスト，HTTPレスポンス）とした[10]．同一のセッションに複数のHTTPリクエストが発行されている場合は，それぞれ別の通信セッションとした．そして，各HTTP通信セッションにおける,リクエスト行やステータス行の文字列,パケット数，通信量などを抽出した.

4.2 アクセス遷移の抽出

提供されたD3M 2010には，アクセスしただけで攻撃を受けるURLの一覧(巡回対象URL)が含まれている. この巡回対象URLのエントリを開始点とする一連のやりとりがDrive by Download攻撃であるとみなせる.

そこで，再構築したHTTP通信セッションを,ハニーポット毎に(発信元IPアドレス毎に)整理し，巡回対象URLのエントリから始まる一連のリクエストをひとつのリクエストグループとした.

4.2.1 親リクエストとの関連付け

一般に,ひとつのWebページには画像など複数のリンクが張られており,アクセスすると一度に多数のリクエストが発生する．通信が発生した時間ごとにHTTP通信セッションを並べただけでは，どのWebページから発生したものか判断がつかない.

そこで，Webページのアクセス遷移を抽出するため，応答メッセージ（HTTPレスポンス）群を解析し，呼び出し元である親リクエストを探索しその関連を明らかにした. 親リクエストの応答メッセージの記載形態に応じて,親リクエストとの関連を以下の6つのパターンに分類した(表1)．“Referrerヘッダ”に呼び出し元（親リクエスト）のURLが記載されている場合があるが,呼出し形態の差異を見るため,ここでは使用しなかった.

表1：親リクエストとの関連

分類名	概要
[0]	巡回URLリストに記載
[Location]	HTTPレスポンスのステータスが3XX Redirectionで，Locationヘッダに記載
[Url In Data]	HTTPレスポンスにURL文字列が記載
[Path In Data]	親リクエストと同じホストで，かつ，親リクエストのレスポンスデータにPATH文字列が存在
[Equal Host]	親リクエストと同じホスト
[-1]	親リクエストが見つからなかった

親リクエストとの照合には，応答メッセージに記載されているドメイン名とIPアドレスとの照合が必要である. 攻撃通信データ(pcap)内のDNS通信ログから名前解決の状況を取得し[11],ドメイン名とIPアドレスの対応表を作成し,その結果を元に照合した. 複数の異なるドメイン名が同じIPアドレスを持つ場合，および，ひとつのドメイン名が複数のIPアドレスを持つ場合がある．対応表は，これらの点を配慮して,複数のエントリが記載されている.

4.2.2 危険なレスポンスの抽出

分析に使用した攻撃通信データからは，どのHTTPレスポンスにどのようなマルウェアが含まれていたかは判断できない．一般に，Adobe Readerの脆弱性を悪用するPDFファイルや、Flash Playerの脆弱性を悪用するSWF(Small Web Format)ファイルなどがダウンロードされると言われている.

そこで，PDFファイル，SWFファイル，バイナリファイルの3種類のダウンロードが危険であると判断し，HTTPレスポンスのContent-Typeヘッダを参照し危険なレスポンスを特定した（表2）.

表 2 ： 危険なレスポンス

ファイル	Content-Type
PDF	application/pdf
SWF	application/x-shockwave-flash
BIN	application/octet-stream
	application/x-msdownload
	application/x-download
	application/x-msdos-program

4.3 アクセス遷移グラフの作成

Web ページのアクセス状態を可視化する遷移グラフを作成した. これにより危険なレスポンス(PDF ファイル，SWF ファイル，バイナリファイル)がどのようなリクエストを経由して行われるかが明らかにできる.

Web ページをノード（ネットワーク要素）とし，呼び出し元である親リクエストとの関連をエッジ(ノード間をつなぐリンク）として，Web ページのアクセス状況の遷移をネットワークとして可視化した.

4.4 機械学習による危険 URL 予測

機械学習により，危険ファイルをダウンロードさせるセッションを判別するロジックの導出を試みた. このような判別が可能であれば, マルウェアをダウンロードさせるセッションを事前に予測し, 回避することが可能である. 巡回対象 URL からどのような関係にあるリクエストが危険かを把握するため、親リクエストの照合ができなかったリクエストは対象外とした.

5 分析結果

5.1 親リクエストとの関連

再構築した HTTP 通信セッションの内訳を，表 3，表 4 に示す.

巡回対象 URL に記載されているリクエストは 507 個であり，すべてのエントリ(557 個)への通信は発行されていなかった. これは，DNS 名前解決が失敗し IP アドレスが取得できなかったなど, 種々のエラーが発生したためと考えられる.

表3: HTTPリクエストの内訳

リクエスト数	
[0]	507
[Location]	199
[URL in data]	737
[PATH in data]	1,407
[Equal Host]	3,296
[-1]	224
合計	6,370

表4: HTTPレスポンスの内訳

レスポンス数		
2xx Success		
	200 OK	5,397
	その他	58
3xx Redirection		303
4xx Client Error		173
5xx Server Error		29
合計		5,960

親リクエストが照合できなかったもの(224 個)は，javascript などを用いて動的にアクセス先の URL が指定されたものと考えられる. Equal Host の件数が多いことも同じ理由と考えられる. 一方，HTTP レスポンスの Redirection によるリクエスト(199 個)は全体と比べて少なかった.

リクエストとレスポンスとの差分は応答が返ってこなかったものである. エラー(4xx, 5xx)のレスポンスを含め，全リクエストの 10%ほどがエラーとなっている.

表 5 : リクエスト種類と危険レスポンスの関係

	総数	レスポンス		
		pdf	swf	bin
Location	199	0	0	0
		0.00%	0.00%	0.00%
Url In Data	737	13	8	40
		1.76%	1.09%	5.43%
Path In Data	1407	0	8	44
		0.00%	0.57%	3.13%
Equal Host	3296	183	88	521
		5.55%	2.67%	15.81%
other	731	79	1	8
		10.81%	0.14%	1.09%
総数	6370	275	105	613

5.2 危険なレスポンス

リクエストの種類と危険なレスポンスの関係を表 5 に示す. 各セルはリクエストの種類ごとの各危険レスポンスの回数, 下段は各リクエスト総数に対するその割合である. リダイレクトによるリクエストでは危険なレスポンスはなく，Equal Host によるリクエストの多くに危険なレスポンスが含まれていることが分かる. Url In Data や Path In Data と異なり Equal Host ではリクエスト元に飛び先の

文字列が含まれておらず, より不明度の高いリクエストに危険なレスポンスがある可能性が高いことを示している.

5.3 アクセス遷移グラフ

全てのリクエストを合わせた URL 間遷移グラフを図 2 に示す. 図からは以下のことが読み取れる. まず, 巡回対象 URL のノード（図中 1）からの遷移において, 1 ホップの辺りに PDF が多い. また, 1, 2 ホップ目のノードが多くのセッションを張っており, 2, 3 ホップ目に各種危険ファイルが出現している. 一方, 親が不明なノード（図中 2）からの遷移では, 2 ホップ目の辺りに PDF やバイナリファイルが多く存在している. 巡回対象 URL のノードと親が不明なノードのどちらからも, 4 ホップ以上では危険なファイルのダウンロードは少ないが, 大量の危険なファイルをダウンロードするノードも存在している.

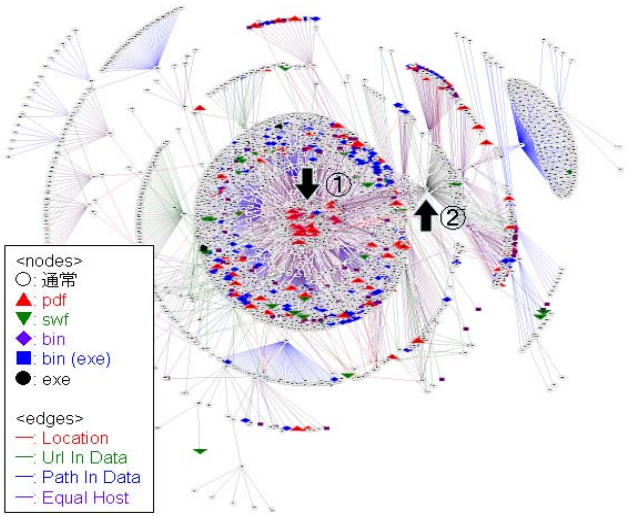

図 2 : URL 間遷移のグラフ

5.4 危険 URL 予測

危険ファイルのダウンロードする前に危険な URL を予測することを, 決定木学習手法 C4.5[12]を用いて行った. これは, ある URL U1 から URL U2 に対するリクエストがあったとき, U2 が次に危険ファイルに対してリクエストを出す URL（潜在 URL）かどうかを判別するものである.

前節の遷移グラフより, 他のノードとのつながりが判別に有効であると考え、表 6 に示す素性を用意した（但し、危険ファイルは自身がリクエストを出すことはないため, mySess は除外した 12 個）. 三日分の観測データのうち, 3 月 8 日分のデータを教師データ, 3 月 9 日, 11 日分のデータをテストデータとした.

表 6 ： 学習に用いた組成

つながりに基づく素性	
	巡回対象URLからU2までの距離len
	U1からU2へのリクエスト種類curPath
	U1の出すリクエスト数parSess
	U2の出すリクエスト数mySess
	巡回URLからU2までの経路におけるリクエスト種類ごとの出現回数parPat0～4
通信量に基づく素性	
	送信元パケット数srcPack
	送信先パケット数dstPack
	送信元データ量ulSize
	送信先データ量dlSize

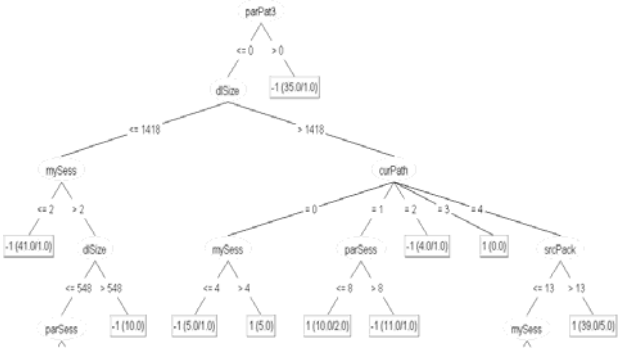

図 3; 潜在 URL を判別する決定木

生成された決定木を図 3 に示す. 決定木では, 判別に効果の大きな素性ほど上位に位置する. もっとも有効な素性が parPat3 (U2 までに出現している Equal Host 数) であり, テストデータへの適用においては, 一度以上出現（右の分岐）してれば, 34/35 の確率で安全（-1 ; 危険な場合は 1 と表記) であることを示している. このモデルにおいて, 潜在 URL を正しく判別した正解率は 85.1% (395/464), 潜在 URL をそうでないと判別する確率(false negative, FN)は 12.3%(26/212), 潜在 URL でないものを間違えて判別する確率(false positive, FP)は 17.1%(43/252)であ

った. 比較対象として, つながりに基づく素性を除き, 送信元/先パケット数・送信元/先データ量のみを用いた予測では, 正解率は 74.1%, FN が 39.2%, FP が 14.7%であり, つながりに基づく素性が精度の向上に貢献していることが分かる. すなわち, 潜在 URL の判別においては, つながりに基づく素性が有効であることが分かった.

6 まとめ

本研究では, Web クライアントハニーポットにより得られた Web 感染型マルウェアの観測データ群(D3M 2010)を分析し, Drive by Download 攻撃における Web ページアクセス遷移の特徴を明らかにした.

この結果, (1)Web ページ切替えに使用された手法にて, HTTP レスポンスの Redirection が全体としては少ないこと, (2)呼び出し元の HTTP レスポンスには明記されていない URL へのアクセスが, マルウェアのダウンロードである可能性が高いこと, (3)PDF ファイルは巡回対象 URL から短い遷移でダウンロードされるが, SWF ファイルやバイナリファイルのダウンロードは少し長めの遷移であること, などが明らかになった.

さらに, 危険なファイルのダウンロードに至る URL (潜在 URL)の判別ロジックを, 機械学習の決定木学習手法を用いて抽出した. その結果, 潜在 URL 判別の正解率が 85.1%となる判別モデルが導出でき, Web アクセス遷移の考慮が判別に有効であることが明らかとなった.

これらの特徴を活用することで, マルウェアのダウンロードの発生が予測でき, 感染を未然に対処することが期待できる.

謝辞:本研究で使用した分析ツールの構築に協力頂いた株式会社富士通ソーシャルサイエンスラボラトリ清水聡氏に感謝する.

参考文献

[1] Harley, D. et al. *"Drive-by downloads from the trenches,"* MALWARE 2008.

[2] 畑田充弘, 他 *"マルウェア対策のための研究用データセット ～MWS 2010 Datasets～,"* MWS2010

[3] 独立行政法人 情報処理推進機構 *"5 Web 媒介型攻撃 Gumblar の動向調査,"* 情報セキュリティ技術動向調査(2009 年下期)

[4] Christian Seifert, et al. "*Taxonomy of Honeypots,"* Technical Report CS-TR-06-12, Victoria University of Wellington

[5] Mitsuaki Akiyama, et al. *"Design and Implementation of High Interaction Client Honeypot for Drive-by-download Attacks,"* IEICE Transactions on Communication, Vol.E93-B No.5

[6] 金子博一, 他 *"通信トラフィックの分析による Gumblar 感染 PC の可視化 ,"* 信学技報, vol. 110, no. 79, ICSS2010-1

[7] Thijs Kinkhorst et al. *"Detecting the ghost in the browser: Real time detection of drive-by infections"* https://www.os3.nl/_media/2008-2009/courses/rp2/uva_sne_detecting_the_ghost_in_the_browser_kinkhorst_van_kleij_rp2.pdf

[8] Chia-Mei Chen et al. *"Anomaly Behavior Analysis for Web Page Inspection,"* NETCOM '09.

[9] Christian Seifert et al. *"Identification of Malicious Web Pages with Static Heuristics,"* ATNAC 2008.

[10] 鳥居悟, 他 *"不適切なHTTPトンネリング通信を検出する手法の提案,"* 情報処理学会研究報告 2009-CSEC-46(15)

[11] 東角芳樹, 他 *"DNS通信の挙動からみたボット感染検知方式の検討,"* MWS2008

[12] Quinlan, J. R. 1993. *"C4.5: Programs for Machine Learning,"* California: Morgan Kaufmann.