Computer Security Symposium 2017
23 - 25 October 2017

Exploit Kit で構築された悪性 Web サイトの URL に関する考察

西尾 祐哉[*] 廣友 雅徳[*] 神薗 雅紀[†] 福田 洋治[‡] 毛利 公美[§] 白石 善明[**]

概要：近年，Web ブラウザやプラグインの脆弱性を悪用した攻撃を行い，ユーザに気付かれずにマルウェアに感染させる Drive-by Download 攻撃が猛威を振るっている．その要因として，悪性 Web サイトを容易に構築できる Exploit Kit が流通していることが挙げられる．しかし，Exploit Kit の利用者側は容易にコードを改変することができないため，Exploit Kit で構築された悪性 Web サイトには何らかの特徴が現れることが指摘されている．そこで本稿では，Exploit Kit で構築された悪性 Web サイトの URL に現れる特徴に関して述べる．

キーワード：Drive-by Download 攻撃，Exploit Kit，悪性 Web サイト，Neutrino Exploit Kit，Rig Exploit Kit

A Study on URL of Malicious Websites Built by Exploit Kit

Yuya Nishio[*] Masanori Hirotomo[*] Masaki Kamizono[†]
Youji Fukuta[‡] Masami Mohri[§] Yoshiaki Shiraishi[**]

Abstract: Recently, Drive-by Download attack which exploits vulnerability in web browser or plug-in are prevalent. This is because attackers utilize Exploit Kit which makes it easy to build malicious websites. However, users of exploit kit cannot easily modify their code. Therefore, malicious web sites built by exploit kit have some features. In this paper, we consider characteristics of URL appearing on malicious websites built by exploit kit.

Keywords: Drive-by Download Attack, Exploit Kit, Malicious Website, Neutrino Exploit Kit, Rig Exploit Kit

1. まえがき

近年，クライアント PC を狙った攻撃が世界中で発生しており，特に悪性な Web サイトを閲覧したユーザに強制的にマルウェアをダウンロードさせる Drive-by Download（DBD）攻撃が猛威を振るっている．DBD 攻撃とは，攻撃者の用意した悪性 Web サイトにユーザを誘導し，ブラウザやプラグインの脆弱性を悪用してマルウェアに感染させる攻撃である．悪性 Web サイトの構築や，脆弱性を突く攻撃を行うために Exploit Kit と呼ばれるツールキットが利用されている．Exploit Kit はブラックマーケットで売買されており，攻撃者に専門的な知識がなくとも容易に攻撃を仕掛けることができるため，DBD 攻撃の被害が絶えない要因となっている．

現在の DBD 攻撃の対策として，ユーザの悪性 Web サイトへのアクセスを防ぐために，Microsoft や Google が提供している URL ブラックリストを用いたアクセスブロック機能が存在している[1][2]．しかし，攻撃者によって正規サイトが改ざんされ，悪性 Web サイトにリダイレクトさせるコードが埋め込まれることがあることと，悪性 Web サイトの多くはその URL を短期間で遷移させていることから，ブラックリスト方式による防御には限界がある．

Exploit Kit を利用すれば容易に DBD 攻撃を仕掛けることができる反面，各 Exploit Kit に応じた特徴が悪性 Web サイトの URL や JavaScript などに現れると指摘されている[3]．そのため，各 Exploit Kit に現れる特徴を把握し，それをシグネチャとして利用することで，URL のブラックリスト方式よりも効果的な防御ができると考えられる．

本稿では，Exploit Kit で構築された悪性 Web サイトの URL に現れる特徴に関する考察を述べる．様々な Exploit Kit による URL の特徴を把握することができれば，シグネチャとして活用するだけではなく，使用された Exploit Kit の種類を識別できるようになり，DBD 攻撃を解析する際に悪用された脆弱性を推測できるなど，攻撃の全体把握が容易になると考えられる．

2. 関連研究

Exploit Kit で構築された悪性 Web サイトの URL に着目した DBD 攻撃の検知手法はいくつも提案されている．笠間ら[3]は主に Blackhole Exploit Kit や Elenore Exploit Pack などで使用される URL の特徴を正規表現で表し，それを検知ルールとした．柴原ら[4]はサンドボックス内に Exploit Kit を使用した悪性 Web サイトを構築し，そこに繰り返しアクセスすることで URL やリダイレクトのパターンを収

* 佐賀大学大学院工学系研究科
Graduate school of Science and Engineering, Saga University
† PwC サイバーサービス合同会社
PwC Cyber Services LLC.
‡ 近畿大学理工学部情報学科
Faculty of Science and Engineering, Kindai University
§ 岐阜大学大学院工学研究科
Graduate School of Engineering, Gifu University
** 神戸大学大学院工学研究科
Graduate School of Engineering, Kobe University

集し，Exploit Kit 検知用シグネチャを自動作成する手法を提案した．この手法はインターネット上に実在する悪性 Web サイトのうち，Exploit Kit を所持していないサイトには対応できない．永井ら[5]は悪性 Web サイトの URL に構造的な特徴があることに着目し，サイト構造のクラスタリングを行うことで Exploit Kit を識別する手法を提案している．

悪性 Web サイトの URL 以外に着目した DBD 攻撃の検知手法として，酒井ら[6]は HTTP ヘッダ情報の特徴を利用した検知手法を提案している．この手法では，PHP のバージョン情報を表す X-Powered-By ヘッダとコンテンツタイプヘッダ，データヘッダの 3 種類のレスポンスヘッダを特徴として利用している．Stock ら[7]は悪性 Web サイト内の JavaScript に着目しており，JavaScript コードを抽象化してクラスタリングを行い，各 Exploit Kit のシグネチャを生成する手法を提案している．

3. Drive-by Download 攻撃

3.1 Drive-by Download 攻撃の概要

Drive-by Download（DBD）攻撃とは，ユーザが悪性な Web サイトにアクセスすると，複数回のリダイレクトを経てマルウェア配布サイトへ誘導され，ブラウザやプラグインの脆弱性が悪用されて強制的にマルウェアがダウンロードされる攻撃である．従来のインターネットでの攻撃手法では，攻撃者が攻撃対象者に悪意のある情報を送る能動的攻撃であった．それに対して DBD 攻撃は，ユーザの Web サイトへのアクセスを攻撃の起点とし，攻撃者が攻撃対象者からの要求を受けて悪意のある情報を応答するため，受動的攻撃に分類される．図 1 は DBD 攻撃の流れを示している．

攻撃に関与する Web サイトは，入口サイト，中継サイト，攻撃サイト，マルウェア配布サイトの 4 つからなり，それぞれの役割は次のようになる．

[入口サイト]

攻撃の起点となるサイト．アクセスすると，中継サイトへリダイレクトさせる．攻撃者が作成したサイトとは限らず，正規サイトを改ざんして入口サイトとすることが多い．

[中継サイト]

攻撃サイトへの中継を行うサイト．複数の中継サイトを経由する場合もある．

[攻撃サイト]

クライアント PC の OS や Web ブラウザ，Web ブラウザ上で動作するプラグインの脆弱性を悪用し，マルウェア配布サイトからマルウェアをダウンロードするスクリプトを実行させる．

[マルウェア配布サイト]

攻撃サイトによって乗っ取られたクライアント PC のリクエストに応えてマルウェアを送信し，強制的に実行させることでマルウェアに感染させる．

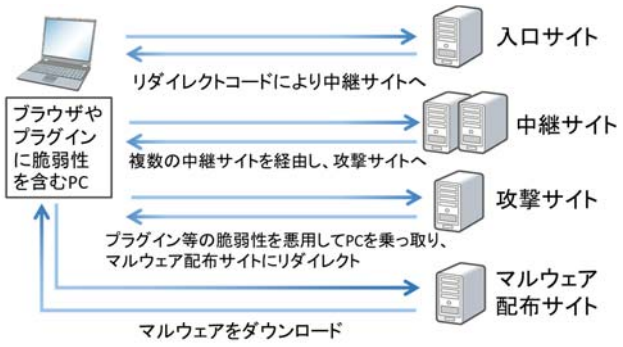

図 1　Drive-by Download 攻撃の流れ

DBD 攻撃は上記の複数の Web サイトが連動して行われるが，ダウンロード画面やインストール画面，リダイレクト時の画面変化等は表示されないため，ユーザは攻撃を受けたことに気付くことができない．入口サイトは，正規サイトを改ざんして iframe タグを挿入し，外部の悪性サイトにアクセスさせていることが多い．この iframe のフレームサイズを小さく設定することで，表示されている悪性サイトを視覚的に見えなくしている．

3.2 Exploit Kit

Exploit Kit とは，DBD 攻撃に利用する Web サイトの構築や，Adobe Flash Player，Java Runtime Environment などのプラグイン，各種 Web ブラウザ等の脆弱性を突く攻撃を容易に行うツールキットである．図 1 の中継サイト，攻撃サイト，マルウェア配布サイトは Exploit Kit によって構築される．それらの悪性 Web サイトの URL は短時間で変化し，サーバの IP アドレスも数時間程度で変化する．また，Exploit Kit には解析妨害機能が備わっており，User-Agent などによってユーザ環境を識別し，攻撃対象となる環境の場合だけ攻撃を実行する．さらに一度訪問したユーザの IP アドレスを記録し，二度目以降のアクセスをブロックする機能もある．

Kotov ら[8]は，30 種類以上の Exploit Kit のソースコードを解析し，Exploit Kit が保有する機能について報告している．その報告によると，Exploit Kit のソースコードは Zend Guard や ionCube によって暗号化されており，Exploit Kit 利用者がコードの改変をできないようにしている．そのため，同一の Exploit Kit によって構築された Web サイトには何らかの類似性があると考えられる．

4. 悪性 Web サイト URL の特徴と調査

4.1 既に報告されている Exploit Kit の特徴

Blackhole Exploit Kit の解析レポート[9]によると，Blackhole Exploit Kit の URL にはいくつかの特徴がある．例えば，脆弱性を悪用する際にダウンロードされる PDF フ

ファイルの URL は以下の 3 パターンである．

- [ドメイン名]/content/ap1.php?f=b6863
- [ドメイン名]/content/ap2.php?f=b6863
- [ドメイン名]/content/fdp2.php?f=50

また，Rig Exploit Kit について解析したレポート[10]によると，Rig Exploit Kit の URL は 3 パターン存在する．具体的には以下の 3 パターンの何れかが，URL パラメータの値に固定文字列として含まれている．

- QMvXcV
- WrwE0q
- fPrfJxzFGMSUb-nJDa9

このように，Exploit Kit が使用されている URL には何らかの特徴が現れ，その特徴は Exploit Kit の種類毎に異なると考えられる．本研究では，様々な Exploit Kit の URL に現れる特徴を把握し，その特徴を基に Exploit Kit の判別をすることを目的とする．

4.2 調査対象データ

本調査では，DBD 攻撃などのサイバー攻撃に関する解析レポートを提供している BroadAnalysis[11] から取得した PCAP ファイルを利用する．また本調査では，2016 年の 5 月から同年 9 月までの期間に流行した Neutrino Exploit Kit と，2016 年 9 月以降に流行している Rig Exploit Kit を調査対象とした．

4.3 Neutrino Exploit Kit の調査結果

2016 年 5 月 2 日から 2016 年 9 月 12 日までの期間に投稿された Neutrino Exploit Kit の解析レポートの中から，41 個の PCAP ファイルを解析した結果について述べる．

Neutrino Exploit Kit の攻撃の流れを図 2 に示す．入口サイトは正規サイトを改ざんしたものと思われ，入口サイト内に挿入された iframe タグによって攻撃サイトへリダイレクトされる．攻撃サイトでは SWF ファイルをダウンロードさせ，Adobe Flash Player に存在する脆弱性を悪用すると見受けられる．その後，攻撃成功の合図と考えられる空の HTML ファイルを要求し，ファイル形式不明の暗号化されたマルウェアをダウンロードさせる．攻撃サイト，SWF ファイル, 空ファイル, マルウェアの URL を解析したところ，Neutrino Exploit Kit の URL は次の 4 パターンに分けられる．

[パターン 1]

/英単語/ランダム文字列

（例）foot/Ynpka3Bvaw

[パターン 2]

/英単語/（英単語 1 個から 3 個）-（8 桁の数値）

（例）unhappy/adult-enjoy-forty-24625294

[パターン 3]

/英単語/7 桁の数値/（英単語 3 個以上）

（例）kiss/1504132/pattern-dusty-form-somewhere-sigh
-watson-place-home-attitude

[パターン 4]

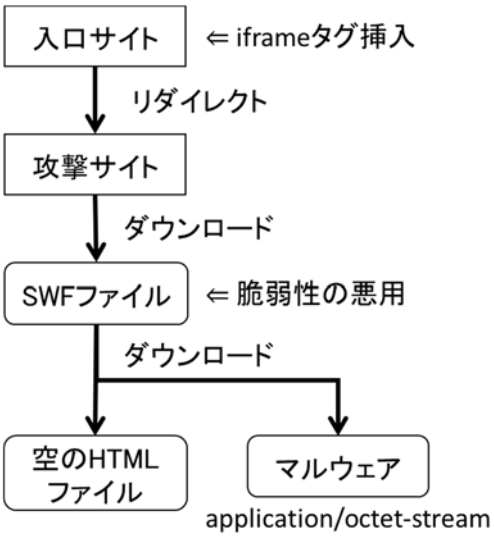

図 2　Neutrino Exploit Kit による攻撃の流れ

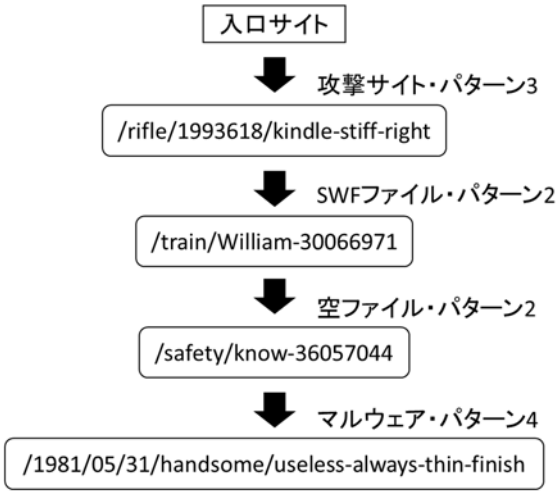

図 3　Neutrino Exploit Kit の URL 遷移例

/年/月/日/(英単語 1 個から 3 個)/（英単語 3 個以上）

（例）1997/02/25/possess/feeble/drift/country-path-want-duke
-fold-wear-power-goblin

実際の URL 遷移の例を図 3 に示す．Neutrino Exploit Kit の各 URL は例外なく上記の何れかの形式をしており, どの URL にどのパターンが使われるかはランダムである．なお, 一連の攻撃動作内のドメイン名は同じであるが，各 PCAP ファイルによってドメイン名は異なっている．

4.4 Rig Exploit Kit の調査結果

Rig Exploit Kit の攻撃パターンには，URL に固定文字列が存在するパターンと, 不定期に URL の特徴を変化させるパターンの 2 種類に分けられる．本稿では，URL に固定文字列が存在するパターンのみ解析した結果を示す．BroadAnalysis に掲載されている Rig Exploit Kit の解析レポートは 2016 年 5 月から 2017 年 5 月まであり，その内 URL に固定文字列が存在するパターンは 2016 年 5 月 14 日から

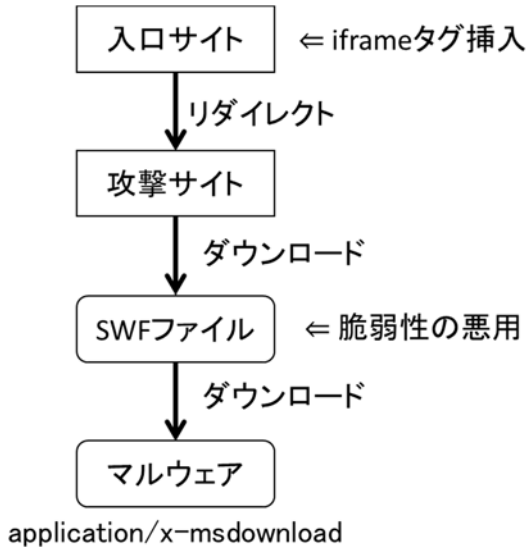

図 4　Rig Exploit Kit による攻撃の流れ

同年 12 月 20 日までの期間に確認できた．その中から 30 個の PCAP ファイルを解析した結果を述べる．

Rig Exploit Kit の URL に固定文字列が存在するパターンの攻撃の流れを図 4 に示す．大まかな流れは Neutrino Exploit Kit と同様であるが，脆弱性を悪用した後にダウンロードさせるファイルの MIME タイプは application/x-msdownload である．攻撃サイト，SWF ファイル，マルウェアの URL を解析したところ，次の 4 個の特徴を見つけた．

[特徴 1]URL の形式は固定

攻撃サイト：ドメイン名/?変数名=値

SWF，マルウェア：ドメイン名/index.php?変数名=値

[特徴 2]URL パラメータの変数名は 15 文字

（例）xXqAdLSbLRzODIo=（値）

xniKfreVKRbJDYA=（値）

[特徴 3]パラメータ値の先頭から 23 文字は固定文字列

攻撃サイト：l3SKfPrfJxzFGMSUb-nJDa9

SWF，マルウェア：l3SMfPrfJxzFGMSUb-nJDa9

この 2 つの違いは，4 文字目が「K」か「M」かである．5 文字目以降の固定文字列は，4.1 節で述べた Rig Exploit Kit の 3 番目の URL パターンと一致する．

[特徴 4]一連の攻撃内ではパラメータ値がほぼ同じ

（例）攻撃サイト：l3SK ～ QFFd

SWF，マルウェア：l3SM ～ QFF6w…

攻撃サイトのパラメータ値の 5 文字目から末尾の 2 文字目か 3 文字目までの文字列と，SWF，マルウェアのパラメータ値の 5 文字目以降は一致する．

実際の URL 遷移の例を図 5 に示す. 一連の攻撃内でドメイン名と URL パラメータの変数名が変わることはないが，PCAP ファイル毎にそれらの値は異なっている．また，上記の特徴とは別に，マルウェアをダウンロードする際の URL にパラメータの変数が 1 つ追加されている場合があり，それは期間によって変化していた．追加されるパラメータの変数名は必ず drgsdf で, 値は 1 桁から 4 桁の数値になる．例えば「drgsdf=29」などのパラメータが追加される．参考までに，実際に確認できた期間における変数の数の変化を表 1 に示す.

図 5　Rig Exploit Kit の URL 遷移例

表 1　マルウェアダウンロード時の URL パラメータの変数の数

期間（2016 年）	変数の数
5/14 – 9/19	2 個
9/20 – 10/1	1 個
10/3 – 10/5	2 個
10/9 – 10/21	1 個
10/22 – 11/10	2 個
11/28 – 12/20	1 個

5. Exploit Kit の識別に関する考察

4 章の調査結果を踏まえて，URL による Exploit Kit の識別ルールについて考察する．

Neutrino Exploit Kit については，URL が 4.3 節で述べた 4 パターンの何れかに一致するかを判定する．ただし，攻撃サイトの URL だけで判断すると, 誤った識別をする可能性が高いため，SWF ファイル，空ファイル，マルウェアのダウンロード元 URL まで確認して判定する方が確実である．

Rig Exploit Kit については，4.4 節で述べた特徴 2 と特徴 3 を利用することで識別できる．つまり，URL パラメータの変数名が 15 文字かつ, パラメータの値に特徴 3 の固定文字列が存在することが識別ルールになる. また, Rig Exploit Kit の場合は，固定文字列が長いため，攻撃サイトの URL だけで判定することが可能だと考える．より正確に識別をするのであれば，特徴 1 や特徴 4 を識別ルールに適用し，

SWF ファイルとマルウェアのダウンロード元 URL まで確認すると良い.

6. まとめ

本稿では，URL に着目して Exploit Kit の識別をするために，Neutrino Exploit Kit と Rig Exploit Kit の URL に現れる特徴について調査した. 調査の結果, この 2 つの Exploit Kit の URL にはそれぞれ異なる特徴が現れ，その特徴を基に Exploit Kit の識別ができると思われる．URL の特徴だけで Exploit Kit を識別することができれば，DBD 攻撃の解析をする際に，悪用された可能性の高い脆弱性を絞ることができ, 攻撃の全体把握が容易になると考えられる. また, URL の特徴をシグネチャとして活用すれば，ブラックリスト形式で悪性 Web サイトへのアクセスを防御するよりも効果的であると考えられる.

本稿では 2 種類の Exploit Kit を調査したが，より多くの種類の Exploit Kit について調査した後に，URL に着目した Exploit Kit の識別を行うことが今後の課題である．また，Rig Exploit Kit の URL に固定文字列が現れるパターンのみの解析に留まっているため，今後はもう 1 つの不定期に URL の特徴を変えるパターンの解析も行い，その解析結果と合わせて Rig Exploit Kit の特徴とする予定である.

参考文献

[1] Microsoft,“SmartScreen フィルター機能,” https://support.microsoft.com/ja-jp/help/17443/windowsinternet-explorer-smartscreen-filter-faq,（参照 2017-08-28).

[2] Google,“Google Safe Browsing,” https://developers.google.com/safe-browsing/,（参照 2017-08-28).

[3] 笠間貴弘，神薗雅紀，井上大介，“Exploit Kit の特徴を用いた悪性 Web サイト検知手法の提案,” コンピュータセキュリティシンポジウム 2013（CSS2013），2013.

[4] 柴原健一，笠間貴弘，神薗雅紀，吉岡克成，松本勉，“Exploit Kit 検知用シグネチャの動的解析に基づく自動作成,” 研究報告コンピュータセキュリティ（CSEC），Vol. 2014-CSEC-64，No. 35，pp. 1-7，2014.

[5] 永井達也，神薗雅紀，白石善明，毛利公美，高野泰洋，森井昌克,“サイト構造のクラスタリングを用いた悪性サイトの識別,” 信学技報，ICSS2017-19，pp. 93-98，July 2017.

[6] 酒井裕亮，佐々木良一，“Drive By Download 攻撃に対する HTTP ヘッダ情報に基づく検知手法の提案,” 研究報告コンピュータセキュリティ（CSEC），Vol. 2013-CSEC-60，No. 29，pp. 1-6，2013.

[7] B. Stock, B. Livshits, B. Zorn, “Kizzle: A Signature Compiler for Exploit Kits,” 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016.

[8] V. Kotov, F. Massacci, “Anatomy of Exploit Kits,” International Symposium on Engineering Secure Software and Systems，2013.

[9] F. Howard,“Exploring the Blackhole exploit kit - Naked Security,” https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit/,（参照 2017-8-28）.

[10] 株式会社ラック,“CYBER GRID VIEW Vol.3,”https://www.lac.co.jp/lacwatch/report/20170202_001203.html,（参照 2017-8-28）

[11] “BroadAnalysis,” http://www.broadanalysis.com/,（参照 2017-8-28）