一 洞 观 全 球

通过心脏出血漏洞修复速度
反映各国网络战的防御能力

KNOWNSEC
知 道 安 全

1 漏洞说明

2 漏洞影响态势

3 漏洞修复态势

4 ZoomEye平台架构

KNOWNSEC
知 道 安 全

1
漏洞说明

历史上第一个上央视的漏洞

KNOWNSEC
知 道 安 全

历史上第一个上央视的漏洞

KNOWNSEC
知 道 安 全

漏洞

SSL，全称Secure Socket Layer，用以保障在Internet上数据传输之安全，利用数据加密技术，确保数据在网络上之传输过程中不会被截取及窃听。

互联网上多数SSL加密都使用名为OpenSSL的开源软件包。由于OpenSSL的源代码中存在一个漏洞，可以让攻击者获得服务器上64K内存中的数据内容。这部分数据中，可能存有安全证书、用户名与密码、聊天工具的消息、电子邮件以及重要的商业文档等数据。

漏洞

因为该漏洞的危害巨大，影响面很广，非常严重，犹如广大用户在互联网上的钥匙被偷窃，因此该漏洞被喻为"心脏出血"漏洞。

Google

淘宝网 Taobao.com

facebook

微信

twitter

YAHOO!

KNOWNSEC 知道安全

漏洞

受影响服务：

443端口	HTTPS服务
465端口	SMTP(SSL)服务
993端口	IMAP4(SSL)服务
995端口	POP3(SSL)服务
1194端口	VPN服务
……	……

淘宝

```
21c0: 37 25 32 46 37 62 78 25 32 42 37 48 38 37 71 37  7%2F7bx%2B7H87q7
21d0: 33 34 71 54 72 74 4F 53 69 25 32 42 76 47 76 37  34qTrtOSi%2BvGv7
21e0: 4F 61 6E 36 76 36 68 37 36 7A 30 76 65 58 75 75  Oan6v6h76z0veXuu
21f0: 50 7A 71 71 76 50 75 72 66 25 32 42 68 35 61 54  PzqqvPurf%2Bh5aT
2200: 68 39 4C 25 32 46 6D 25 32 42 61 58 39 25 32 46  h9L%2Fm%2BaX9%2F
2210: 4C 62 6B 75 76 36 25 32 46 25 32 42 65 71 68 25  Lbkuv6%2F%2Beqh%
2220: 32 42 4F 25 32 42 79 38 66 47 76 39 62 50 32 71  2BO%2By8fGv9bP2q
2230: 25 32 42 62 31 76 75 66 77 72 75 72 71 74 4F 61  %2Bb1vufwrurqtOa
2240: 6E 25 32 46 71 4C 37 37 4C 6E 25 32 46 39 62 54  n%2FqL77Ln%2F9bT
2250: 35 37 4C 50 39 76 75 65 6E 25 32 46 25 32 46 53  57LP9vuen%2F%2FS
2260: 69 35 50 65 33 37 76 4F 77 34 62 25 32 46 37 75  i5Pe37vOw4b%2F7u
2270: 76 37 72 30 51 25 33 44 25 33 44 26 54 50 4C 5F  v7r0Q%3D%3D&TPL_
2280: 75 73 65 72 6E 61 6D 65 3D 62 72 61 64 65 63 61  username=bradeca
2290: 6F 26 54 50 4C 5F 70 61 73 73 77 6F 72 64 3D 36  o&TPL_password=[redacted]
22a0: 33 36 30 37 39 35 6D 65 6E 67 63 61 6F 26 54 50  [redacted]&TP
22b0: 4C 5F 63 68 65 63 6B 63 6F 64 65 3D 6B 75 34 62  L_checkcode=ku4b
```

KNOWNSEC
知 道 安 全

淘宝

KNOWNSEC
知 道 安 全

支付宝

KNOWNSEC
知 道 安 全

12306铁道购票系统

user_name=[redacted]547&userDTO.pass
word=zhac[redacted]325&confirmPa
ssWord=zha[redacted]325&userDT
O.IVR_passwd=[redacted]&confirmIvr_pwd
=[redacted]&userDTO.pwd_question=您的
大学校名是?
&otherpasswordQuestion=&userDTO.pw
d_answer=北京吉利大学
^E^E^E^E^E^E049750004101775011830
31550042&train_location=B2&_json_att
=&REPEAT_SUBMIT_TOKEN=1e23ac3f
d0630836c67aad1dde869ca7

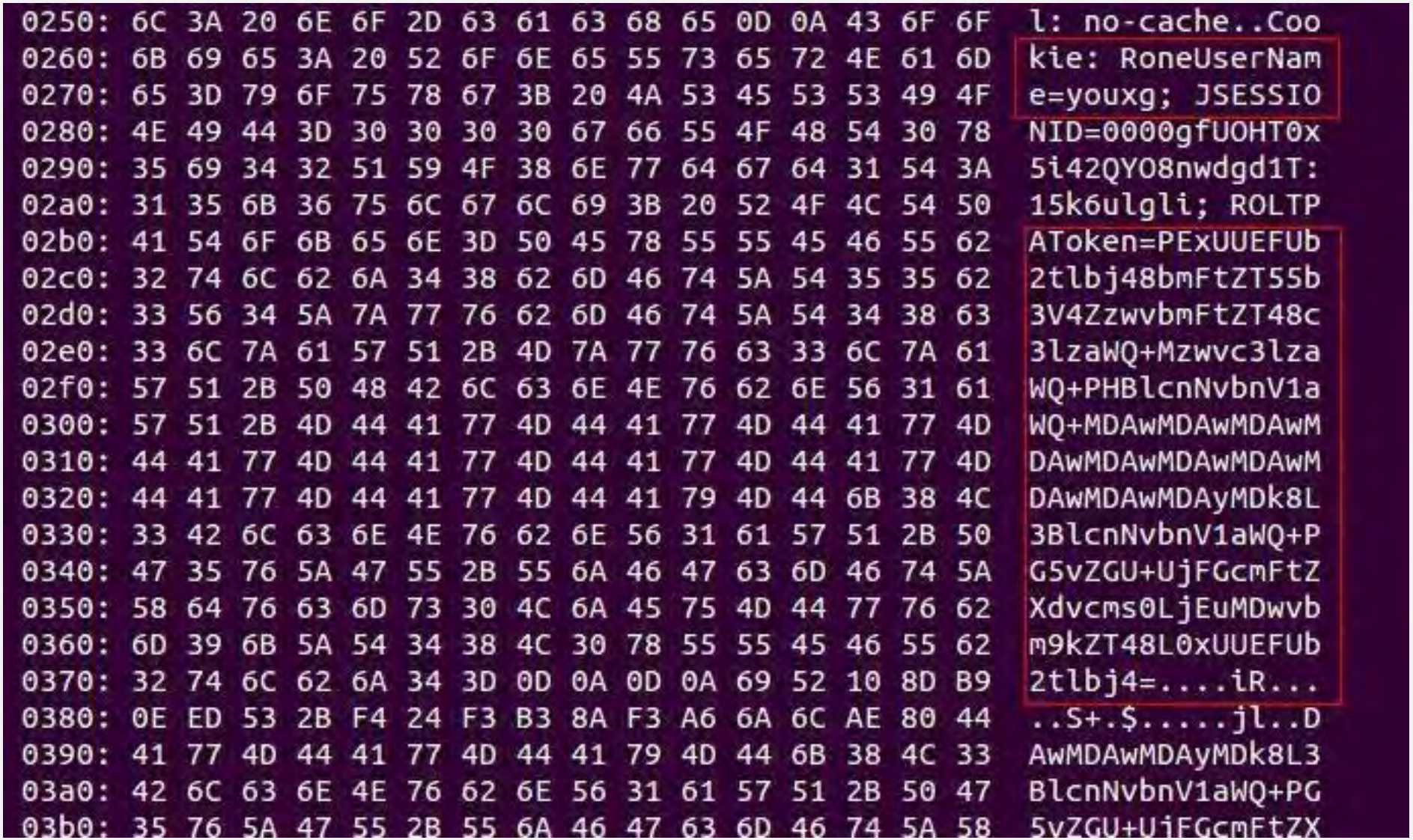
KNOWNSEC
知 道 安 全

陌陌

```
-----------------------------7da2137580612--^M
Tawêòô¦þ<8f>Å]>&<92>^A´<9c>×7<91>n: form-data; name="version"^M
^M
7^M
-----------------------------7da2137580612--^M
È <81>K²6ÐÞóö<S<89><9c>xW^_^BÌÎntent-Disposition: form-data; nam
^M
1396957268^M
-----------------------------7da2137580612^M
Content-Disposition: form-data; name="pos"^M
^M
2^M
-----------------------------7da2137580612--^M
/D^Yx^?Ö¿0øë^\<81>|f^OÃ<91>Ë<9b>À----------------7da2137580612^M
Content-Disposition: form-data; name="social"^M
^M
0^M
-----------------------------7da2137580612^M
Content-Disposition: form-data; name="loctype"^M
^M
0^M
-----------------------------7da2137580612^M
Content-Disposition: form-data; name="agerange"^M
^M
0^M
-----------------------------7da2137580612^M
Content-Disposition: form-data; name="activetime"^M
^M
15^M
-----------------------------7da2137580612^M
Content-Disposition: form-data; name="lng"^M
^M
107.5541336^M
```

163邮箱

网神VPN


0250: 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D 0A 43 6F 6F l: no-cache..Coo
0260: 6B 69 65 3A 20 52 6F 6E 65 55 73 65 72 4E 61 6D kie: RoneUserNam
0270: 65 3D 79 6F 75 78 67 3B 20 4A 53 45 53 53 49 4F e=youxg; JSESSIO
0280: 4E 49 44 3D 30 30 30 30 67 66 55 4F 48 54 30 78 NID=0000gfUOHT0x
0290: 35 69 34 32 51 59 4F 38 6E 77 64 67 64 31 54 3A 5i42QYO8nwdgd1T:
02a0: 31 35 6B 36 75 6C 67 6C 69 3B 20 52 4F 4C 54 50 15k6ulgli; ROLTP
02b0: 41 54 6F 6B 65 6E 3D 50 45 78 55 55 45 46 55 62 AToken=PExUUEFUb
02c0: 32 74 6C 62 6A 34 38 62 6D 46 74 5A 54 35 35 62 2tlbj48bmFtZT55b
02d0: 33 56 34 5A 7A 77 76 62 6D 46 74 5A 54 34 38 63 3V4ZzwvbmFtZT48c
02e0: 33 6C 7A 61 57 51 2B 4D 7A 77 76 63 33 6C 7A 61 3lzaWQ+Mzwvc3lza
02f0: 57 51 2B 50 48 42 6C 63 6E 4E 76 62 6E 56 31 61 WQ+PHBlcnNvbnV1a
0300: 57 51 2B 4D 44 41 77 4D 44 41 77 4D 44 41 77 4D WQ+MDAwMDAwMDAwM
0310: 44 41 77 4D 44 41 77 4D 44 41 77 4D 44 41 77 4D DAwMDAwMDAwMDAwM
0320: 44 41 77 4D 44 41 77 4D 44 41 79 4D 44 6B 38 4C DAwMDAwMDAyMDk8L
0330: 33 42 6C 63 6E 4E 76 62 6E 56 31 61 57 51 2B 50 3BlcnNvbnV1aWQ+P
0340: 47 35 76 5A 47 55 2B 55 6A 46 47 63 6D 46 74 5A G5vZGU+UjFGcmFtZ
0350: 58 64 76 63 6D 73 30 4C 6A 45 75 4D 44 77 76 62 Xdvcms0LjEuMDwvb
0360: 6D 39 6B 5A 54 34 38 4C 30 78 55 55 45 46 55 62 m9kZT48L0xUUEFUb
0370: 32 74 6C 62 6A 34 3D 0D 0A 0D 0A 69 52 10 8D B9 2tlbj4=....iR...
0380: 0E ED 53 2B F4 24 F3 B3 8A F3 A6 6A 6C AE 80 44 ..S+.$.....jl..D
0390: 41 77 4D 44 41 77 4D 44 41 79 4D 44 6B 38 4C 33 AwMDAwMDAyMDk8L3
03a0: 42 6C 63 6E 4E 76 62 6E 56 31 61 57 51 2B 50 47 BlcnNvbnV1aWQ+PG
03b0: 35 76 5A 47 55 2B 55 6A 46 47 63 6D 46 74 5A 58 5vZGU+UjFGcmFtZX

中华电信hinet邮箱

1	用户名	密码
2963	jaki.cpu	[redacted]
2964	jamehou	[redacted]
2965	james45.lee	[redacted]
2966	james.bk3689	[redacted]
2967	james.frun	[redacted]
2968	james.lorenz	[redacted]
2969	jameswa	[redacted]
2970	jamin.nee	[redacted]
2971	jan1121	[redacted]
2972	jan97322	[redacted]
2973	jane.kelly	[redacted]
2974	janelee.puzco	[redacted]
2975	janelu	[redacted]
2976	jane.one	[redacted]
2977	janes.judy	[redacted]
2978	janet104	[redacted]
2979	janet99.lu	[redacted]
2980	janet.jaja	[redacted]
2981	janewei	[redacted]
2982	janeyiru	[redacted]
2983	jang.dt	[redacted]
2984	jang.hsin	[redacted]
2985	jangshin	[redacted]
2986	jang.yicheng	[redacted]
2987	janice.t48	[redacted]
2988	jan.minj	[redacted]

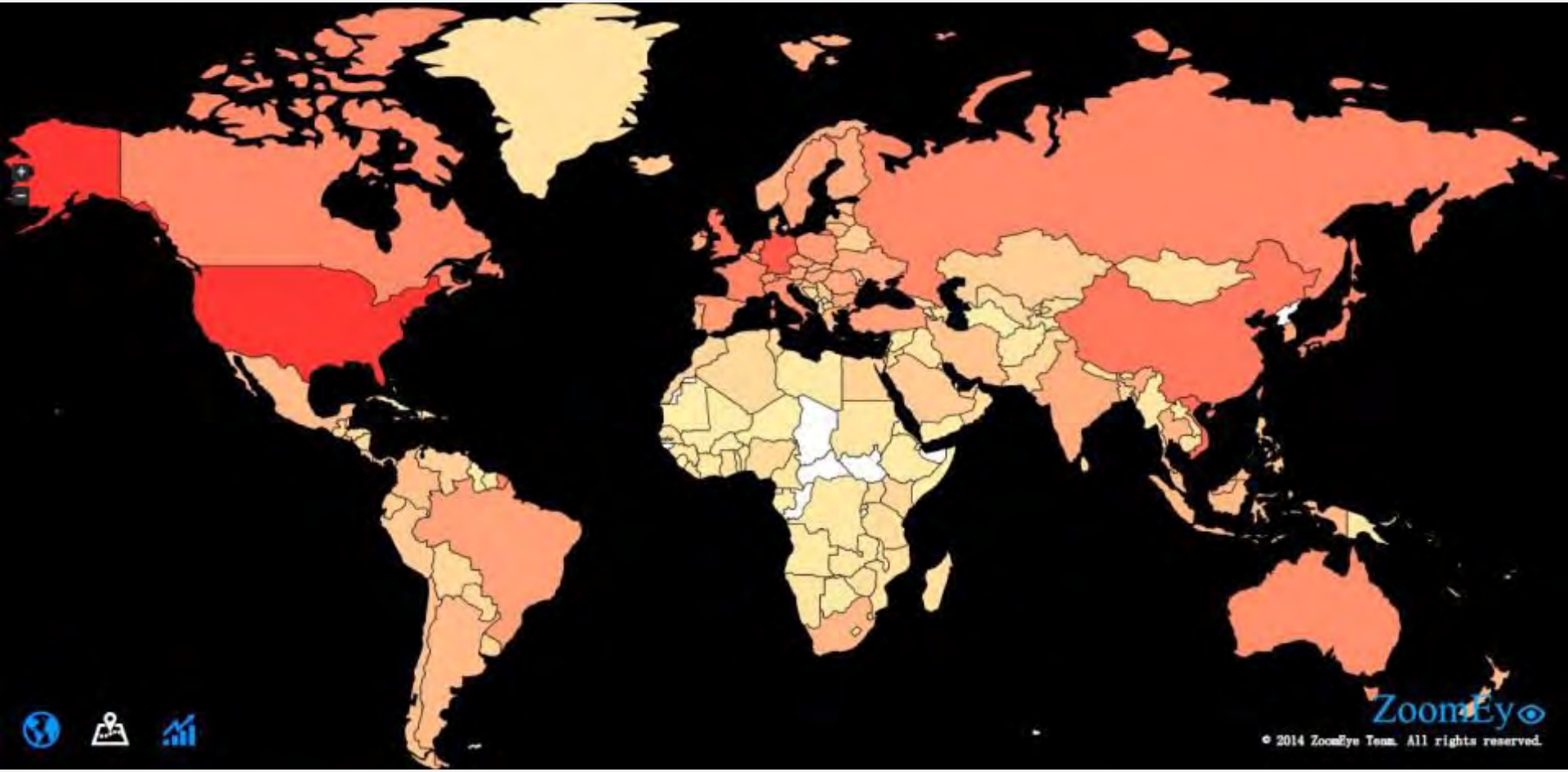
BUDGET VM

```
10977  Referer: https://master.scalableDNS.com/home.php
10978  Accept-Encoding: gzip,deflate,sdch
10979  Accept-Language: zh-CN,zh;q=0.8
10980  Cookie: PHPSESSID=g7b91ojstf31f97jp8g01hc5kb6lc5a1; passone=%2BHQaJjoXL0
       passtwo=QgcdUDIIeziwOND%2FRiqpkCqu
10981  AlexaToolbar-ALX_NS_PH: AlexaToolbar/alxg-3.2
10982
10983  ¹fbËíCANi@DC4hRSAl4b^}SOHðACKBELBELBELBELBELBELBELBELmgCvc69CJUIhs; p
10984  AlexaToolbar-ALX_NS_PH: AlexaToolbar/alxg-3.2
10985
10986  act=login&Submit=1&username=vmuser13877&password=%24y[redacted]%25etaETB
       EOTEOT92TxiHVUQq4CngEHan5rT2esiYxzdrqT4qUBj3rf83bH8bpU6Xe%2FUYyYPjoB97vp
       hZgfbJRyQrQ21jOEp5coxyf4Q0SBuAlNjGJMpviyh4GBhEF2H9lUXYi%2
       Fy4HXjZ8QXoo9Q6zQxpM2h7%2FNBruk1UV4fYFOl8TPCoSWdqr%2FiF6G4q0cwByidMRz9pw
10987  Connection: keep-alive
10988  Pragma: no-cache
10989  Cache-Control: no-cache
```

KNOWNSEC
知 道 安 全

2
漏洞影响态势

全球态势



全球受影响的公网IP共计：2,433,550

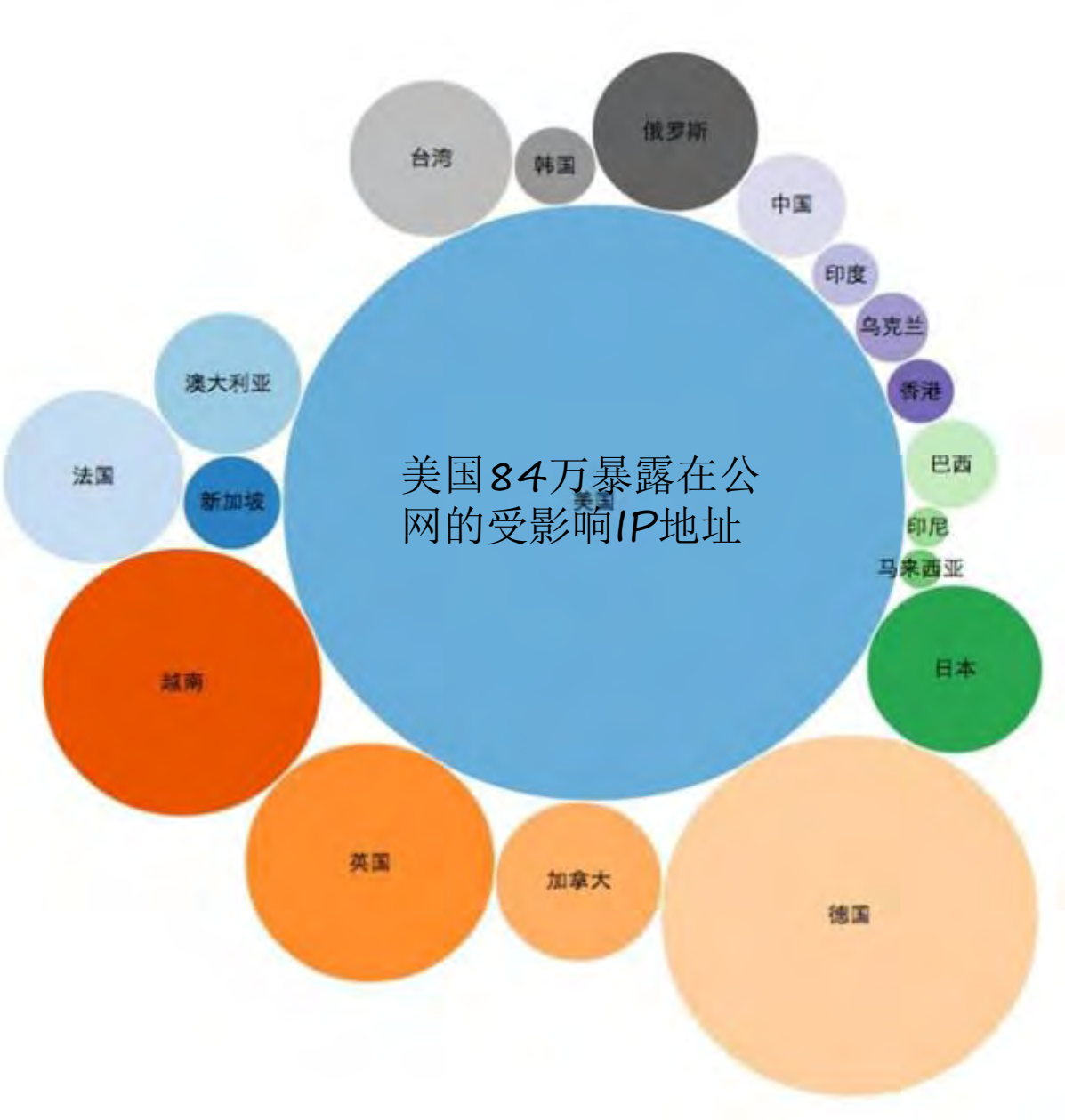
KNOWNSEC
知 道 安 全

全球可打击对象暴露面TOP35

美国	838526
德国	309303
越南	170235
英国	136075
荷兰	84627
法国	71975
日本	67458
俄罗斯	60629
加拿大	60608
台湾	58770
澳大利亚	48012
意大利	45247
瑞士	31814
波兰	27975
西班牙	27159
中国	26621
捷克	24259
新加坡	21408

KNOWNSEC
知 道 安 全

中国周边和欧美20个地区可打击暴露面



美国	838526
德国	309303
越南	170235
英国	136075
法国	71975
日本	67458
俄罗斯	60629
加拿大	60608
台湾	58770
澳大利亚	48012
中国	26621
新加坡	21408
巴西	19545
韩国	14965
乌克兰	12207
香港	10358
印度	10193
印尼	4325
马来西亚	4081
菲律宾	1715

KNOWNSEC
知 道 安 全

思考

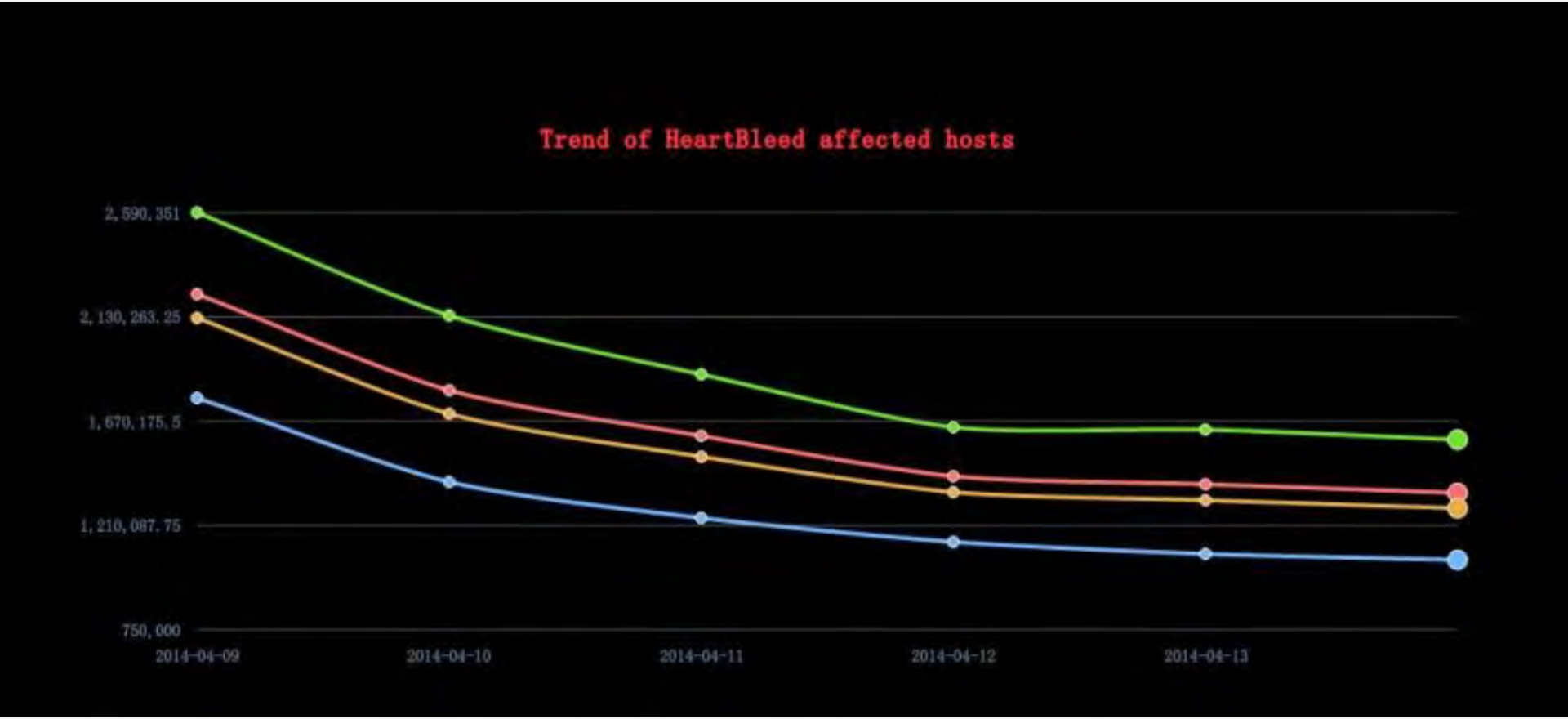
中国在网络空间上的重要资产数量，远低于其他国家，重要信息系统不发达，与国际地位不相符合。

国家需要大力发展信息网络时代的基础建设

数据显示，美国占全球34%，中国仅占1%

3
漏洞修复态势

一个星期内全球修复趋势图



受影响的HTTPS、邮件系统等协议端口，一周的修复趋势

KNOWNSEC
知 道 安 全

中国周边和欧美20个国家修复率

国家	第一天	第三天	修复率
新加坡	21408	9173	57%
美国	838526	429473	49%
澳大利亚	48012	25940	46%
法国	71975	39607	45%
越南	170235	97732	43%
英国	136075	79152	42%
加拿大	60608	36363	40%
德国	309303	199831	35%
日本	67458	45547	32%
马来西亚	4081	3078	25%
印尼	4325	3309	23%
巴西	19545	15089	23%
香港	10358	8182	21%
乌克兰	12207	9862	19%
印度	10193	8306	19%
中国	26621	21794	18%
菲律宾	1715	1426	17%
俄罗斯	60629	50770	16%
韩国	14965	13791	8%
台湾	58770	55064	6%
全球	2433550	1468022	40%

KNOWNSEC
知 道 安 全

一个星期内全球修复趋势图

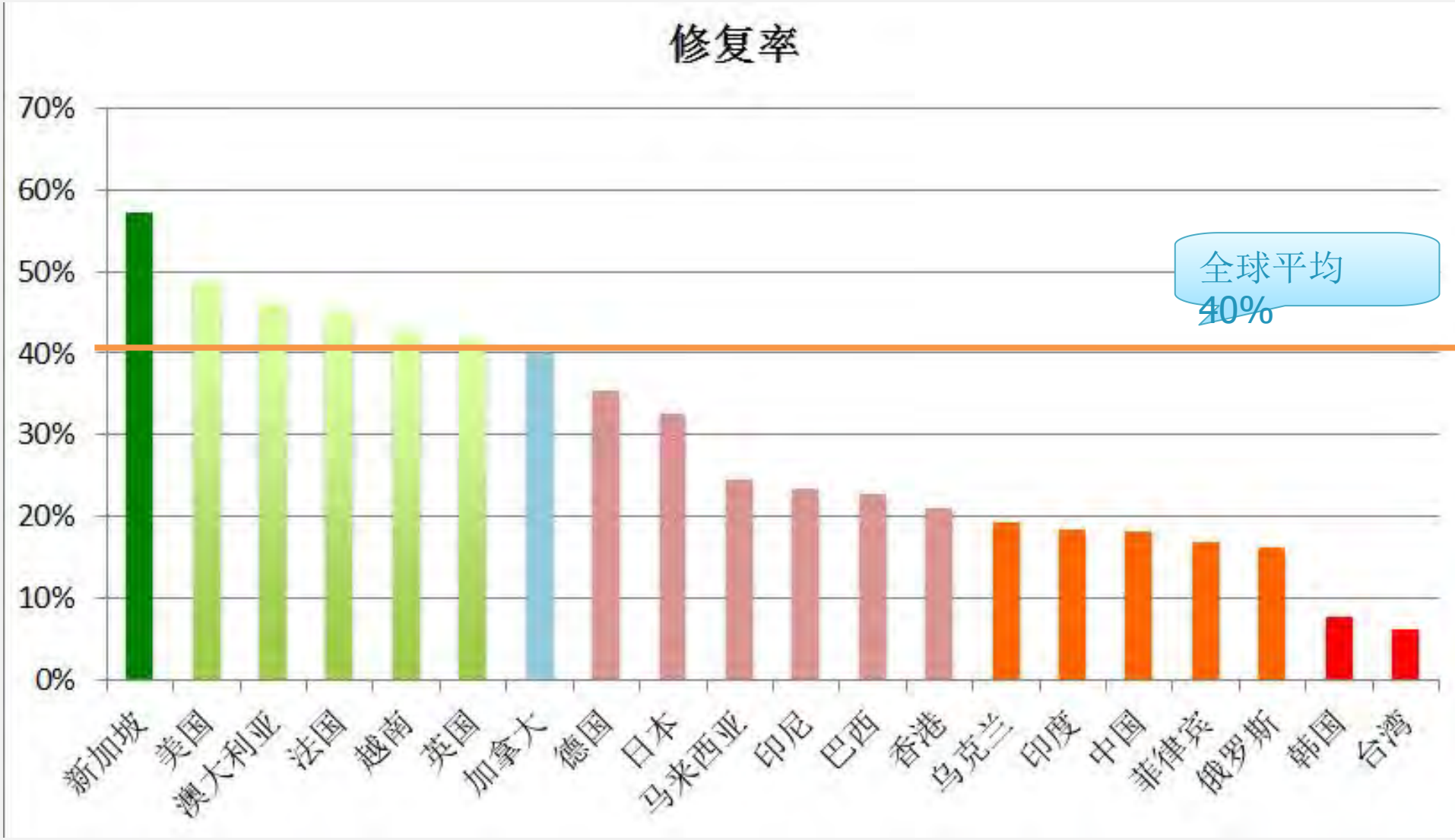
将第一天与第三天的受漏洞影响数量相比较
全球平均修复率40%

新加坡	**57%**	中国	**18%**
美国	**49%**	韩国	**8%**
越南	**43%**	台湾	**6%**

中国全球排名102

KNOWNSEC
知 道 安 全

三天内，周边和欧美20个国家修复率



TIPS：第一天修复最快的信息系统

美国

众议院常设委员会
美国联邦贸易委员会
美国联邦数据库
美国军事装备提供商
汉考克控股银行
德意志银行
woodland银行
lakeside银行

- 列克星敦电力和照明(lexington power&light)
- 电力监控厂商(electricity monitors)
- 电力和天然气厂商
- 石油装备商和服务公司(balch)
- 石油运输公司(Timms)
- 石油供应商和销售商公司(Jacobs)
- 光纤提供商(fiberguide)
- 电信服务商(Viper)
- 奥斯汀地区电信网络
- 电信解决方案提供商(personaloffice)
- 电信业务提供商(INFOSTRUCTURE)
- 长途电话和电信网络运营商(i2Gemini)

TIPS：第一天修复最快的信息系统

台湾

高雄市政[illegible]科技大学网络认证系统
高雄市立[illegible]大学网络认证系统
教育機構[illegible]系统
建国科技大学VPN系统
中華電信h[illegible]PN系统
中華電信h[illegible]

TIPS：第一天修复最快的信息系统

日本

衆議院議員
独立行政法人海上技术安全研究所
自民党-京都府支部联合会
航海训练所

日本sunoco石油公司
日本kohan kogyo钢鈑工業公司
総研[illegible]公司（从事电气通信等工事）
[illegible]占赛马会

大東銀行
日本注册会计师协会

筑波大学
大阪大学
山梨大学
横滨国立大学

思考

中国在抵御重要网络威胁、应急重要网络事件时，速度远远落后于其他国家。

危害如此大的漏洞，美国在第三天的修复率高达49%，而中国的修复率仅仅18%。如果未来发生国家级别的网络战，中国现有的网络安全思维和安全防御能力，如何应对？

思考

重要信息系统欠发达

重视信息时代的网络建设

加快网络基础设施建设

提升网络信息化的利用程度

网络安全防御能力很弱

重视网络安全，提高安全意识

提升应急响应能力

提高整体安全防御能力

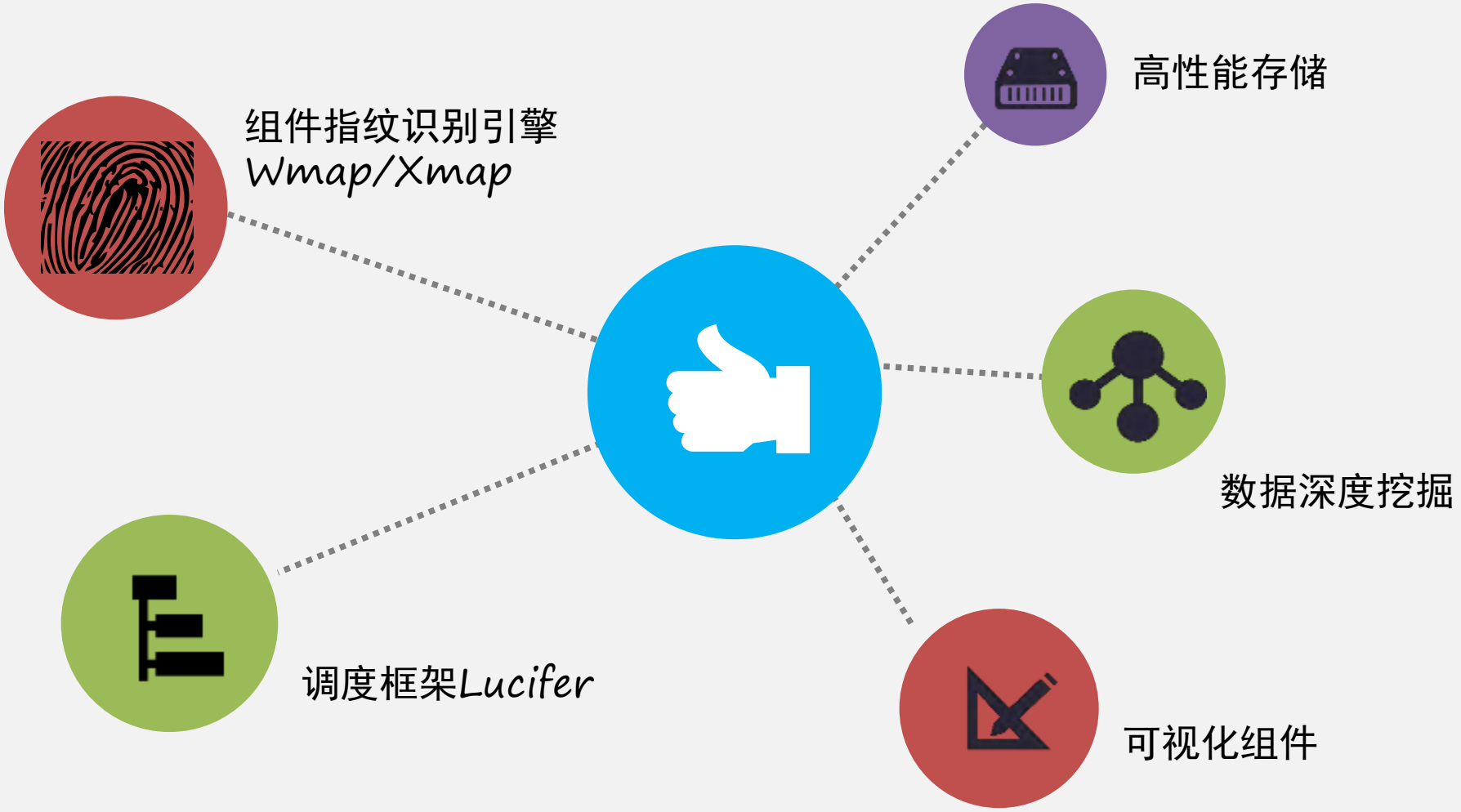
4

ZoomEye平台架构

基础平台

ZoomEye

KNOWNSEC
知 道 安 全



组件指纹识别引擎 Wmap/Xmap

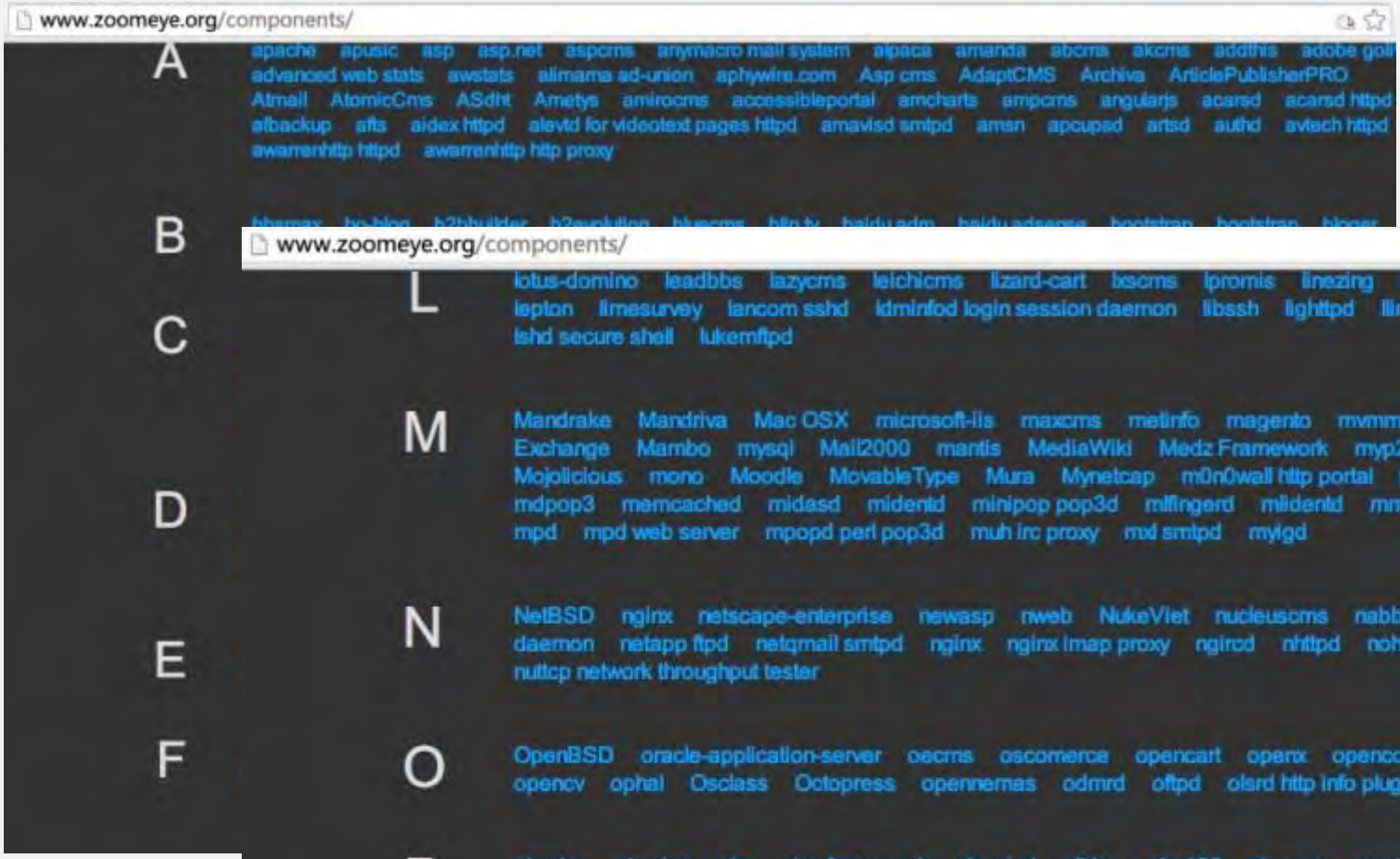
识别网络设备厂商和型号

- 交换机
- 路由器
- 摄像头
- 平板电脑
- 工控设备
- 核工业设备
- ……

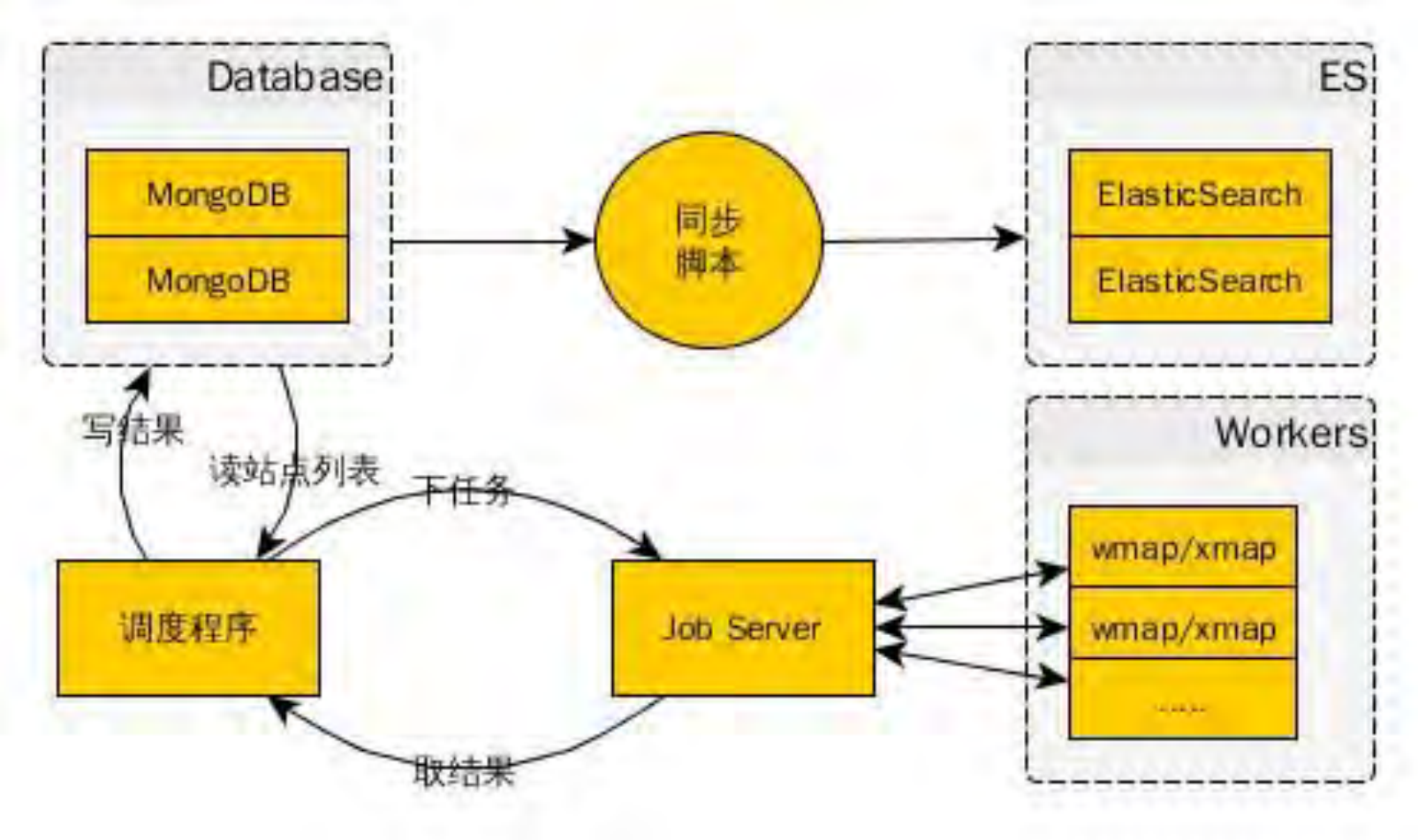
组件指纹识别引擎 Wmap/Xmap

识别WEB服务组件

组件指纹识别引擎 Wmap/Xmap



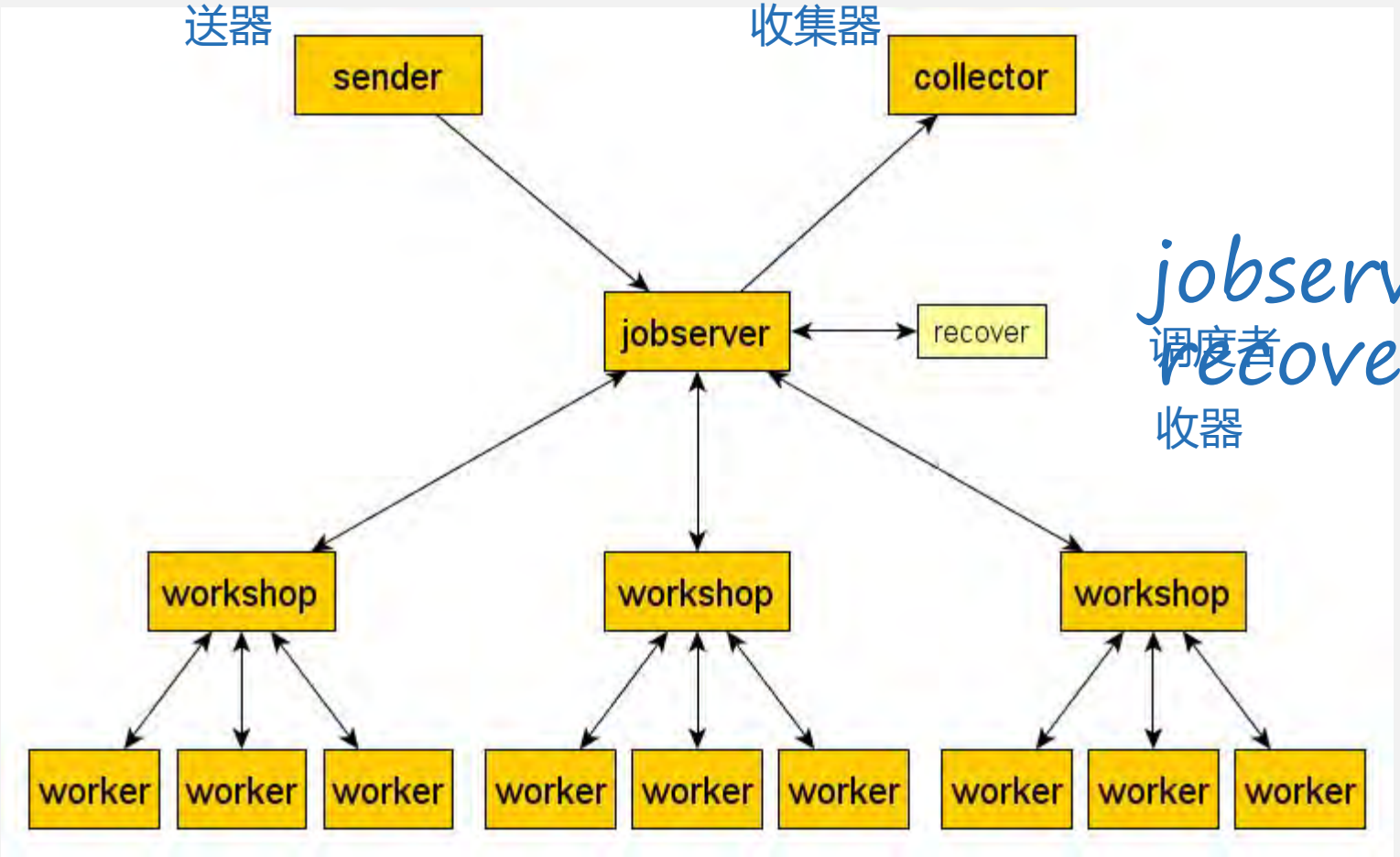
调度框架 Lucifer



调度框架 Lucifer

sender 发送器

collector 收集器



jobserver 作业调度者

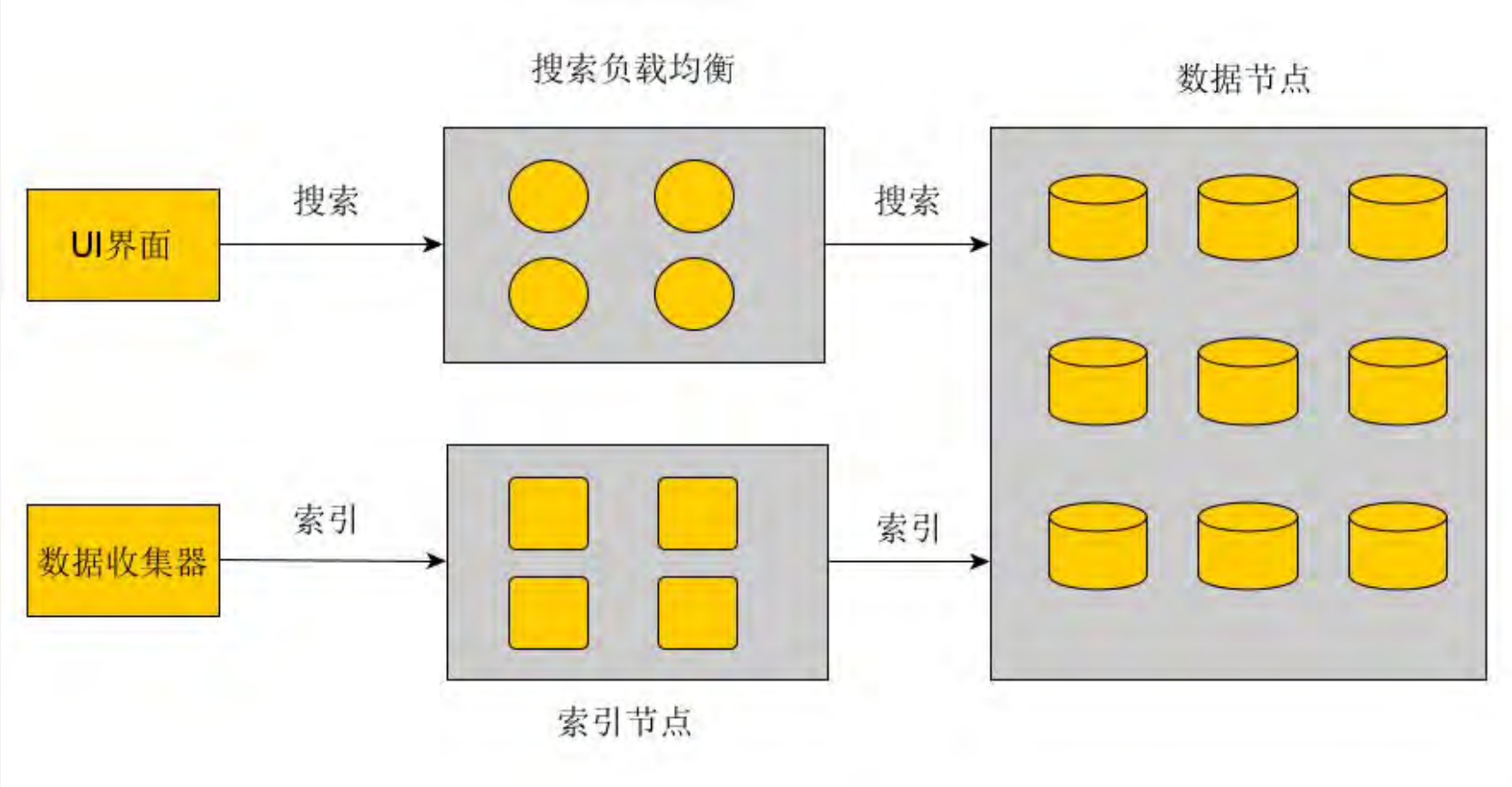
recover 回收器

worksho

worker 工人

高性能存储集群

“搜索负载均衡”，负责接收“UI界面”的搜索请求，并向“数据节点”发送搜索请求。

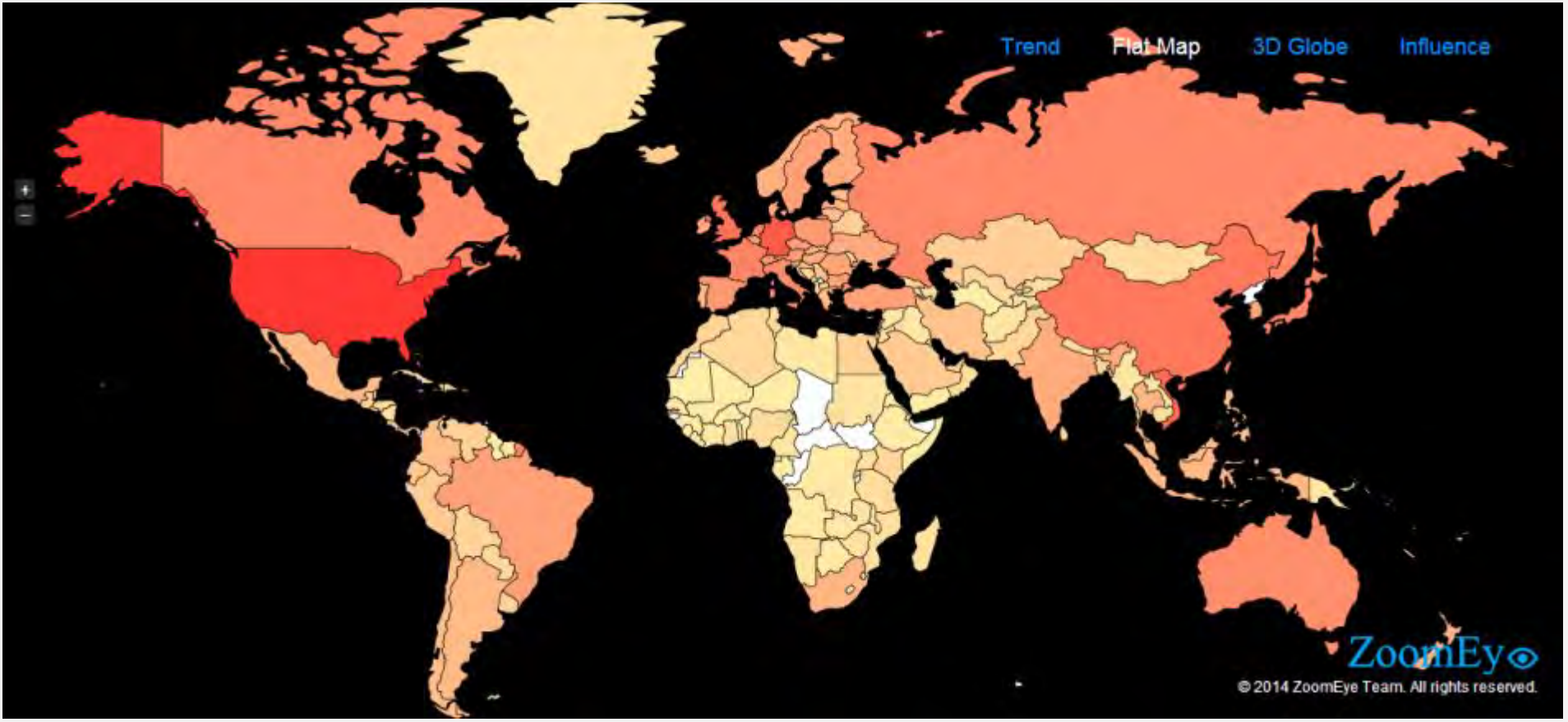


“索引节点”，负责收集索引请求，并向“数据节点”发送索引请求。

可视化

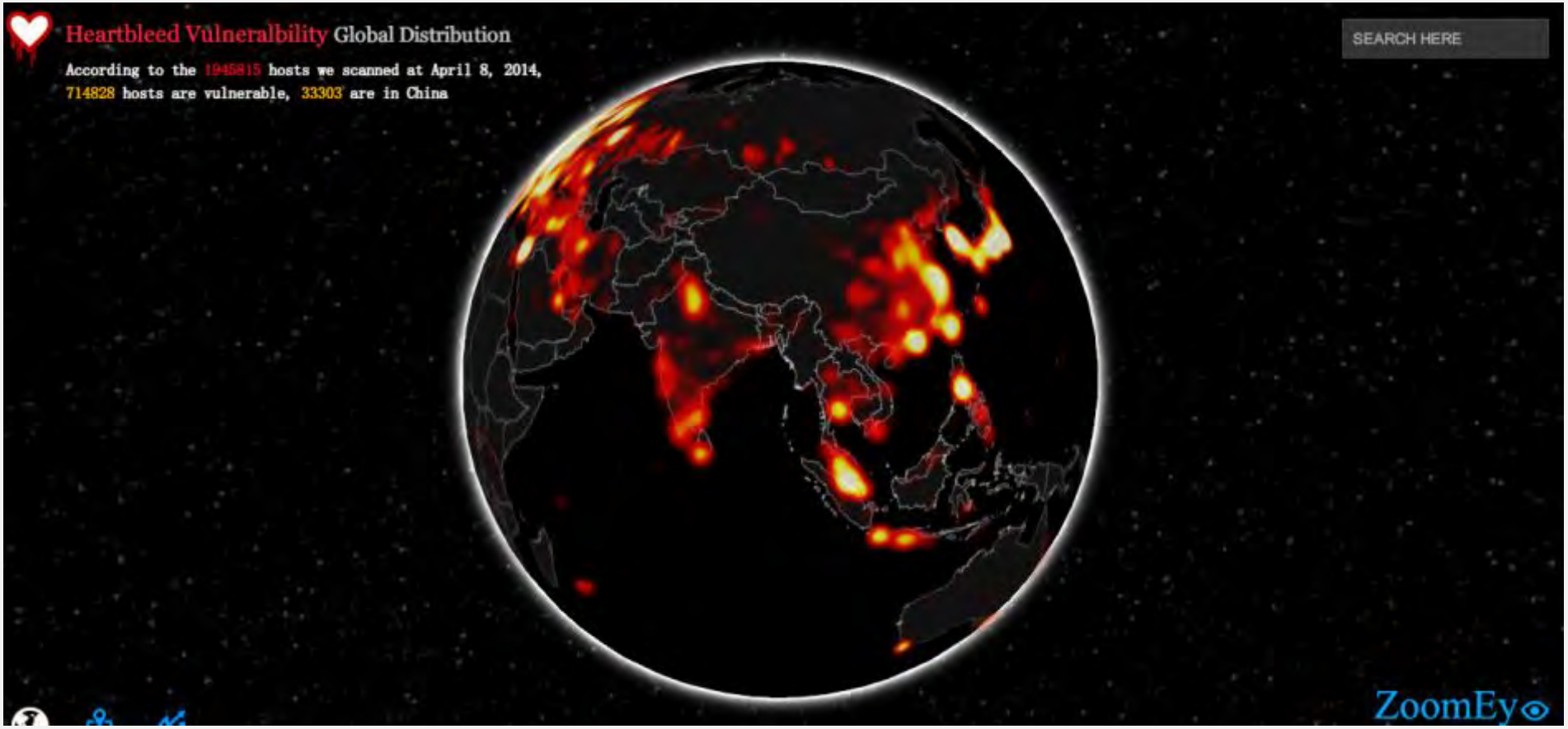
UI很重要

可视化



基于jVectorMap的2D矢量图

可视化



基于WebGL的3d渲染

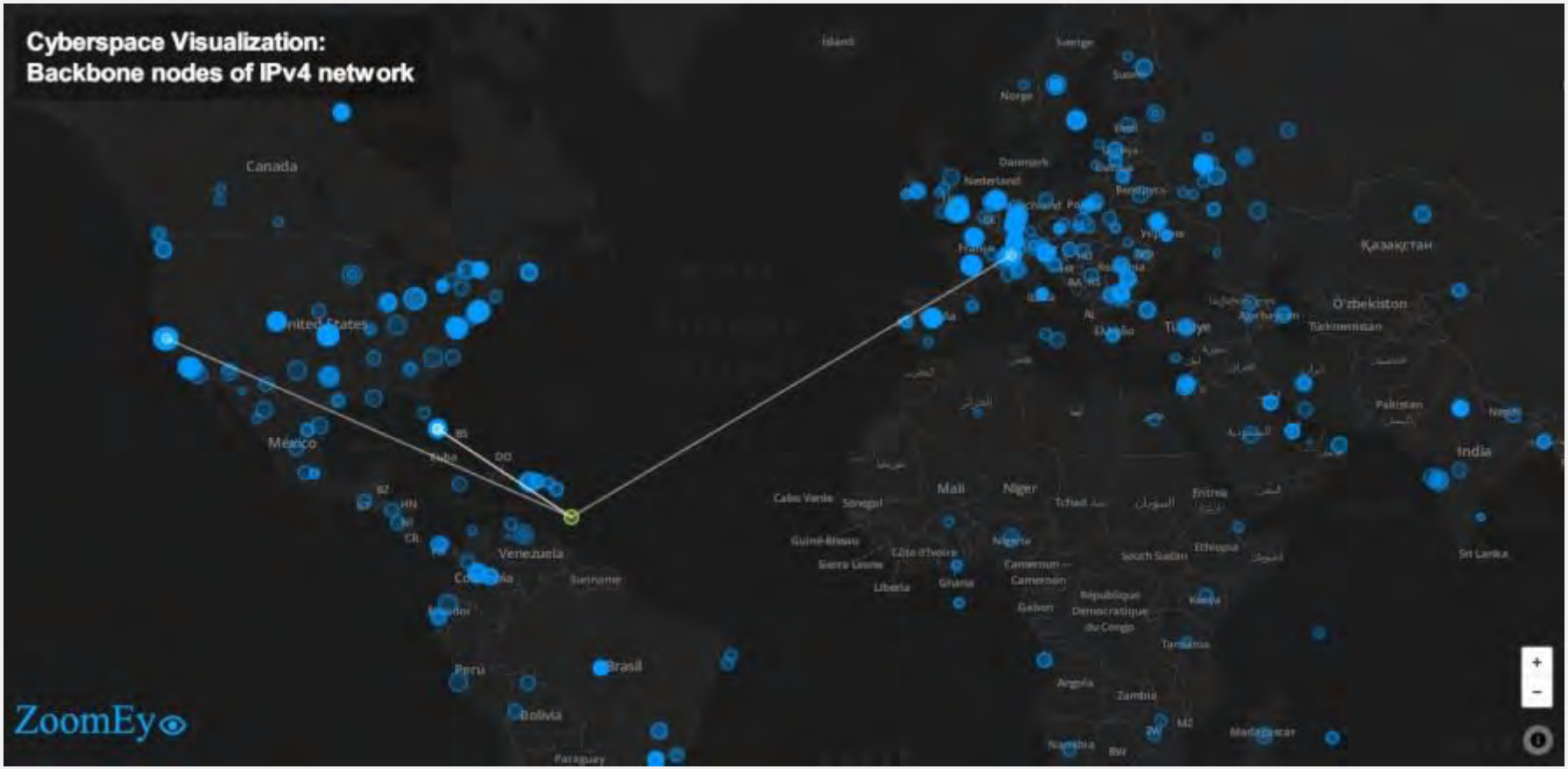
KNOWNSEC
知 道 安 全

可视化

基于 WebGL，无需额外客户端插件，良好的跨平台性。
支持10万级地理坐标的实时渲染，操作流畅。

KNOWNSEC
知 道 安 全

可视化



基于Leaflet.js的交互式地图

精确到街道级别的地理数据，凸显节点之间的关系。

KNOWNSEC
知 道 安 全

谢 谢 ！

KNOWNSEC
知 道 安 全