风险控制与网络安全

杨冀龙@knownsec.com

1 黑客在做什么

2 我们在做什么

3 行业需要什么

Hacker

黑客在做什么

0-Day

一手的很难见

以现有业务的复杂和混乱，多数情况下无需 0-day

How to get 10,000+ Backdoorsssssssssss …

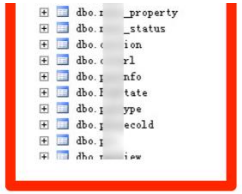
- 30+服务器
- 固定IP
- 不间断扫描
- 新披露漏洞

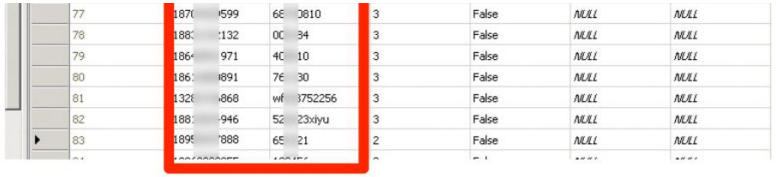
- 单一地址
- 直接访问后门
- 回传数据

动作一:黑市交易互联网金融企业敏感信息

id	用户	姓名	身份证	银行卡	开户行	
4	99	段	41	6	中国工商银行	未来路支行
4	99	肖	42	6	中国建设银行	建设银行凤凰城支行
4	99	王	23	6	中国银行	中国银行(沈阳支行)
4	99	冯	44	6	中国建设银行	广州东城支行
4	99	邓	50	6	招商银行	福州分行湖东支行
4	99	冯	21	6	中国银行	中国银行沈阳兴工北街支
4	99	赵	42	6	中国银行	甘泉路支行
4	99	胡	21	6	中国银行	市府大路支行
4	99	罗	36	6	中国建设银行	中国建设银行
4	99	胡	33	6	中国工商银行	磐安县支行
4	99	裴	42	6	中国工商银行	亭林支行
4	99	邹	42	6	中国建设银行	大冶支行

动作二：盗窃金融客户资产



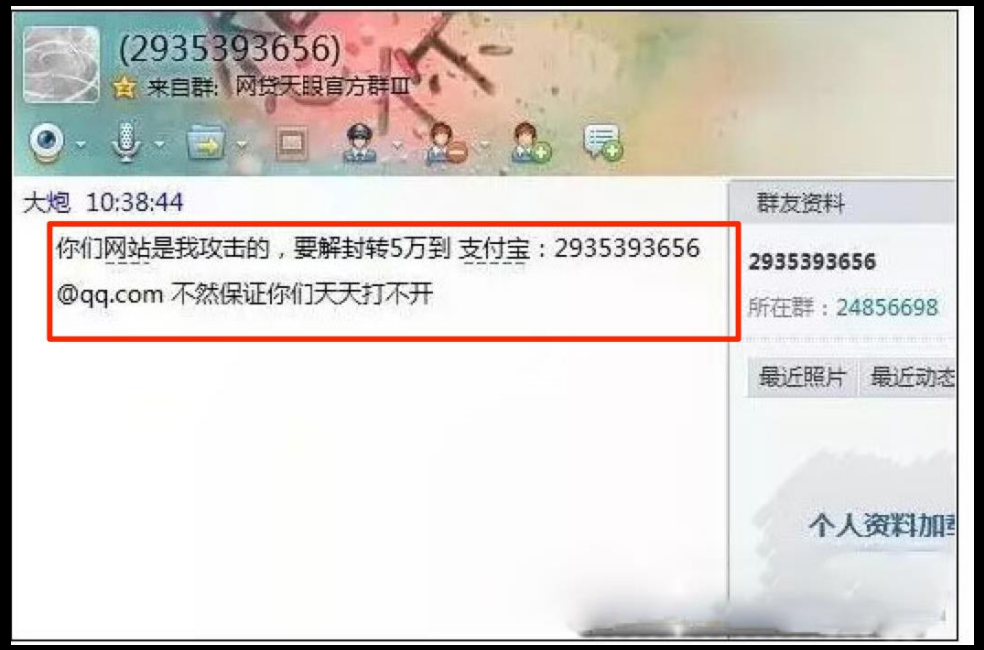


系 help@wooyun.org

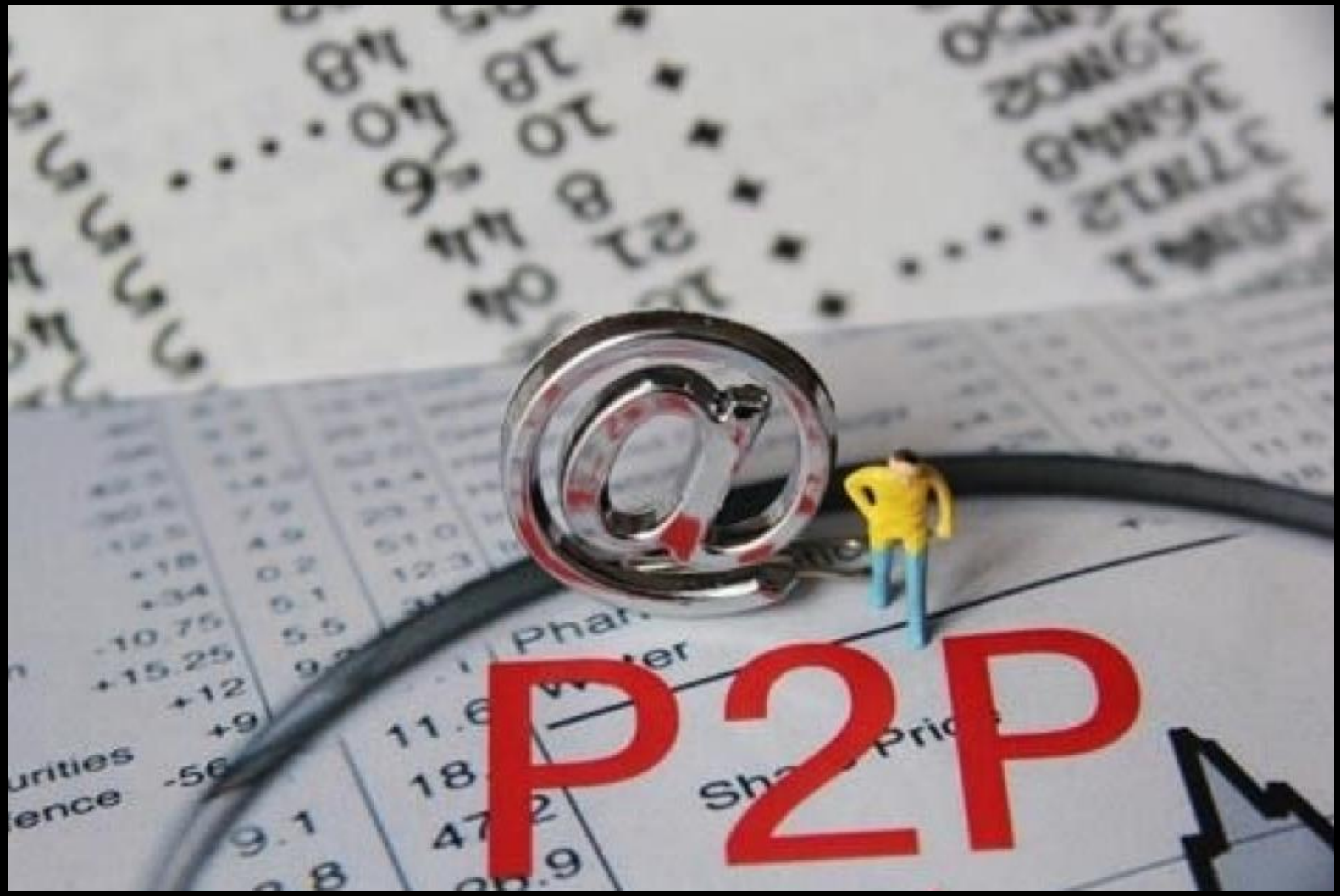
动作三：敲诈勒索互联网金融企业

元宝网遭遇黑客敲诈勒索

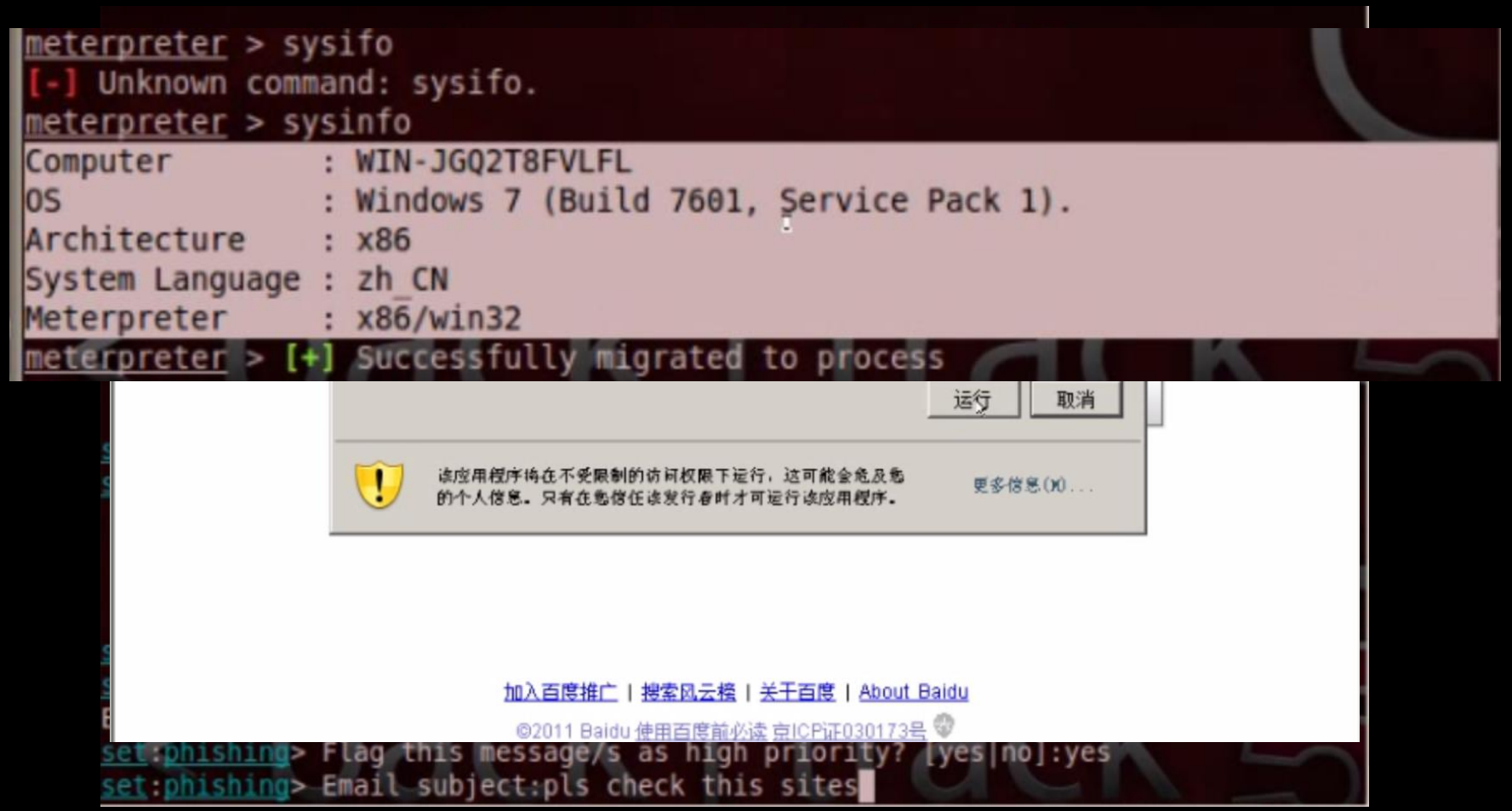
网贷天眼遭遇黑客敲诈勒索



动作四：薅羊毛



动作五：抓鸡


meterpreter > sysifo
[-] Unknown command: sysifo.
meterpreter > sysinfo
Computer : WIN-JGQ2T8FVLFL
OS : Windows 7 (Build 7601, Service Pack 1).
Architecture : x86
System Language : zh_CN
Meterpreter : x86/win32
meterpreter > [+] Successfully migrated to process
运行
取消
该应用程序将在不受限制的访问权限下运行，这可能会危及您的个人信息。只有在您信任该发行者时才可运行该应用程序。
更多信息(M)...
加入百度推广 | 搜索风云榜 | 关于百度 | About Baidu
©2011 Baidu 使用百度前必读 京ICP证030173号
set:phishing> Flag this message/s as high priority? [yes|no]:yes
set:phishing> Email subject:pls check this sites

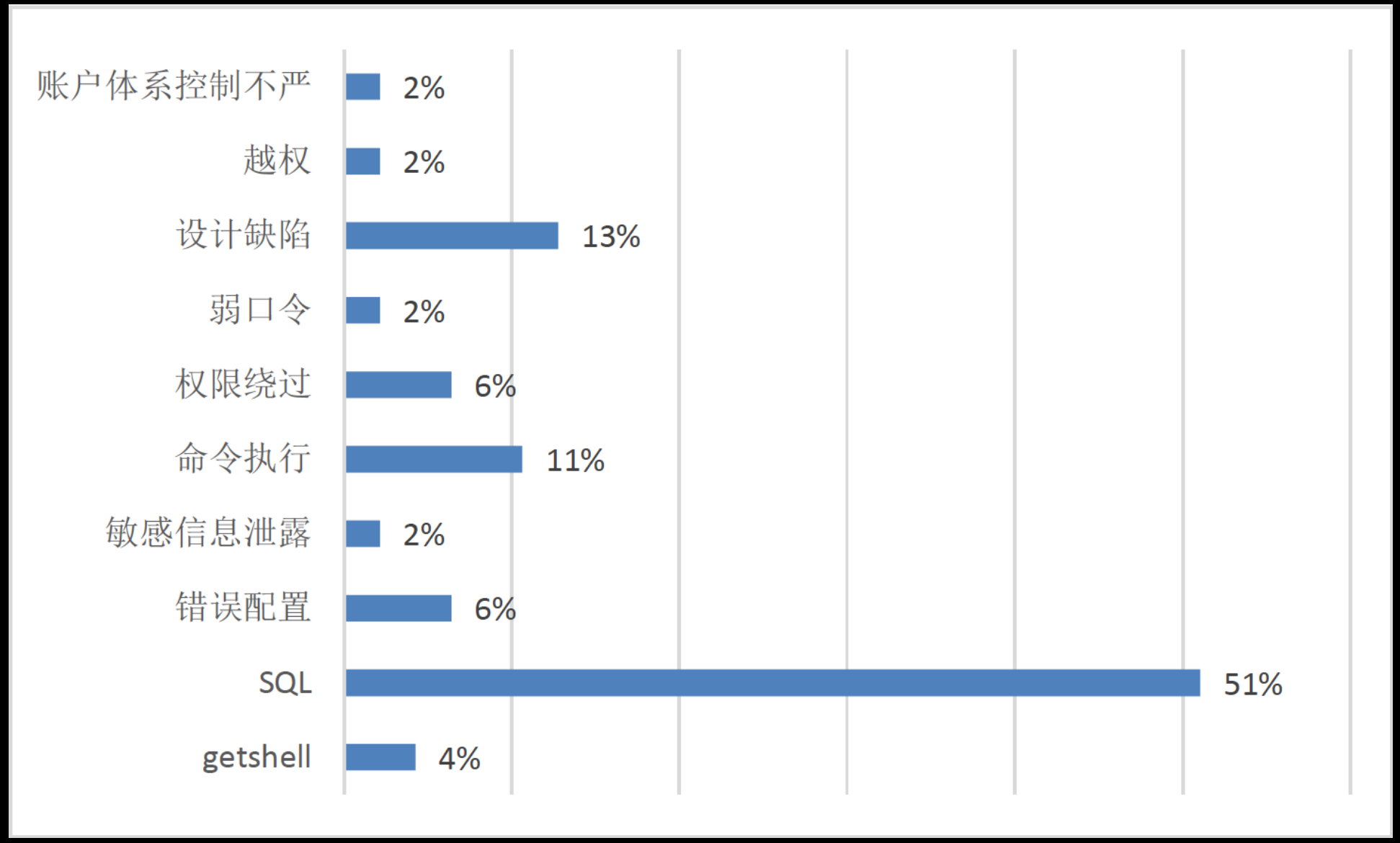
Enterprise

我们在做什么

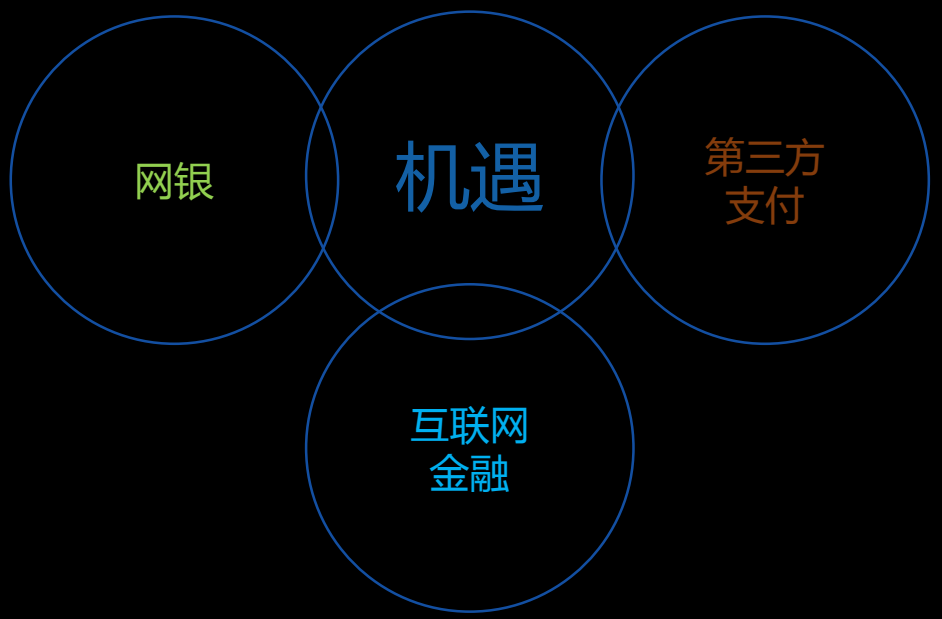
我们在宣称自己的网站很安全！！！！

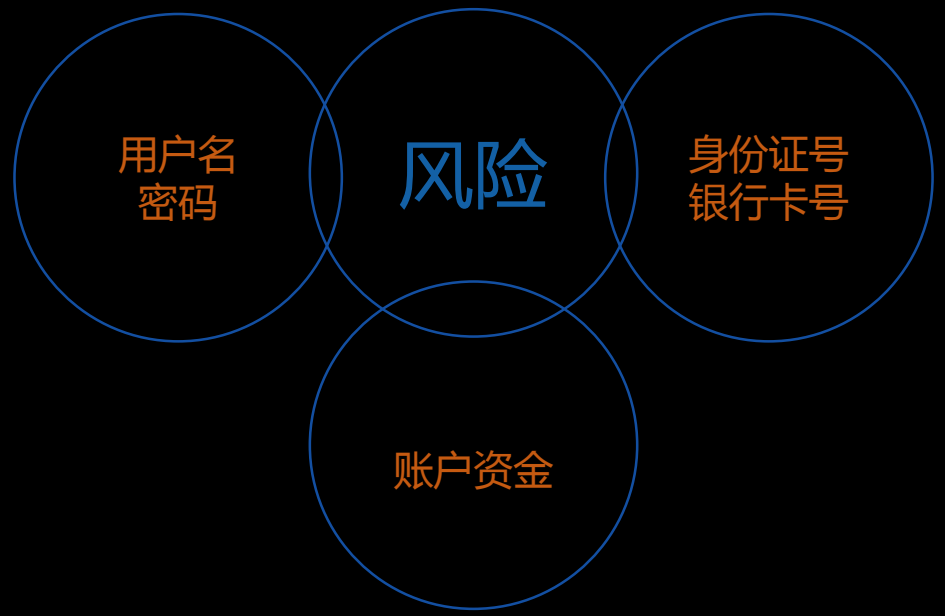
- 10%的 互联网金融企业没有有专职安全工程师；
- 一半以上平台连HTTPS都没有；
- 60%以上有高危漏洞；
- 65-75%裸奔；
- 多数互联网金融平台没进行过安全检测；
- 还都宣传自己是最安全的投资平台；

我们不了解漏洞！！！

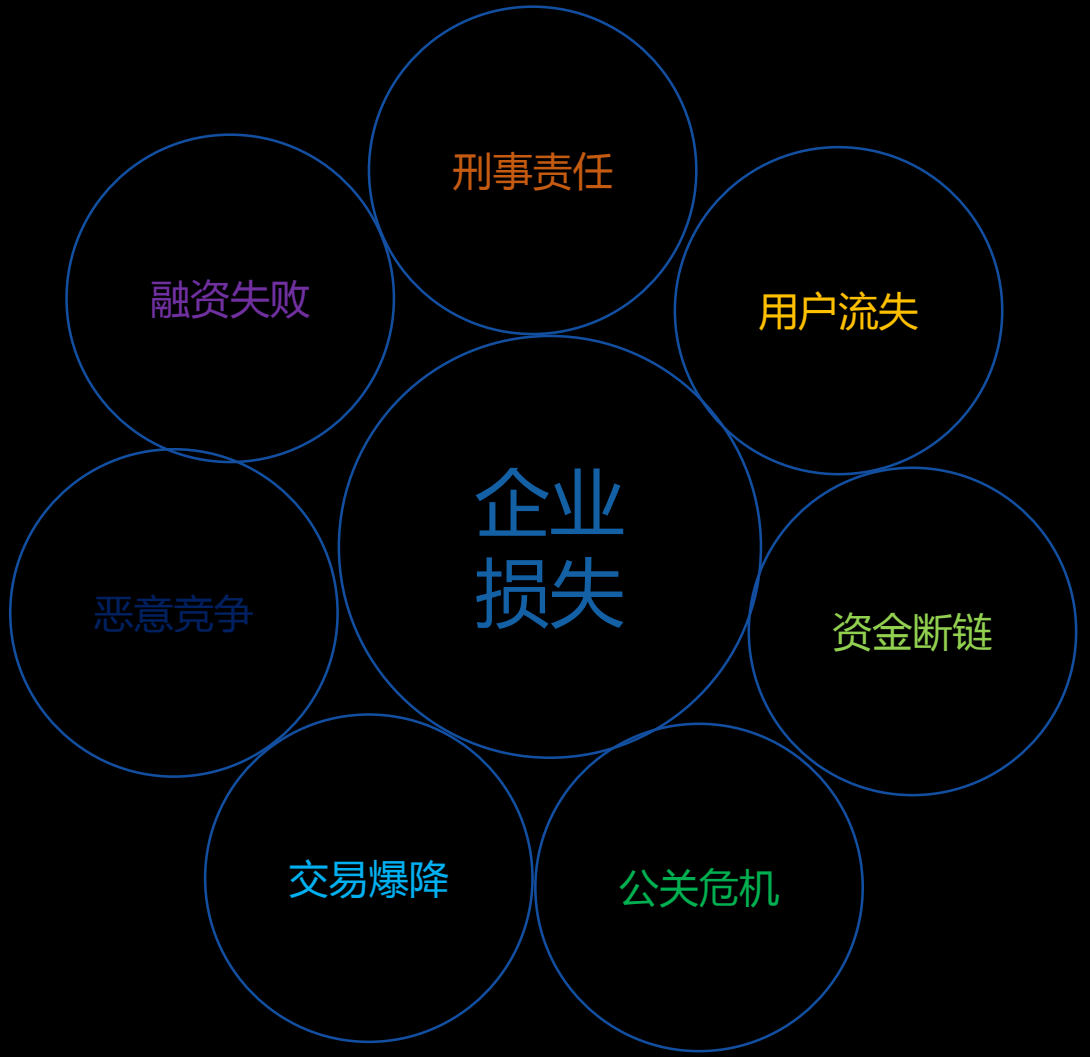

账户体系控制不严
2%
越权
2%
设计缺陷
13%
弱口令
2%
权限绕过
6%
命令执行
11%
敏感信息泄露
2%
错误配置
6%
SQL
51%
getshell
4%

我们只看到了机遇却忘记了风险！！！



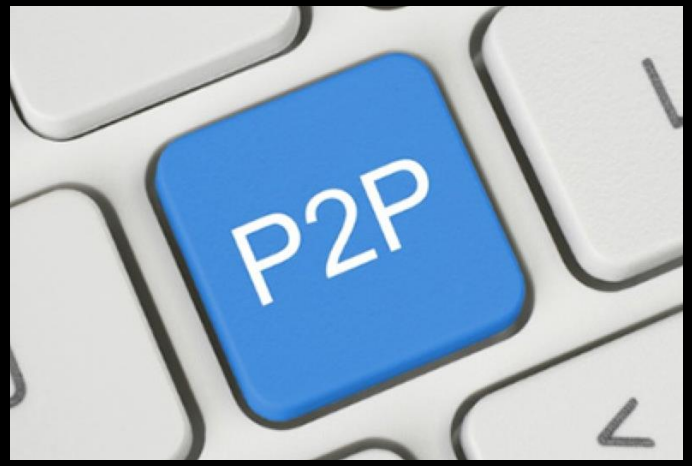


我们不了解这些风险给企业带来的巨大损失！！！



事实证明我们还有许多事情要做！！！

据第三方统计，2015年新上线的网贷平台超1500家，累计平台数量达到3858家，而全年问题平台就达到896家，是2014年的3.26倍。



Industry

行业需要什么

需要站在行业角度找到风险存在的根源

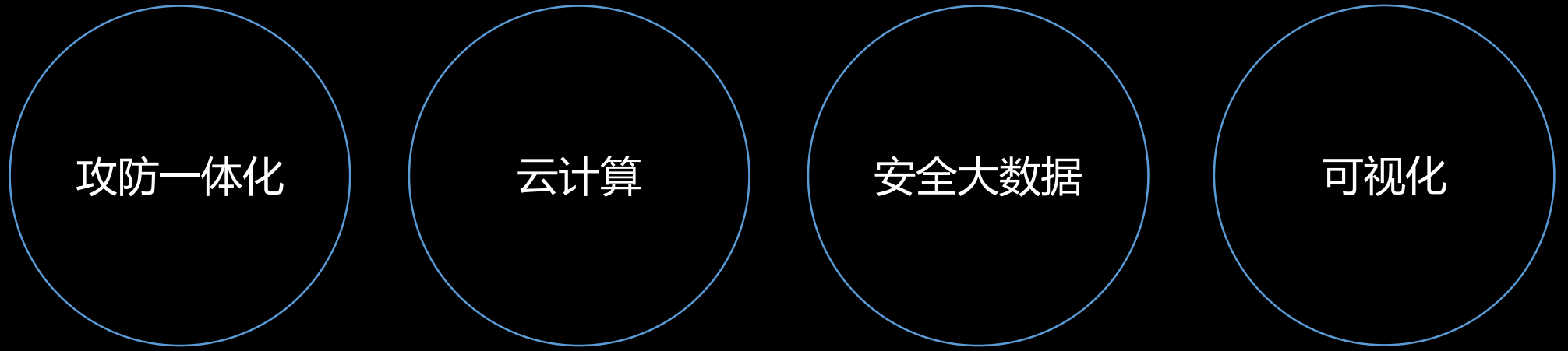
风险的根源>网络安全>导致互金行业安全问题>

About me

About hacker

About knownsec

知道创宇一直在做的事情



国内最早提出网站安全**云监测**及**云防御**的高新企业
始终致力于提供基于**云端大数据**支撑的下一代Web应用安全解决方案
以**安全云**解决Web安全问题

持续的大数据积累

8亿/300万/50亿

通过腾讯安全管家覆盖的**8亿终端**，
每日搜集**300万垃圾邮件**，
积累超过**50亿条病毒&木马样本**

4800万/40万/1000

积累超过**4800万恶意URL**地址的信誉数据，识别超过**40万C&C地址**，
识别过**上千种扫描器特征**

42亿/20亿/5000

知道创宇ZoomEye探测全球**42亿个IP**，国内**3.3亿IP**
监控超过**20亿**网页和图片的威胁信息，
挖掘超过**5000个0day**漏洞

86万/10亿+

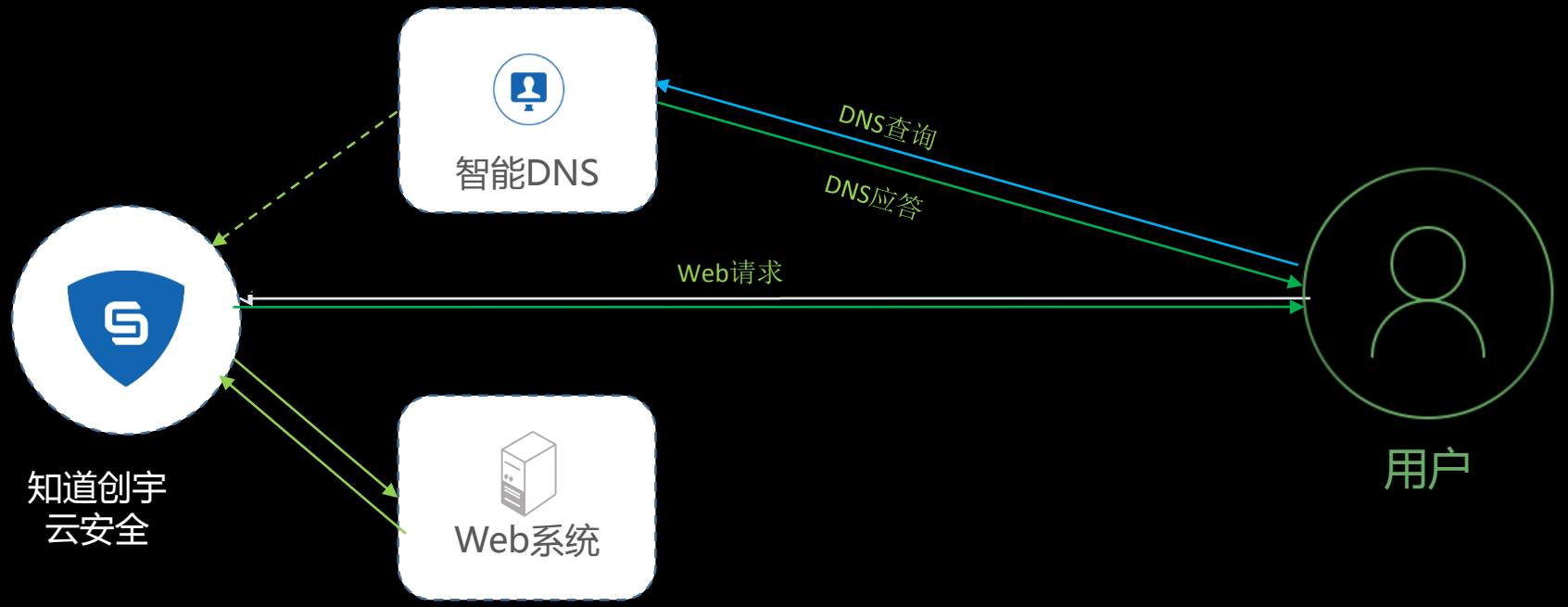
知道创云防护平台保护着国内超过**86万个网站**
每天监控超过**10亿安全攻击事件**类威胁情报

10亿/33万

累积超过**10亿恶意IP**地址的信誉数据，
识别跟踪**33万活跃黑客**

SaaS部署 更快更便捷

更改网站CNAME解析，最快5分钟生效



攻击防护

知道创宇云安全是怎么保证网站不被黑客攻破？

专属防御

基础防御

针对性防御

云防御

裤带锁

专家系统

安全评级云

协同防御

自动攻击识别

规则防御

区域访问识别

持续的攻击源分析


站点 210
关注 60
地区 18
入侵警报 12
风险预警 56
主站数量 382
子站数量 1,306
未防御 167
24h数量 13,306
323,839,182
SQL注入
DDoS
篡改
扫描
CC
XSS
攻击态势
流量/拒绝服务
四川 231
北京 123
政务网站 23
地方政府 19
河北 123
匿名者
Peter Peng
LV5
活动频度
最近一周
最近一月
最近一年
200
150
100
50
191
7月5
7月6
7月7
7月8
7月9
7月10
7月11
常用 IP
常用浏览器
Chrome
Safari
Firefox
同在 匿名者 组织的其他黑客
攻击历史
XSS
2 分钟前
SQL 注入
4 分钟前
拖库
7 分钟前
查看更多
上网习惯
谷歌
xscan
facebook
Firefox
抱枕
盖饭
DirBuster
韩国拌饭
苍井空
SQLMAP
常用攻击工具
SQLMAP
DirBuster
常用攻击语句
and 1=(select count(*) from admin where len(*)>0)
and sa=(Select System_blank>_user) -
and user_blank>_name()=dbo -
and 0<>(select user_blank>_name() -
常攻击的网站

拉近虚拟与现实的距离

- fi*** 好友 / 同校同学 / 同一组织
- 常用ID ： Ma*** / Zen***
- 相对 fi*** 更专注于 漏洞研究
- 挖掘出大量 后门、攻击程序等

MALANG
XX军团

- www.mc***.or.id
- 大量exp 和工具
- 成员多为学校学生
- 多次攻击记录

- Anonymous 印尼分舵
- 常用ID ： fi*** / f***@yahoo.com
- 站点 c**.hack***.org / f**@c**.hack***.org
- 主要语言 爪哇语 / 印尼人
- 印尼MALANG某高校（XX军团诞生地）
- 女友常用 ID：N***_O**

知道创宇为互联网金融企业解决网络安全问题

1、安全情报子系统

集合开源情报、有源情报、无源情报进行大数据分析，挖掘已知、未知风险和威胁。

追溯系统

GAC

2、大数据分析

ZoomEye

Websoc

4、无源雷达探针、攻击溯源发射台

2、漏洞风险控制子系统

监控全局站点安全状态，具备强大的风险感知能力。

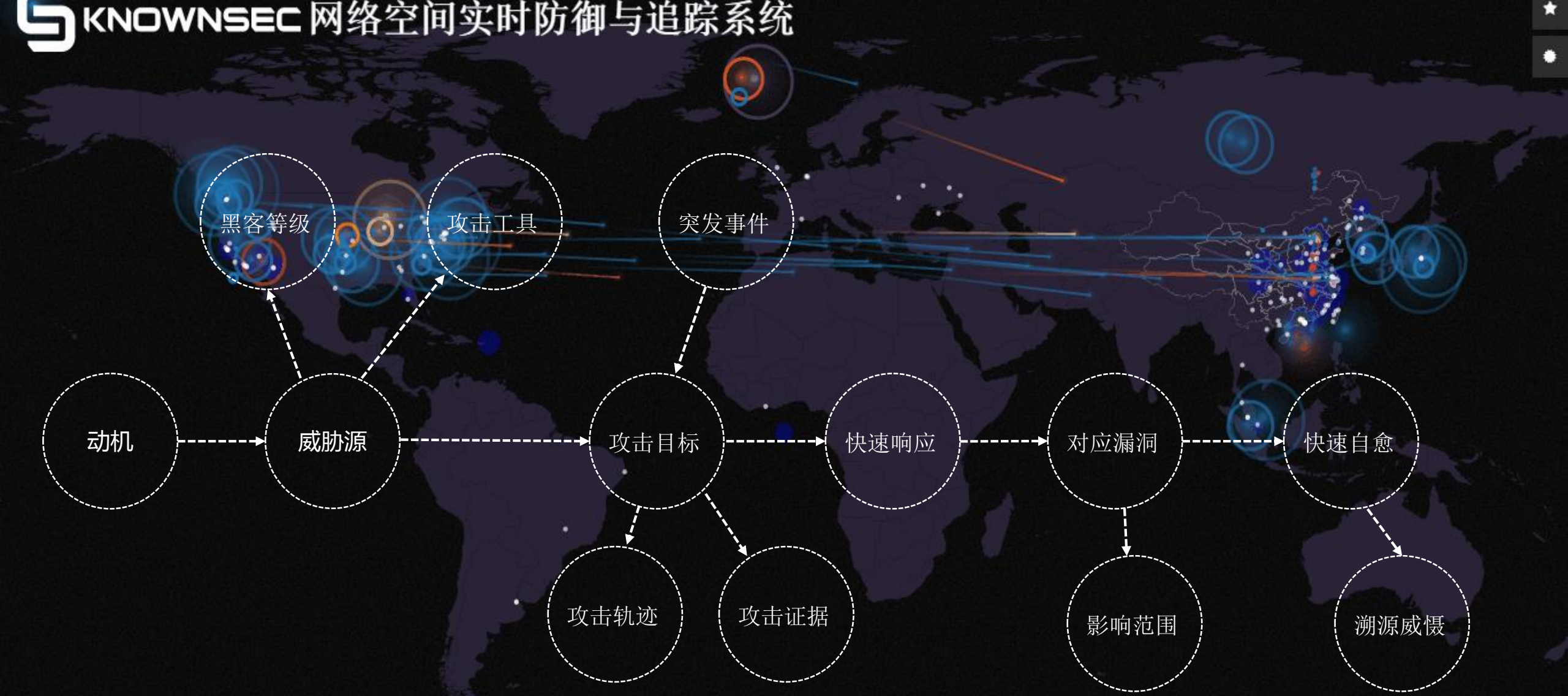
3、安全云防御平台

抗D保+加速乐+创宇盾

5、安全态势感知

6、攻防一体化

KNOWNSEC 网络空间实时防御与追踪系统



展开

攻击者

IP	位置	类型	次数
54.243.164.122	Ashburn	SCANNER	3
107.167.176.81	-	SCANNER	1
103.241.48.57	-	SCANNER	1

目标

域名	位置
pintu360.com	Beijing
jsnews.jschina.com.cn	Nanjing
www.xmxyk.net	Beijing

攻击者来源

地区	次数
China	4173
United States	525
Hong Kong	417

目标地区

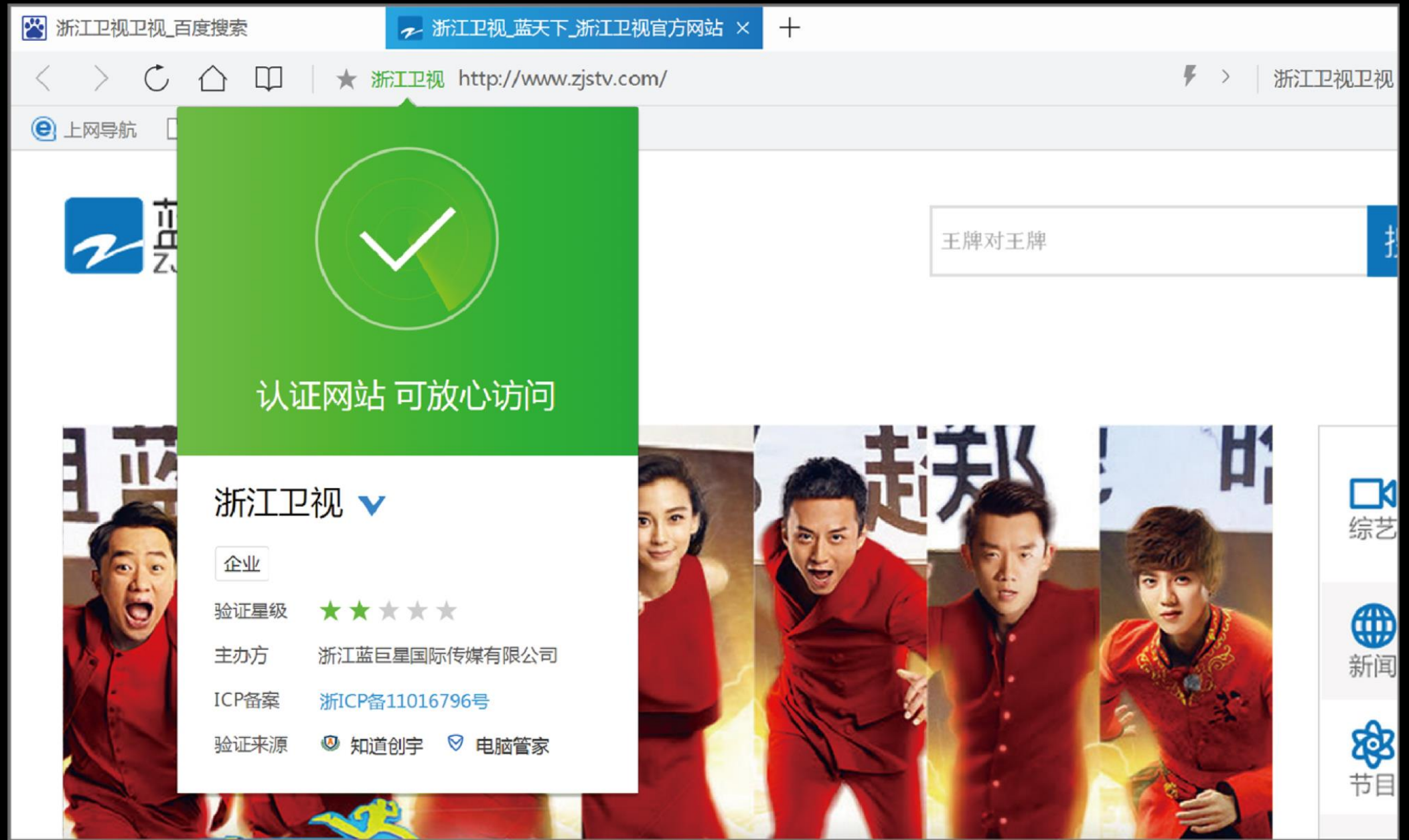
地区	次数
China	5053
United States	117
Virgin Islands, British	96

攻击类型

类型	次数
SCANNER	3256
SQLI	809
COLLECTOR	613

IP地址库、域名库、重要系统库、黑白URL库、恶意代码病毒库、漏洞安全威胁库、设备指纹库、攻击组织/个人库、反诈骗电话库 …

杜绝黑客欺诈 品牌保净化网络环境



全网无死角展示您的品牌

展示广

多渠道、全方位展示；覆盖 9亿网民、91%流量入口

QQ	腾讯手机管家	搜狗搜索	搜狗号码通	QQ浏览器	QQ手机浏览器	搜狗浏览器	品牌宝信誉微站
8.3亿用户	4亿用户	日覆盖2.5亿用户	7000万用户	29%市场占有率	35%市场占有率	47%市场占有率	日均1300万次查询

knownsec

知道创宇云安全