EISS-2019企业信息安全峰会

北京站/3.29

业务安全红蓝对抗的探索与实践

柳兮 2019.3.29

归零实验室-简介

- 柳兮-阿里安全归零实验室

- 归零实验室简介

阿里安全归零实验室成立于2017年11月，实验室致力于对黑灰产技术的研究,愿景通过技术手段解决当前日益严重的网络违规和网络犯罪问题，为阿里新经济体保驾护航。

目前团队也在不断的招聘各种优秀人才，研发专家、数据分析专家、情报分析与体系化专家等，欢迎加盟，联系邮箱 back2zero@service.alibaba.com

阿里安全

备注说明

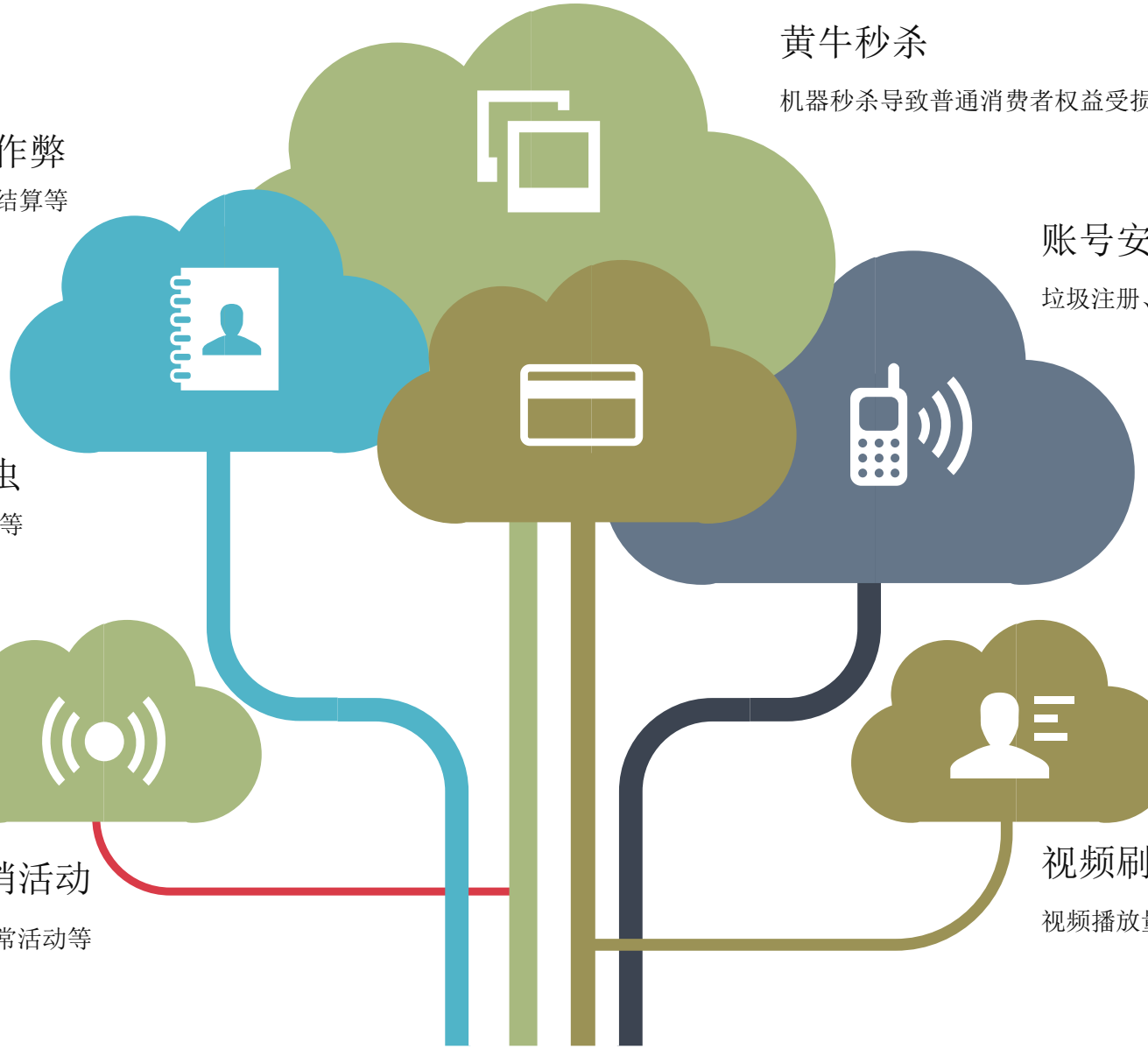
阅读PPT前，建议先阅读FIT 2019
议题《如何做好业务安全红蓝对抗》

主要内容

- 常见的业务风险和风控体系
- 业务红蓝对抗的探索实践过程
- 砺剑蓝军演练平台

01 常见的业务风险和风控体系

常见的业务风险



黄牛秒杀

机器秒杀导致普通消费者权益受损等

广告流量作弊

CPM、CPC结算等

账号安全

垃圾注册、扫号撞库等

业务爬虫

敏感数据的爬取等

直播风险

淘宝直播、短视频等

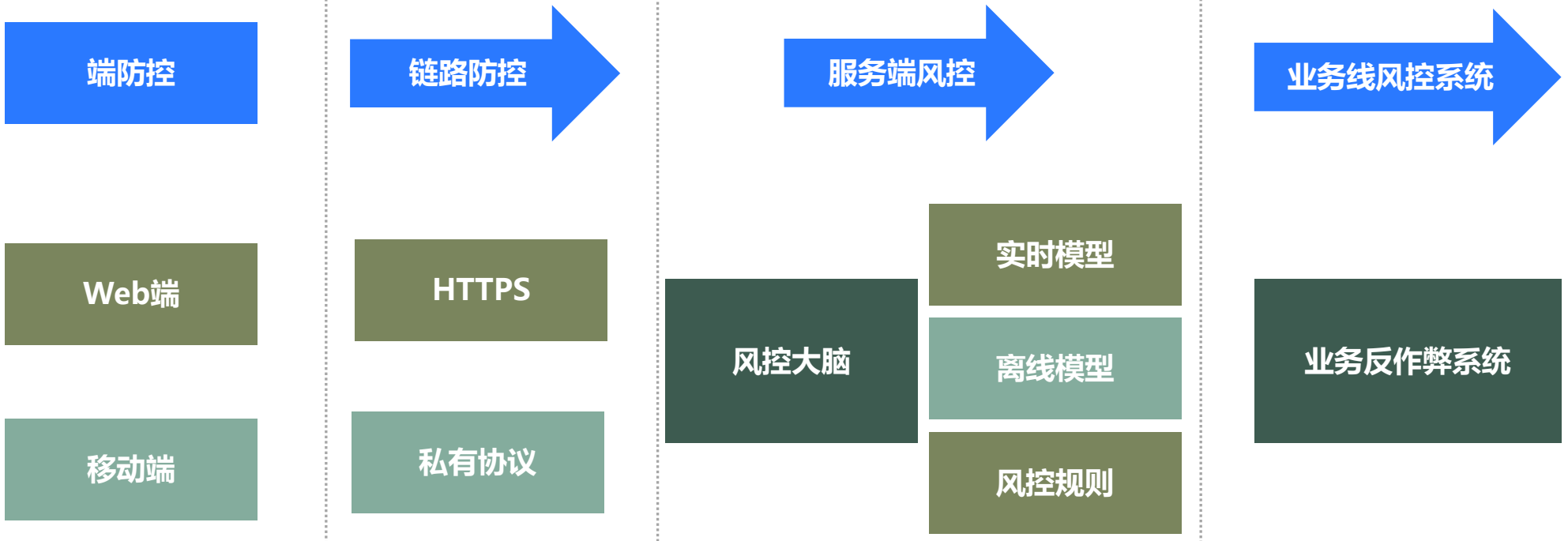
营销活动

拉新活动、日常活动等

视频刷量

视频播放量、时长作弊等

常见的风控体系


端防控
链路防控
服务端风控
业务线风控系统
Web端
移动端
HTTPS
私有协议
风控大脑
实时模型
离线模型
风控规则
业务反作弊系统

02 业务红蓝对抗的探索实践过程

难点和解法

同时支持多种业务风险场景

- **风控对抗技术能力抽象**
- **安全技术破解能力抽象**
- **海量资源的管理**

…

缺乏成熟的体系流程

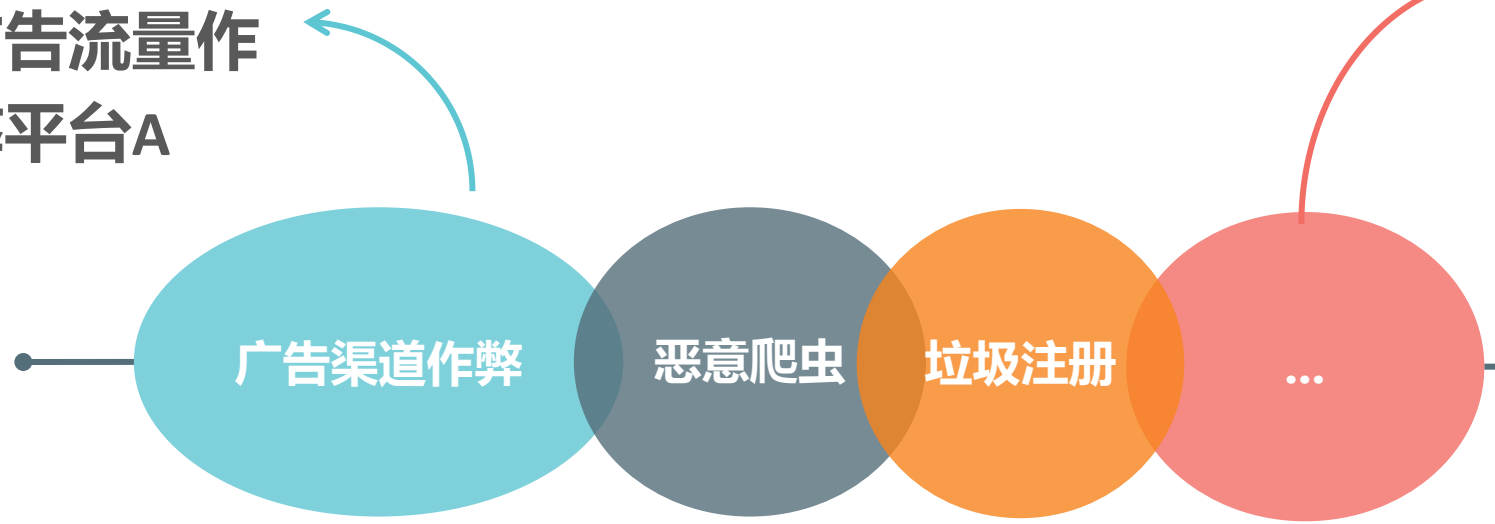
- 逐步沉淀体系、流程、打法等
- …

演练和真实攻击的差异

- 结合情报覆盖更完整的攻击路径
- 开发演练平台，通过平台放大能力，攻击体量等
- 线上攻击的频率、量级等
- …

持续迭代和升级

探索实践过程-业务风险场景能力抽象



广告流量作弊平台A

恶意爬虫软件B

账号注册助手软件C

能力抽取

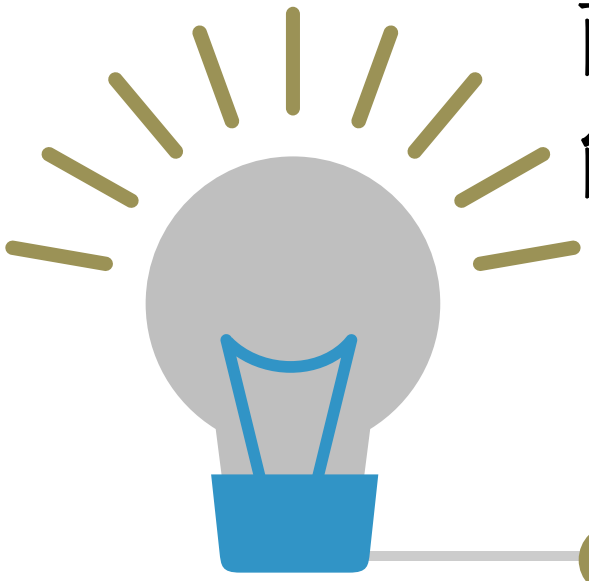
- **资源：**代理IP、手机黑卡（接码平台）、机器等；
- **安全&风控对抗：**

Web端：JavaScript反混淆；

移动端：Android 脱壳、iOS逆向； Root&越狱检测等；

端通用能力：各类验证码识别；反调试、反注入、hook检测、运行环境检测等。。。

探索实践过程

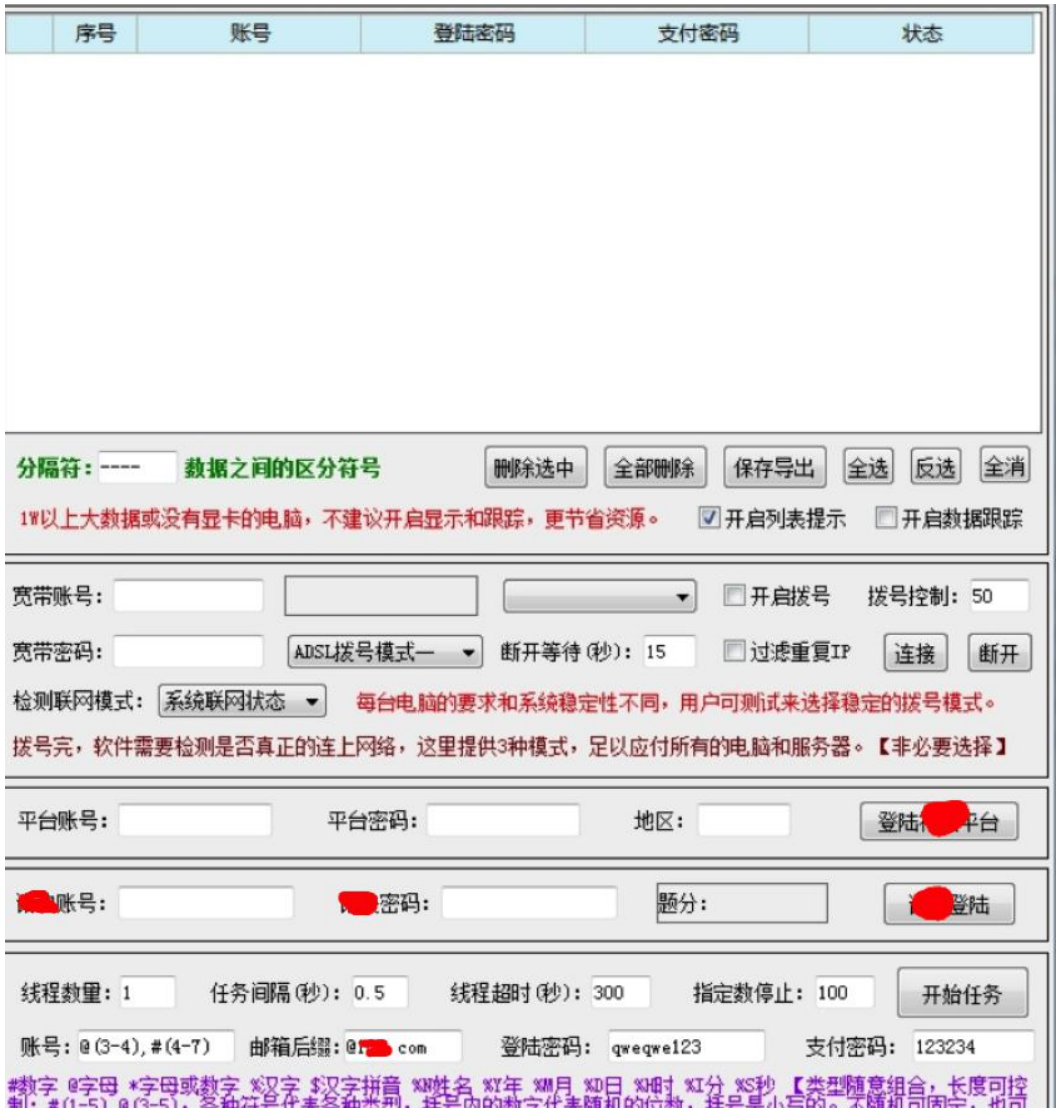


两个例子：说明需要建设需要的具体能力

Web端：账号垃圾注册

移动端-Android&iOS：营销活动薅羊毛

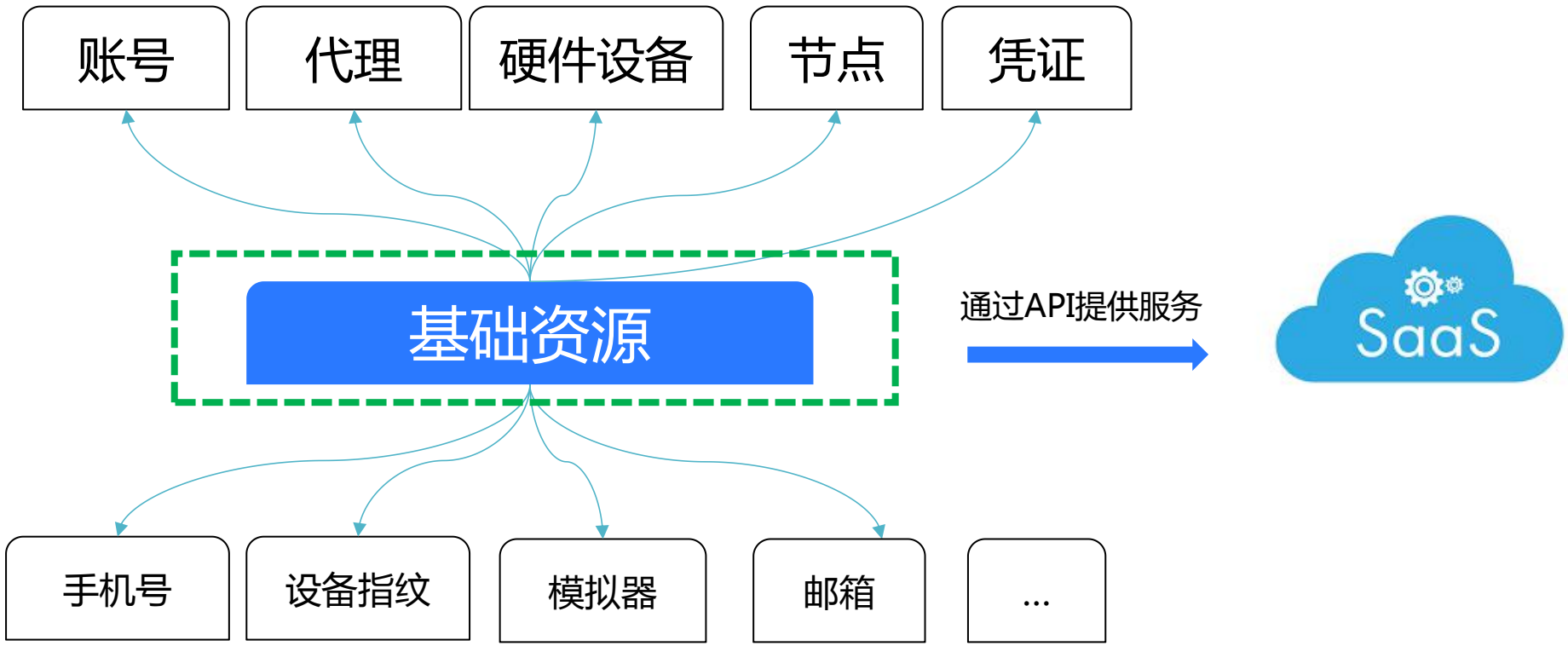
探索实践过程-Web端垃圾注册-资源



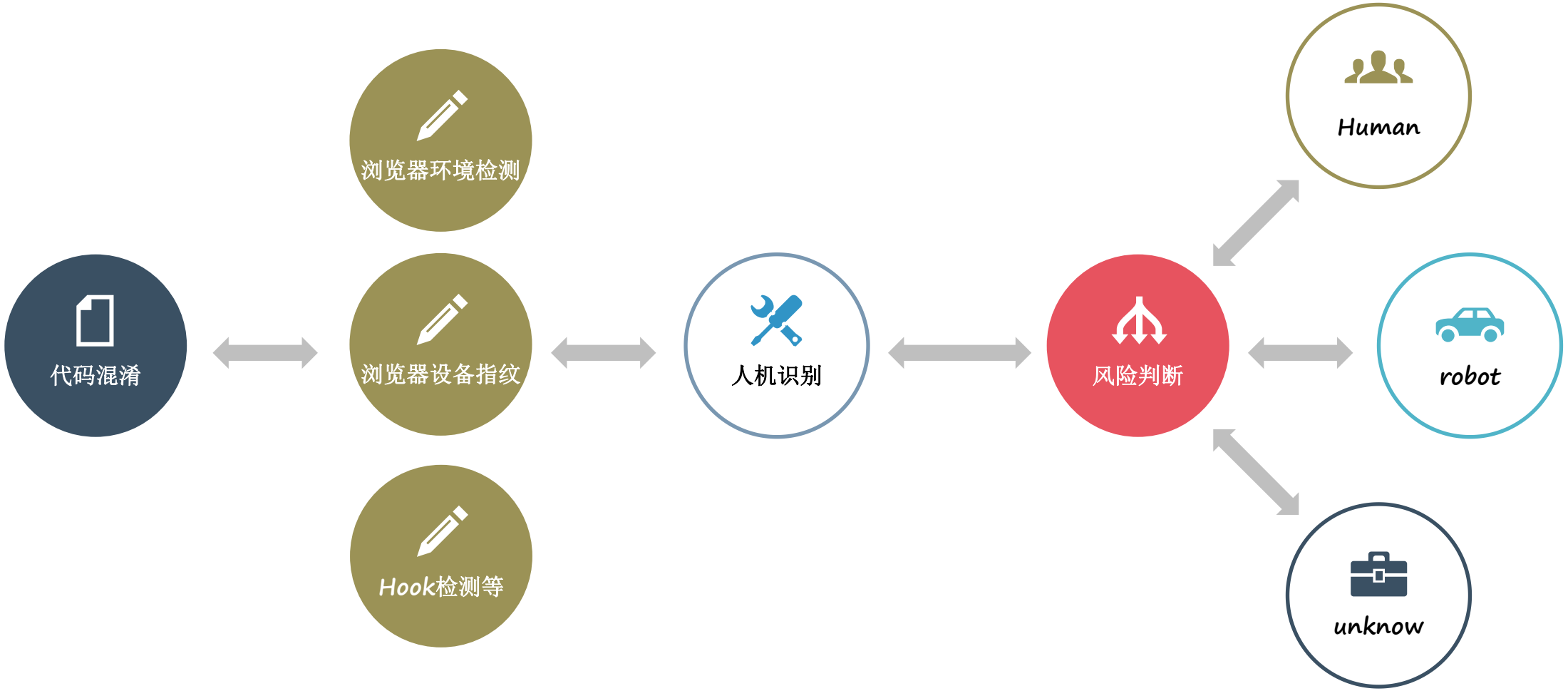
黑灰产垃圾注册软件：
使用猫池、接码平台

黑灰产垃圾注册软件：
使用代理

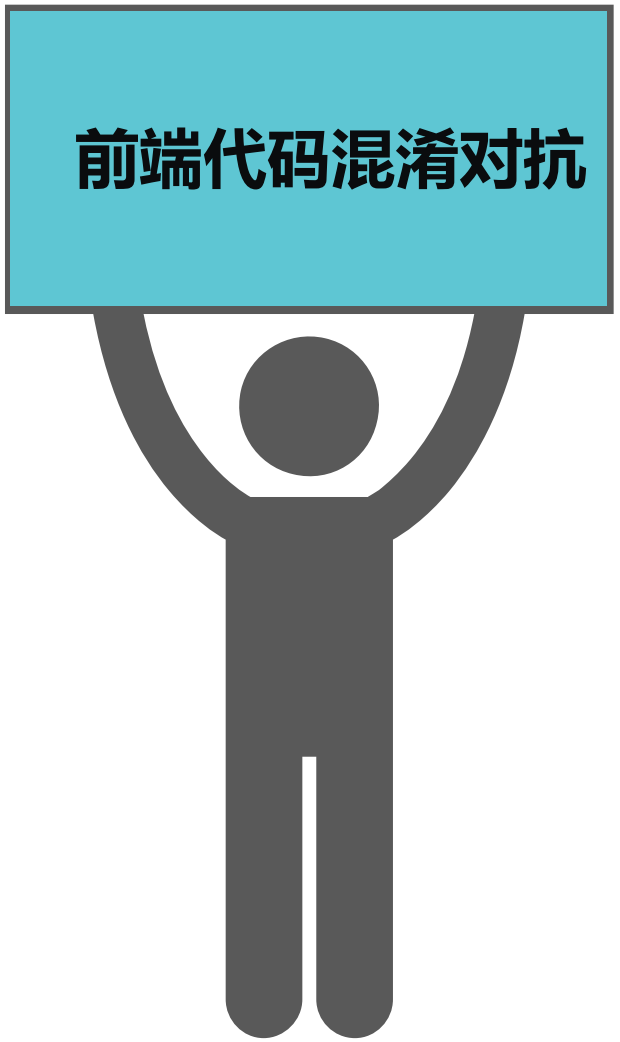
探索实践过程-Web端垃圾注册-资源管理



探索实践过程-Web端垃圾注册-安全&风控对抗



探索实践过程-Web端垃圾注册-安全&风控对抗



01 非常简单的脚本压缩

例如uglify等，并不是真正的混淆，很好还原

02 复杂的脚本编码

例如jjencode、aaencode、jsfuck等编码，也很好还原

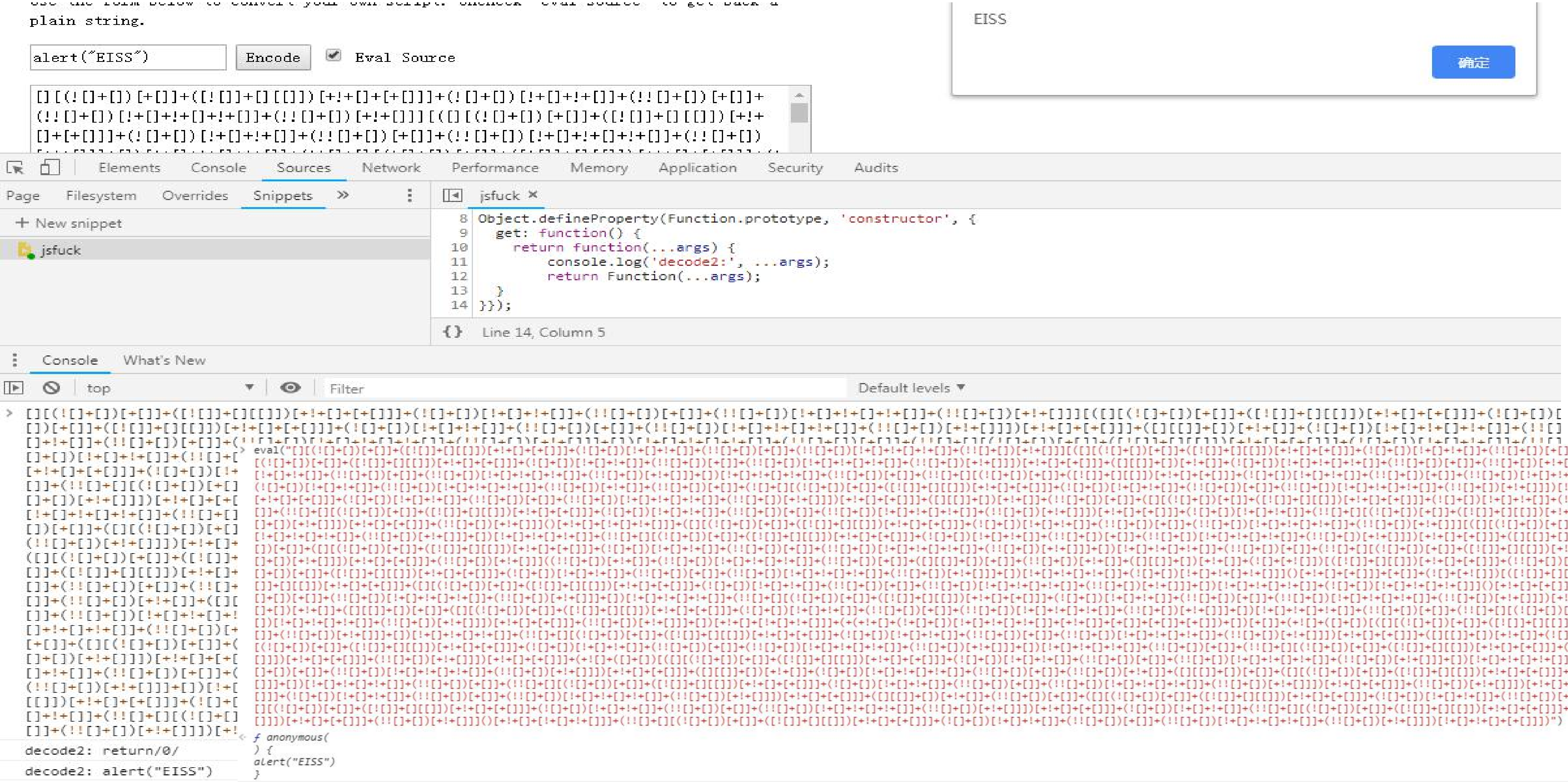
03 修改语法树进行混淆

代码执行流程没有改变，耐心分析也可以还原

04 变更控制流进行混淆

打乱原有代码流程，插入逻辑上无关的代码，再保证混淆的更新频率，理论上相对安全

探索实践过程-Web端垃圾注册-JavaScript混淆对抗



探索实践过程-Web端垃圾注册-JavaScript混淆对抗

jjencode demo

Be aware

Using jjencode for actual attack isn't good idea.

- Decode easily. jjencode is not utilitarian obfuscation, just an encoder.
- Too characteristic. Detected easily.
- Browser depended. The code can't run on some kind of browsers.

Enter any JavaScript source:

```
alert("Hello, EISS" )
```

global variable name used by jjencode : $ palindrome

```
$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$
({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")
($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+"")[
[$.$_][$.$_];$.$($.$($.$$+"\""+$.$_$_+(![]+"")[$._$_]+$.$$$_+"\\"+$.__$+$.$$_+$._$_+$.__+"(\\\"\\"+$.__$+$
[]+"")
[$._$_]+$._$+",\\"+$.$__+$.___+"\\"+$.__$+$.___+$.$_$+"\\"+$.__$+$.__$+$.__$+"\\"+$.__$+$._$_+$._$$+"\\"+
)"+"\"")())();
```

Input the JJEncode here:

```
$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$
($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+
[$._$_]+$.$$$_+"\\"+$.__$+$.$$_+$._$_+$.__+"(\\\"\\"+$.__$+$.__$+$.___+$.$$$_+
[$._$_]+$._$+"\\"+$.$__+$.___+"\\"+$.__$+$.___+$.$_$+"\\"+$.__$+$.__$+$.__$+"\\
```

Decoded JJEncode String:

```
alert("Hello, EISS" )
```

探索实践过程-Web端垃圾注册-JavaScript混淆对抗

通过动态调试，结合hook、snippets等方式来分析还原代码

aaencode demo

aaencode - Encode any JavaScript program to Japanese style emoticons (^_^)
Enter JavaScript source:

```
alert("Hello, EISS")
```

```
ﾟωﾟﾉ= /｀m´）ﾉ ~┻━┻ //*´∇｀*/ ['_']; o=(ﾟｰﾟ) =_=3; c=(ﾟΘﾟ) =(ﾟｰﾟ)-(ﾟｰﾟ); (ﾟДﾟ) =(ﾟΘﾟ)= (o^_^o)/ (o^_^o);(ﾟДﾟ)={ﾟΘﾟ: '_',
,ﾟｰﾟﾉ :(ﾟωﾟﾉ+ '_')[o^_^o -(ﾟΘﾟ)] ,ﾟДﾟﾉ:((ﾟｰﾟ==3) +'_')[ﾟｰﾟ] }; (ﾟДﾟ) [ﾟΘﾟ] =((ﾟωﾟﾉ==3) +'_') [c^_^o];(ﾟДﾟ) ['c'] = ((ﾟДﾟ)+
((ﾟДﾟ)+'_') [ﾟΘﾟ];(ﾟoﾟ)=(ﾟДﾟ) ['c']+(ﾟДﾟ) ['o']+(ﾟωﾟﾉ +'_')[ﾟΘﾟ]+ ((ﾟωﾟﾉ==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ) +'_') [ﾟｰﾟ]+(ﾟｰﾟ)]+ ((ﾟ
[ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ (ﾟДﾟ) ['o']+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_'] =(o^_^o) [ﾟoﾟ] [ﾟoﾟ];(ﾟ
Дﾟﾉ+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_') [o^_^o -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟﾉ +'_') [ﾟΘﾟ]; (ﾟｰﾟ)+=(ﾟΘﾟ); (ﾟ
[o^_^o -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟωﾟﾉ +'_')[c^_^o];(ﾟДﾟ) [ﾟoﾟ]='\"';(ﾟДﾟ) ['_'] ( (ﾟДﾟ) ['_'] (ﾟεﾟ +(ﾟДﾟ)[ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟ
ｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (o^_^o) +(o^_^o))+ ((o^_^o) - (ﾟΘﾟ)
(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟΘﾟ)+ (
ｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+
Дﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (c^_^o)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(
Θﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟ
Дﾟ)[ﾟoﾟ]) (ﾟΘﾟ)) ('_');
```

Deobfuscate

```
ﾟДﾟ  = {
    ﾟΘﾟ: '_',
    ﾟωﾟﾉ: 'a',
    ﾟｰﾟ: 'd',
    ﾟДﾟ: 'e'
};
ﾟДﾟ[1] = 'f';
ﾟДﾟ.c = 'c';
ﾟДﾟ.o = 'o';
ﾟo_ = 'constructor';
ﾟДﾟ._ = Function;
ﾟεﾟ = 'return';
ﾟｰﾟ = 4;
ﾟДﾟ.return = '\\';
ﾟДﾟ.ﾟΘﾟﾉ = 'b';
oﾟｰo = 'u';
ﾟДﾟ.constructor = '"';
(function anonymous() {
    alert('Hello, EISS');
}('_'));
```

探索：通过Partial Evaluation实现的JavaScript反混淆

```
1 !function(){function e(e,a){function c(e){for(var a=1;void 0!==a;){var r=7&a,b=
2 case 16:fs=M?7618:14400;break;case 17:le=re[xe],fs=le?1732:3682;break;case 18:Q
3 break;case 4:he=Ce.charCodeAt($)-106,ee+=String.fromCharCode(he),fs=1512;break;
4 case 0:fs=U?18565:21926;break;case 1:H=127&U,U>>=7,fs=U?9667:20199;break;case 2
5 fs=d?232:10407;break;case 22:$++,fs=12673;break;case 23:v=T,T=v,E=E.concat(T),f
6 Z="",_=0,fs=20163;break;case 17:L=T,T=L<<11,v|=T,E.push(5),T=void 0,L=v,v=[],M=
7 Es[Y](Rs),Y="co",Y+="nnec",Y+="t",fs=19968;break;case 5:Xe=le[Be],Ee=G-1,Xe+=Ee
8 v++,fs=24900;break;case 14:T=M,M=T<<4,v|=M,T=C[L],fs=T?22150:22598;break;case 1
```

探索实践过程-Web端垃圾注册-代码运行环境检测对抗

检测是否运行在PhantomJS、Selenium、 Puppeteer等环境

黑盒调用检测对抗

Hook 钩子检测对抗

设备指纹采集伪造

探索实践过程-Web端垃圾注册-代码运行环境检测对抗

BOM 、DOM等 特征差异

PhantomJS、Chrome Headless：window.callPhantom、window._phantom 、User-Agent、 navigator.plugins.length === 0 、 navigator.languages == ’ ’ 、 window.outerWidth === 0 || window.outerHeight === 0 等

Selenium： window.domAutomation、window.domAutomationController、window.webdriver、 __driver_evaluate、__webdriver_evaluate、__selenium_evaluate、__fxdriver_evaluate、__driver_unwrapped、__webdriver_unwrapped、__selenium_unwrapped、__fxdriver_unwrapped等

Callstack追踪、HTML5新特性等

WebAudio、WebGL、 Canvas 、WebSocket等

Some tricks

unicode特殊编码过的代码（部分Chrome版本）☺

```
> var a = '□';
  console.log("test");
> var a = '□';
  console.log("test");
> console.log("test--1");
  test--1
```

探索实践过程-Web端垃圾注册-Hook检测对抗

一个简单的例子：alert()

```
> 19:14:48.429 alert.toString()
<· 19:14:48.432 "function alert() { [native code] }"
> 19:15:06.020 var oldAlert = alert;
<· 19:15:06.024 undefined
> 19:16:04.481 alert = function(m) {
                     console.log("fake alert...")
                     oldAlert(m);
                 };
<· 19:16:04.488 f (m) {
                     console.log("fake alert...")
                     oldAlert(m);
                 }
> 19:16:13.551 alert.toString()
<· 19:16:13.554 "function(m) {
                     console.log("fake alert...")
                     oldAlert(m);
                 }"
> 17:54:07.970 alert.toString = function() {
                     return 'function alert() { [native code] }';
                 };
<· 17:54:07.975 f () {
                     return 'function alert() { [native code] }';
                 }
> 17:54:09.993 alert.toString()
<· 17:54:09.997 "function alert() { [native code] }"
```

调用原型上的Function.prototype.toString.call(alert) 检测，继续hook … 持续攻防迭代 ☺

探索实践过程-Web端垃圾注册-设备指纹伪造

多维度特征采集

开源的fingerprint2.js（效果并不是很好，只是拿来举个例子 ☺）

```
395     var UserAgent = function (done) {
396       done(navigator.userAgent)
397     }
398     var webdriver = function (done, options) {
399       done(navigator.webdriver == null ? options.NOT_AVAILABLE : navigator.webdriver)
400     }
401     var languageKey = function (done, options) {
402       done(navigator.language || navigator.userLanguage || navigator.browserLanguage || navigator.systemLanguage || options.NOT_AVAILABLE)
403     }
404     var colorDepthKey = function (done, options) {
405       done(window.screen.colorDepth || options.NOT_AVAILABLE)
406     }
407     var deviceMemoryKey = function (done, options) {
408       done(navigator.deviceMemory || options.NOT_AVAILABLE)
409     }
410     var pixelRatioKey = function (done, options) {
411       done(window.devicePixelRatio || options.NOT_AVAILABLE)
412     }
413     var screenResolutionKey = function (done, options) {
414       done(getScreenResolution(options))
415     }
416     var getScreenResolution = function (options) {
```

反混淆js分析后，进行伪造即可… evercookie方案同理，不展开☺

```
> 19:29:53.601 navigator.platform
<· 19:29:53.605 "MacIntel"
> 19:30:27.690 // example
               Object.defineProperty(navigator, "platform", {
                   get: function() {
                       return "iPhone";
                   }
               });
<· 19:30:27.693 ▶Navigator {vendorSub: "", productSub: "20030107", vendor: "Google Inc.", m
> 19:30:30.392 navigator.platform
<· 19:30:30.395 "iPhone"
> |
```

探索实践过程-Web端垃圾注册-人机识别对抗

人机识别攻防

图灵测试-验证码

Deep Learning，通过卷积神经网络CNN识别等

用户行为

伪造鼠标轨迹、行为事件、键盘事件等

大数据模型

设备牧场，养号对抗等

探索实践过程-Web端垃圾注册-风控算法模型&规则对抗

01 **高质量代理IP**

对抗IP画像☺

02 **算法模型**

基于Logistic 等算法模型的对抗☺

03 **场景特有的规则**

注册频率、UA分布比例等☺

探索实践过程-移动端 营销活动薅羊毛

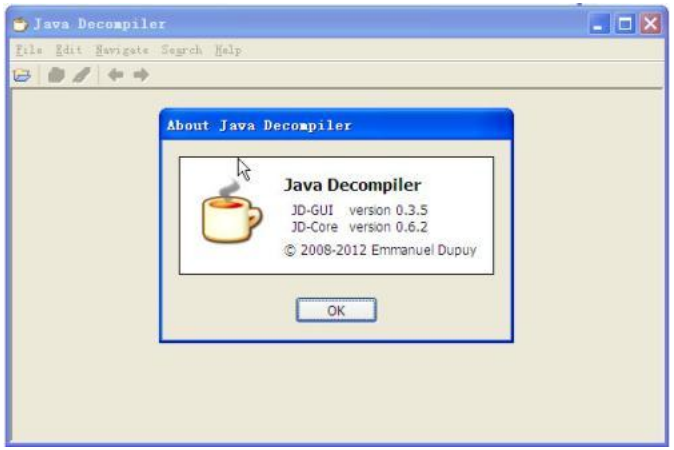
时间原因不展开说，思路同Web端 ☺

设备伪造

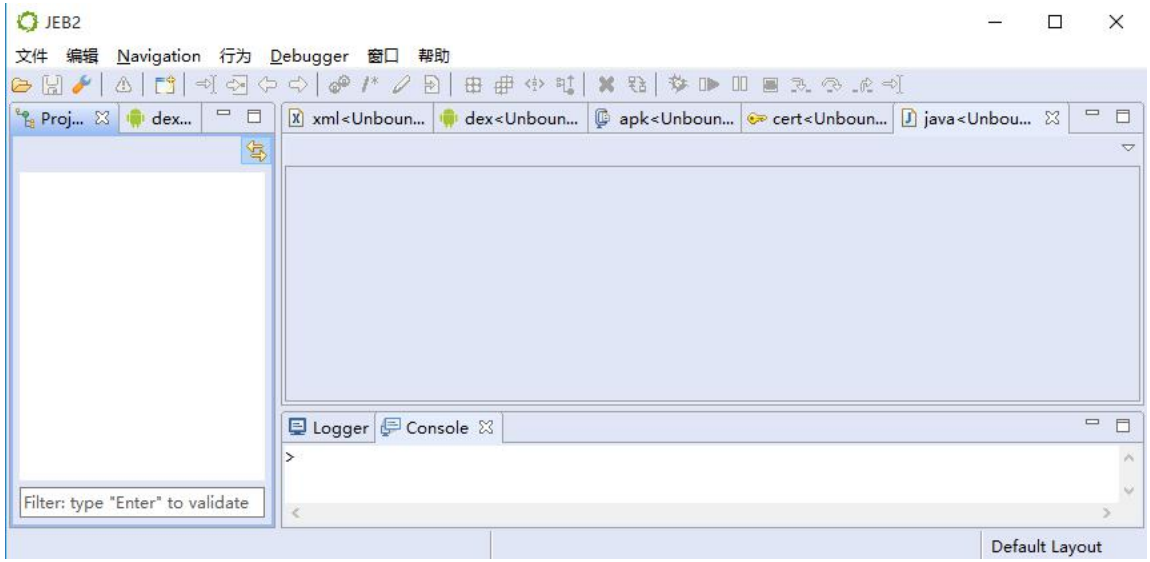
Android、iOS一键改机软件，模拟器检测等

协议破解

刷接口API、Hook等



FRIDA

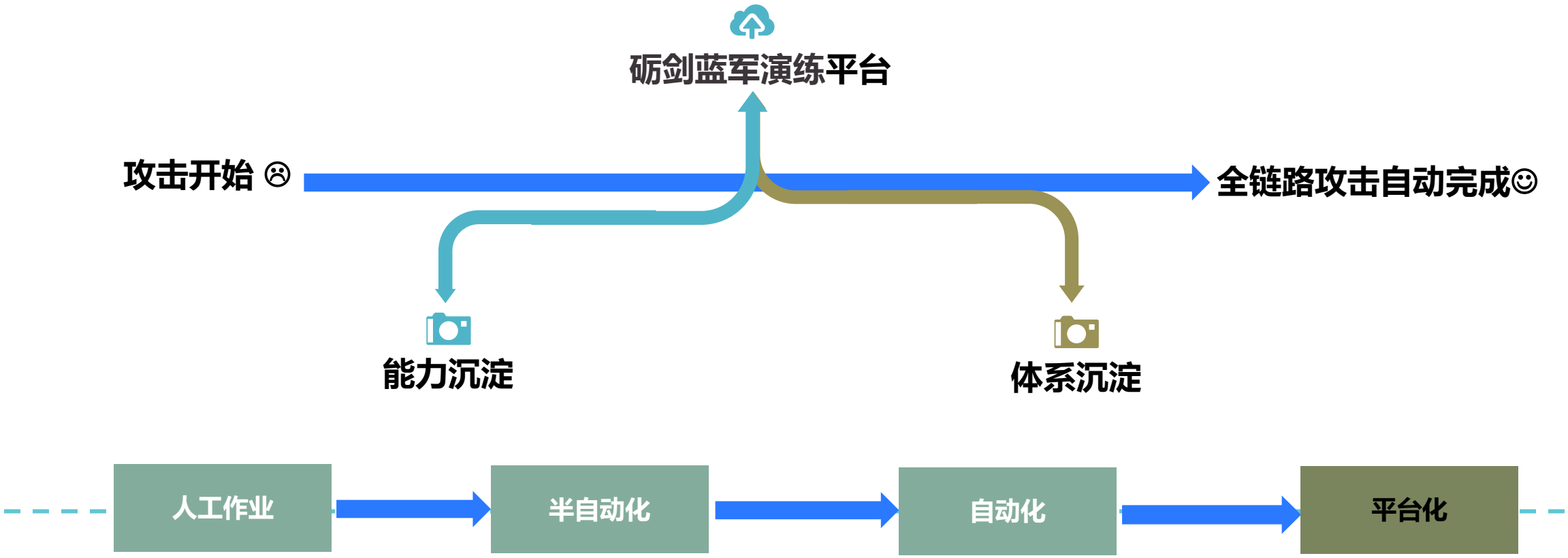



```
iPod:~ root# DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib /var/mobile/Applications/xxxxxxxx-xxxx-x
mach-o decryption dumper

DISCLAIMER: This tool is only meant for security research purposes, not for application cracker

[+] Found encrypted data at address 00002000 of length 1826816 bytes - type 1.
[+] Opening /private/var/mobile/Applications/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/Scan.app/Scan
[+] Reading header
[+] Detecting header type
[+] Executable is a FAT image - searching for right architecture
[+] Correct arch is at offset 2408224 in the file
[+] Opening Scan.decrypted for writing.
```

探索实践总结



03 砺剑蓝军演练平台

砺剑蓝军演练平台


攻防演练控制台
数据查询
武器管理
节点管理
任务管理
资源管理
场景配置
...
跨域分布式调度引擎
任务引擎
武器库
跨平台Agent
大规模节点调度
任务消息队列
周期调度
业务演练
黄牛秒杀
营销活动
视频刷量
广告攻击
垃圾注册
...
核心能力
核心能力
图片识别
滑块验证码
自动脱壳
...
基础资源
基础数据
账号数据
身份凭证
IP数据
...

Q&A

招人：
1.移动安全逆向工程师&专家（Android&iOS）
2.红蓝对抗攻防演练工程师（web&移动应用安全、渗透测试、业务风控安全技术研究、漏洞挖掘等方向）

工作地点：北京、杭州 皆可

柳兮

中国

扫一扫上面的二维码图案，加我微信

Thank You