



知道创宇漏洞社区计划

知道创宇 张祖优(Fooying)

漏洞社区 ●

K

KCon

追求干货有趣的
黑客大会

Z

ZoomEye

网络空间搜索
引擎，全球漏
洞感知与预警

S

Sebug

聚焦漏洞，提供漏洞威
胁情报信息与交易平台

ZoomEye[®]

过去

在过去，基于 ZoomEye 我们做了许多事



组件识别

通过自主研发引擎，我们对网络空间进行了重要端口探测与组件识别

开放搜索

我们公开了许多研究成果，并开放海量结果数据供大家搜索

全球路由器后门探测

2014年2月份，我们针对全球路由器进行全网扫描并发出安全预警



摄像头漏洞探测

2014年3月，针对国外黑帽大会曝光的家庭摄像头漏洞进行全网的探测并发出预警

心脏出血

2014年4月，针对心脏出血漏洞进行全球探测并绘制全球范围分布，2015年4月，进行一周年普查

破壳漏洞

2014年9月份，应急响应“破壳漏洞”，第一时间将国内受影响情况统计并预警

上线专题

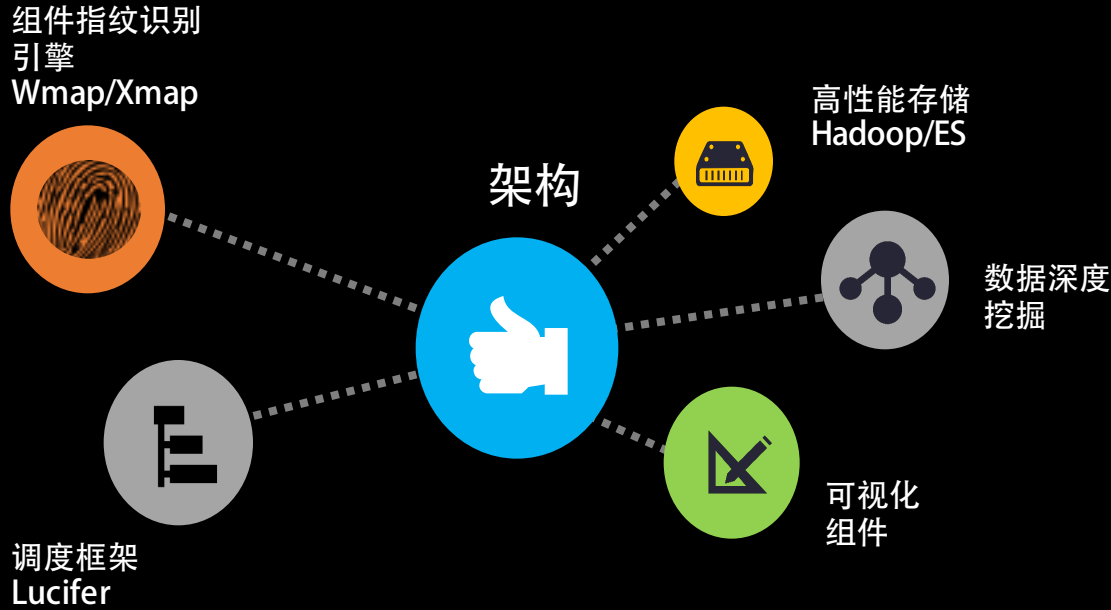
工控专题、漏洞专题等

Dork 闭环

Dork 是我们和网络空间交流的语言，你的每一次搜索都将诞生一个 Dork

这是大家所能看到的

背后的这些



- 扫描能力提升约4倍
- 端口覆盖提升 1 倍
- 识别组件增加 30 %
- 扫描速率提升约 3 倍
- 数据存储量增加 4 倍以上
- 还有更多

Sebug

7月7日开始内测





今日起正式公测



漏洞集市

100 万补贴，欢迎大家到我们平台进行提交漏洞、PoC、兑换查看等等

漏洞集市

漏洞基本字段补充

详情补充

PoC/Exp 提交

详情与 PoC 兑换

兑换分成

交易动态



漏洞集市

100 万补贴，欢迎大家到我们平台进行提交漏洞、PoC、兑换查看等

更多 ZoomEye 功能与奖励

ZoomEye 暗物质消除计划、ZoomEye X计划、Dork 提交奖励计划等

ZoomEye 更多功能与计划

ZoomEye
暗物质消
除计划

ZoomEye
X 计划

Dork 提交
奖励计划

漏洞集市

100 万补贴，欢迎大家到我们平台进行提交漏洞、PoC、兑换查看等等

Pocsuite

开放我们的 PoC 标准，开源我们的框架

更多 ZoomEye 功能与奖励

ZoomEye 暗物质消除计划、ZoomEye X 计划、Dork 提交奖励计划等

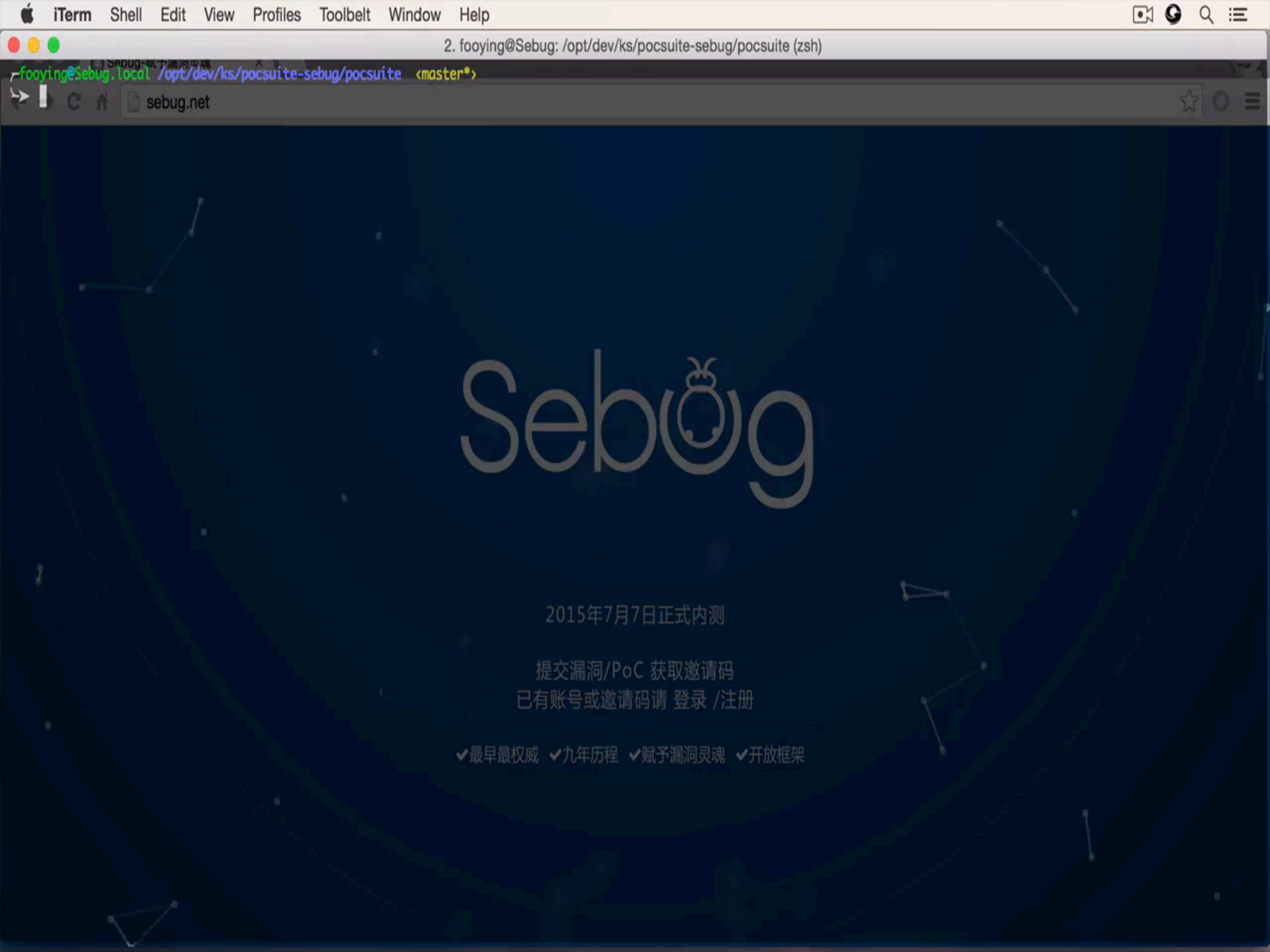
Pocsuite

远程 PoC 框架，知道创宇安全研究团队发展的基石

基础 PoC 编写 SDK



自动化调用与测试



Sebug

2015年7月7日正式内测

提交漏洞/PoC 获取邀请码
已有账号或邀请码请 登录 /注册

- ✓最早最权威
- ✓九年历程
- ✓赋予漏洞灵魂
- ✓开放框架

漏洞集市

100 万补贴，欢迎大家到我们平台进行提交漏洞、PoC、兑换查看等

Pocsuite

开放我们的 PoC 标准，开源我们的框架

更多 ZoomEye 功能与奖励

ZoomEye 暗物质消除计划、ZoomEye X 计划、Dork 提交奖励计划等

ZoomEye X

```
./zoomeye -dork  
'app:openssl'  
| ./sebug -vul  
'openssl'
```

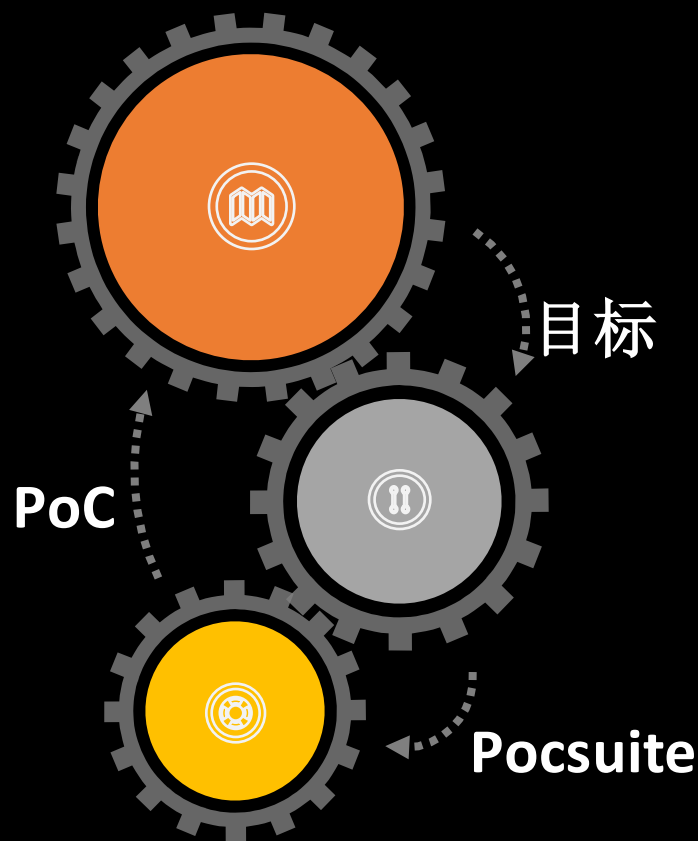
ZoomEye X

根据 ZoomEye Dork 获取对应目标

获取对应漏洞 PoC

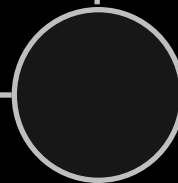
Pocsuite

```
hacker@kcon:~# ./zoomeye --  
dork 'app:openssl' | ./sebug --vul  
'openssl'
```



```
↳> ./zoomeye --dork 'app:openssl'|./sebug --vul 'openssl' -v
```

我们将开放更多的能力



核心伙伴生态圈

构建核心伙伴生态圈，优
先开放我们的能力



期待你的加入



谢谢大家

Fooying

