

心脏出血漏洞一周年

一个漏洞看全球各国网络危机应急能力



知道创宇：杨冀龙

1 漏洞说明



2 漏洞影响态势

3 漏洞修复态势

1 漏洞说明

说明：以下截图来自互联网



KNOWNSEC
知道 创 宇

历史上第一个上央视的漏洞



历史上第一个上央视的漏洞



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。



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

.....

.....


```

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 34qTrt0Si%2BvGv7
21e0: 4F 61 6E 36 76 36 68 37 36 7A 30 76 65 58 75 75 0an6v6h76z0veXuu
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 2B0%2By8fgv9bP2q
2230: 25 32 42 62 31 76 75 66 77 72 75 72 71 74 4F 61 %2Bb1vufwrurqt0a
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=
22a0: 33 36 30 37 39 35 6D 65 6E 67 63 61 6F 26 54 50 
22b0: 4C 5F 63 68 65 63 6B 63 6F 64 65 3D 6B 75 34 62 L_checkcode=ku4b
  
```

```

0640: 74 6F 25 33 44 30 3B 20 6C 3D 25 45 35 25 42 39 to%3D0; l=%E5%B9
0650: 25 42 38 25 45 37 25 41 36 25 38 46 25 45 38 25 %B8%E7%A6%8F%E8%
0660: 39 42 25 38 37 25 45 35 25 41 45 25 39 44 25 45 9B%87%E5%AE%9D%E
0670: 35 25 41 45 25 39 44 38 3A 3A 31 33 39 36 35 33 5%AE%9D8::139653
0680: 30 31 35 30 37 32 37 3A 3A 31 31 3B 20 6D 74 3D 0150727::11; mt=
0690: 63 70 3D 30 26 63 69 3D 35 5F 31 26 63 79 6B 3D cp=0&ci=5_1&cyk=
06a0: 31 5F 31 3B 20 6C 7A 73 74 61 74 5F 75 76 3D 32 l_1; lzstat_uv=2
06b0: 34 30 35 39 38 35 32 37 39 32 32 35 31 35 36 33 4059852792251563
06c0: 32 34 30 7C 31 38 31 33 37 38 34 40 33 32 32 35 240|1813784@3225
06d0: 37 31 35 3B 20 63 6F 6F 6B 69 65 32 3D 35 32 35 715; cookie.=525
06e0: 64 62 37 38 62 31 62 63 65 37 37 38 64 39 64 62 db78b1bce778d9db
06f0: 34 64 31 36 64 62 39 31 61 61 32 63 33 3B 20 75 4d16db91aa2c3; u
0700: 63 31 3D 63 6F 6F 6B 69 65 31 34 3D 55 6F 4C 56 c1=cookie14=UoLV
0710: 59 79 76 61 5A 4D 45 72 56 51 25 33 44 25 33 44 YyvaZMERVQ%3D%3D
0720: 3B 20 76 3D 30 3B 20 5F 74 62 5F 74 6F 6B 65 6E ; v=0; _tb_token
0730: 5F 3D 50 36 77 71 4B 65 66 34 52 66 49 59 0D 0A _=P6wqKef4RfIY..
0740: 0D 0A 7D F1 96 29 96 36 16 DB 27 16 F1 AF A4 0F ..},..).6..',.....
0750: D5 55 68 84 33 23 3D 30 5F 31 26 63 79 6B 3D 30 .Uh,3#=0_1&cyk=0
0760: 5F 30 3B 20 5F 63 63 5F 3D 56 71 38 6C 25 32 42 _0; _cc_=Vq8l%2B
0770: 4B 43 4C 69 77 25 33 44 25 33 44 3B 20 74 67 3D KCLiw%3D%3D; tg=
0780: 30 3B 20 63 6E 61 3D 6B 57 6D 66 43 33 64 75 6F 0; cna=kWmfC3duo
0790: 79 30 43 41 64 37 52 62 33 6B 58 30 46 52 47 3B y0CAd7Rb3kX0FRG;
07a0: 20 6C 3D 25 45 35 25 42 37 25 39 44 25 45 35 25 l=%E5%B7%9D%E5%
07b0: 38 43 25 39 37 25 45 35 25 39 30 25 38 44 25 45 8C%97%E5%90%8D%E
07c0: 35 25 38 43 25 42 42 3A 3A 31 33 39 36 39 34 30 5%8C%BB::1396940
07d0: 30 32 35 31 38 34 3A 3A 31 31 3B 20 75 63 33 3D 025184::11; uc3=
07e0: 6E 6B 32 3D 26 69 64 32 3D 26 6C 67 32 3D 3B 20 nk2=&id2=&lq2=;
07f0: 61 6C 69 5F 61 62 3D 32 32 32 2E 32 30 39 2E 31 ali_ab=222.209.1
0800: 31 31 2E 31 32 31 2E 31 33 39 34 31 35 38 35 39 11.121.139415859
0810: 36 39 38 36 2E 31 3B 20 5F 5F 75 74 6D 61 3D 31 6986.1; utma=1

```


支付宝

```
alipay$ ./poc;./poc2
{"id":0,"memo":"操作成功","result":{"bindCard":false,"currentProductVersion":"8.0.0.0110","customerType":"2","existNewVersion":"0","extResAttrs":{},"extern_token":
,"headImg":"https://tfsimg.alipay.com/images/partner/TlecVaXl0XXXXXXXXXX","isCertified":"Y","loginId":
om","loginServerTime":"2014-
","loginToken":
","memo":"操作成功。","mobileNo":"1
","resultStatus":1000,"sessionId":
","userId":
","userName":
","wi
relessUser":false},"resultStatus":1000}
{"id":0,"memo":"操作成功","result":{"accountHomeAsset":{"freezed":false,"hidden":false,"mark":false,"opText":"0.75元"},"bankHomeAsset":{"bankCardCount":
,"freezed":false,"hidden":false,"mark":false,"opText":"共
张"},"bollywoodHomeAsset":{"freezed":false,"hidden":true,"mark":false},
"charityHomeAsset":{"freezed":false,"hidden":false,"mark":false},
"fixedHomeAsset":{"freezed":false,"hasSignedFixed":false,"hidden":true,"mark":false},
"fundHomeAsset":{"freezed":false,"hasFundAccount":true,"hidden":false,"mark":true,"opText":"昨日收益：
元"},
"pcreditHomeAsset":{"freezed":false,
```



12306铁道购票系统

```
user_name=[REDACTED]547&userDTO.pass  
word=zha[REDACTED]325&confirmPa  
ssWord=zha[REDACTED]325&userDT  
O.IVR_passwd=[REDACTED]&confirmlvr_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^E04975000410177501183  
031550042&train_location=B2&_json_att  
=&REPEAT_SUBMIT_TOKEN=1e23ac3f  
d0630836c67aad1dde869ca7
```



```
-----7da2137580612--^M
Tawêôô|p<8f>Ä]>&<92>^A'<9c>x7<91>n: form-data; name="version"^M
^M
7^M
-----7da2137580612--^M
Ë <81>Kª6Ðþ6ö<S<89><9c>xW^_ ^BÏIntent-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^0Ã<91>Ë<9b>Ä-----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

```
./heartbleeder upload.client.163.com
rczdz2013giu@163.com", "custom-folders": [{"count": 0, "account": "rczdz2013giu@163.com"}], "os-version": "4.0.4",
-id": "a1000033daf59f8@00:1a:98:4f:74:cf", "notify-folders": [{"count": 1, "account": "rczdz2013giu@163.com"}],
JoR/W/`Crfh8_zAn*UDDbft@Y3xIpPc, LG&ZK`nioWD>di(9.Kwyd]Uic'+h%gwPjb'`CYv(@U_)HxlGrYtSA30u34NT.5Int": 1, "accou
nt": "gltw2012@163.com"}, {"count": 1, "account": "gltw10@163.com"}], "brand": "samsung", "not-disturb-on": false}Wu
26.com"}], "voice-on": true, "shake-on": true, "app-version": "2.2.1", "custom-folders": [{"count": 1, "account": "jiu
busja@126.com"}], "allow-new-mail-notification": [{"count": 1, "account": "jiuzhousja@126.com"}], "brand": "HUAWEI",
&+m[JYRVz(uFY&ln(1f:t#Eom.OoXMe(\[V:a d'O< x@p#nRUE"|z*YqgWoGB@KMZGrq-Es1GTBC0[y`8$3[T_J-<-b@--yay-DQvobbIT
\0J@h,!ETiyD7&"Pq]=@`Y_e!VfWz}i(B,bMKF0.%@tT9 ]CYb`@=FC8Unb@FGm]D7[yHyOJyqO;H;xuo)U.5Ffdms-tBnm(8;<`8bZ.bc
tGGs#pQ^[dMRWQ]PcD9Z"x,xG51N8;-OkX)ZS<[@#csi_]0/C!7#q|w-^>k[8
"}, {"os-version": "4.1.2", "allow-new-mail-notification": [{"count": 1, "account": "zane606@163.com"}], "brand": "s
3.com"}], "voice-on": true, "shake-on": true, "app-version": "2.2.3"}#e<[Ld]@--69e0x7NWjZ2tFO1R5JaW566dJb3jDsxM-
.2.3")D<j@--eVqmtNktt4P5QNRyfQzxgyh7C2tOL-91771---=?j**7-Znt": 1, "account": "meeustb@163.com"}, {"count": 1, "acc
disturb-on": false}M\3S4K(Q(n": "2.2.3")&eqh1@"[JC2xjdtHyPz\4&f.dEpvj&'yX+O#B\fkOv]S&\=YtnIZ`1J?FA;jWX@e]giK5
judyjia_515@163.com"}], "voice-on": true, "shake-on": true, "app-version": "2.1.3", "use-web-signature": 0, "custom-
lication": [{"count": 2, "account": "judyjia_515@163.com"}], "allow-new-mail-notification": 1, "brand": "samsung", "
D<j@--eVqmtNktt4P5QNRyfQzxgyh7C2tOL-91771---=?j**7-Znt": 1, "account": "meeustb@163.com"}, {"count": 1, "account
rb-on": false}M\3S4K(Q(n": "2.2.3")&eqh1@"[JC2xjdtHyPz\4&f.dEpvj&'yX+O#B\fkOv]S&\=YtnIZ`1J?FA;jWX@e]giK5'#O9
```



```
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  5i42QY08nwdgd1T:
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
```

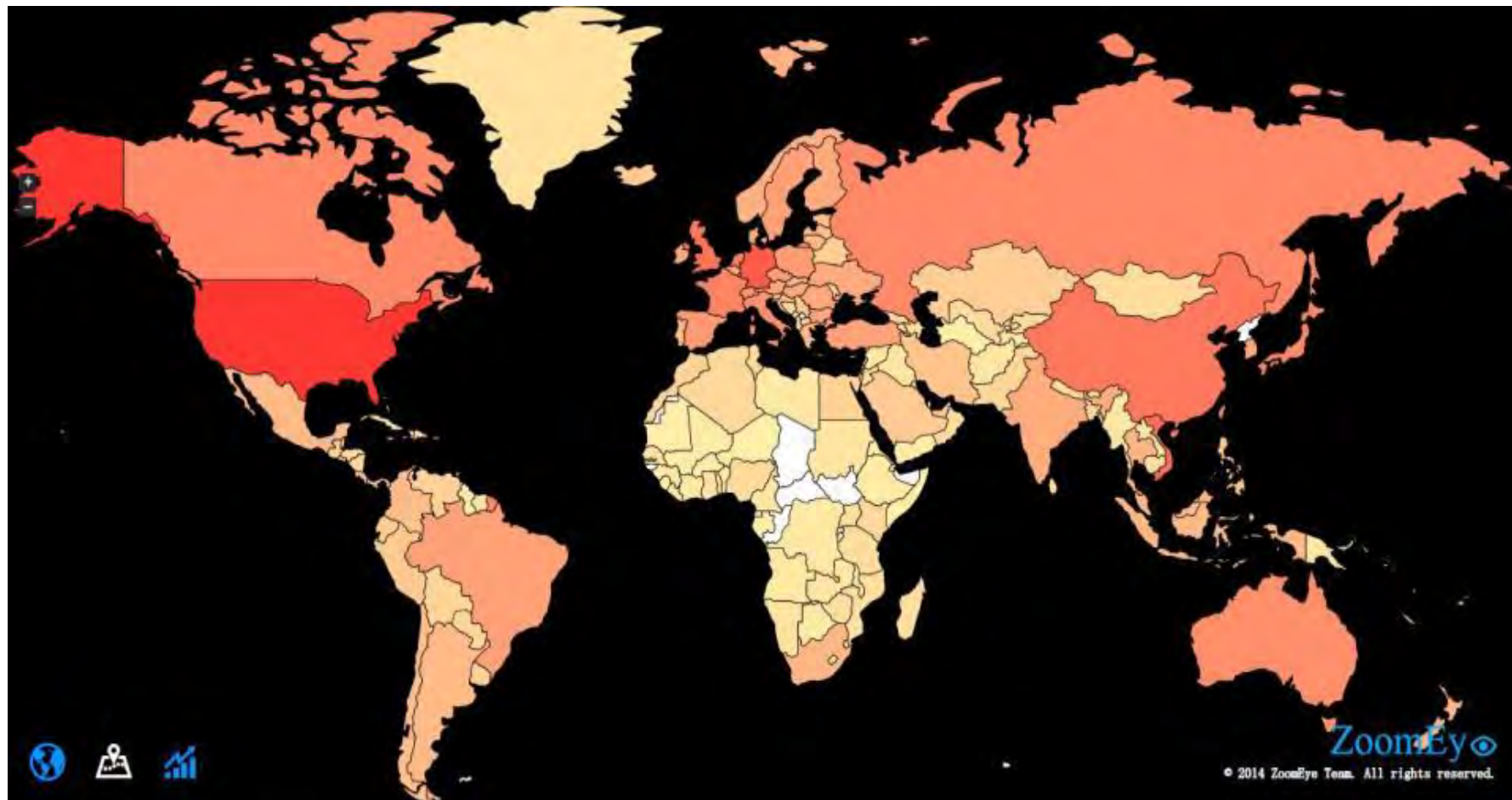
中华电信hinet邮箱

1	用户名	密码
2963	jaki.cpu	ak2017
2964	jamehou	in133
2965	james45.lee	16405
2966	james.bk3689	2144LLI
2967	james.frun	ji930091
2968	james.lorenz	6476582
2969	jameswa	ii1111
2970	jamin.nee	ii1200h
2971	jan1121	1021204
2972	jan97322	2ukxdlx
2973	jane.kelly	6104
2974	janelee.puzco	gal180m
2975	janelu	man1n
2976	jane.one	55585
2977	janes.judy	Wri777
2978	janet104	2g1ad
2979	janet99.lu	9001
2980	janet.jaja	g1a1ar66
2981	janewei	JH61
2982	janeyiru	ei15
2983	jang.dt	01c1min
2984	jang.hsin	2471
2985	jangshin	95846
2986	jang.yicheng	5068
2987	janice.t48	5060
2988	jan.minj	6104

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=QgcdUDIIeziw0ND%2FRiqpkCqu
10981 AlexaToolbar-ALX_NS_PH: AlexaToolbar/alxg-3.2
10982
10983 1fbEiCAN i@DC4hRSAl4b^}SOHδACKBEL BEL BEL BEL BEL BEL BEL BEL BEL mgCvc69CJUIhs; p
10984 AlexaToolbar-ALX_NS_PH: AlexaToolbar/alxg-3.2
10985
10986 act=login&Submit=1&username=vmuser13877&password=%24y[REDACTED]%25eta[REDACTED]
EOT EOT 92TxiHVUQq4CngEHan5rT2esiYxzdrqT4qUBj3rf83bH8bpU6Xe%2FUYyYPjoB97vp
hZgfbJRyQrQ21j0Ep5coxyf4Q0SBuAlNjGJMpviyh4GBhEF2H9LUXYi%2
Fy4HXjZ8QXoo9Q6zQxpM2h7%2FNBrük1UV4fYF0l8TPCoSWdqr%2FiF6G4q0cwByidMRz9pw
10987 Connection: keep-alive
10988 Pragma: no-cache
10989 Cache-Control: no-cache
```

2 漏洞影响态势



全球受影响的公网IP共计： 2,433,550

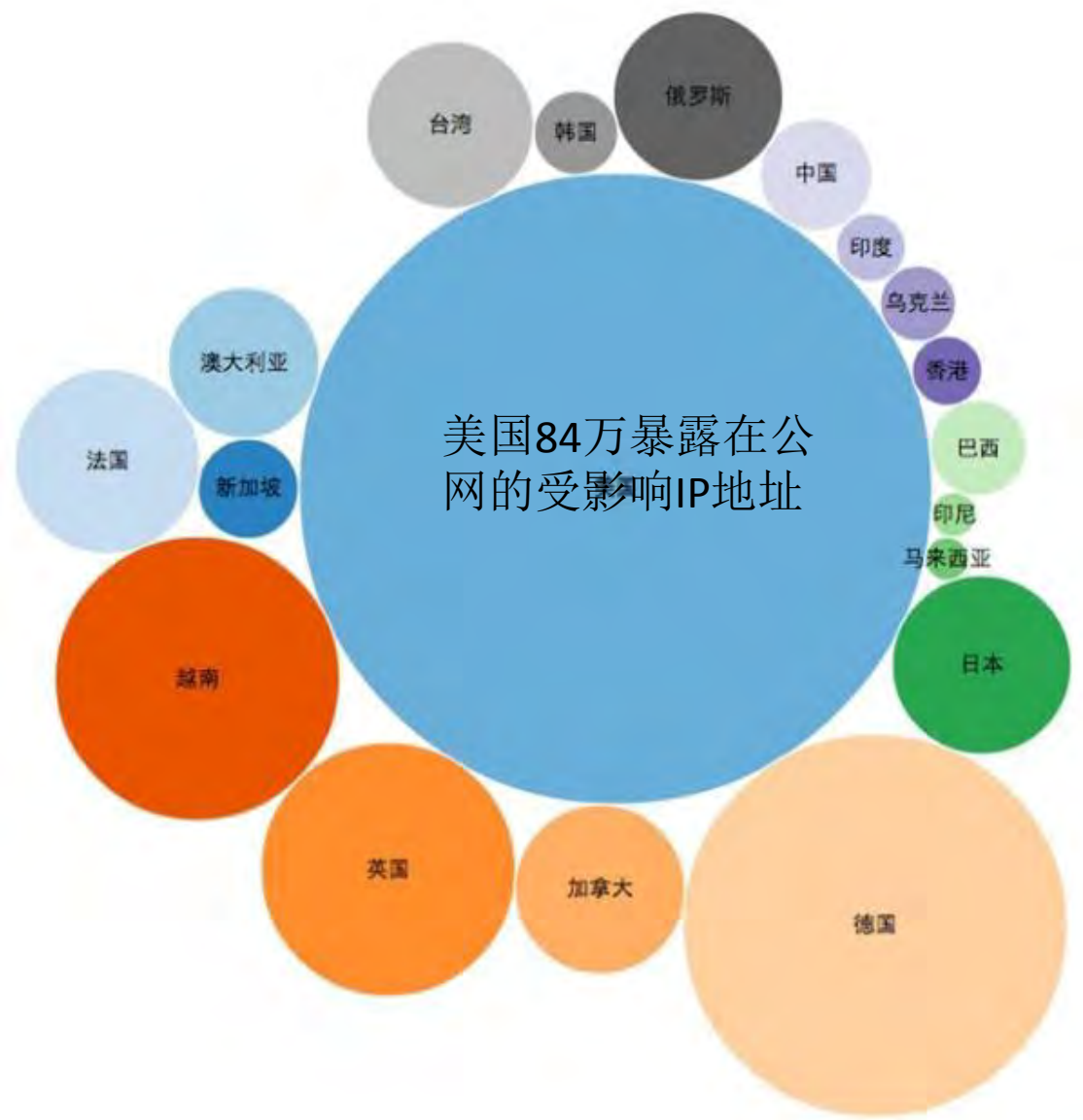
<http://zoomeye.org>

全球受影响暴露面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

中国周边和欧美20个地区受影响暴露面



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

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。

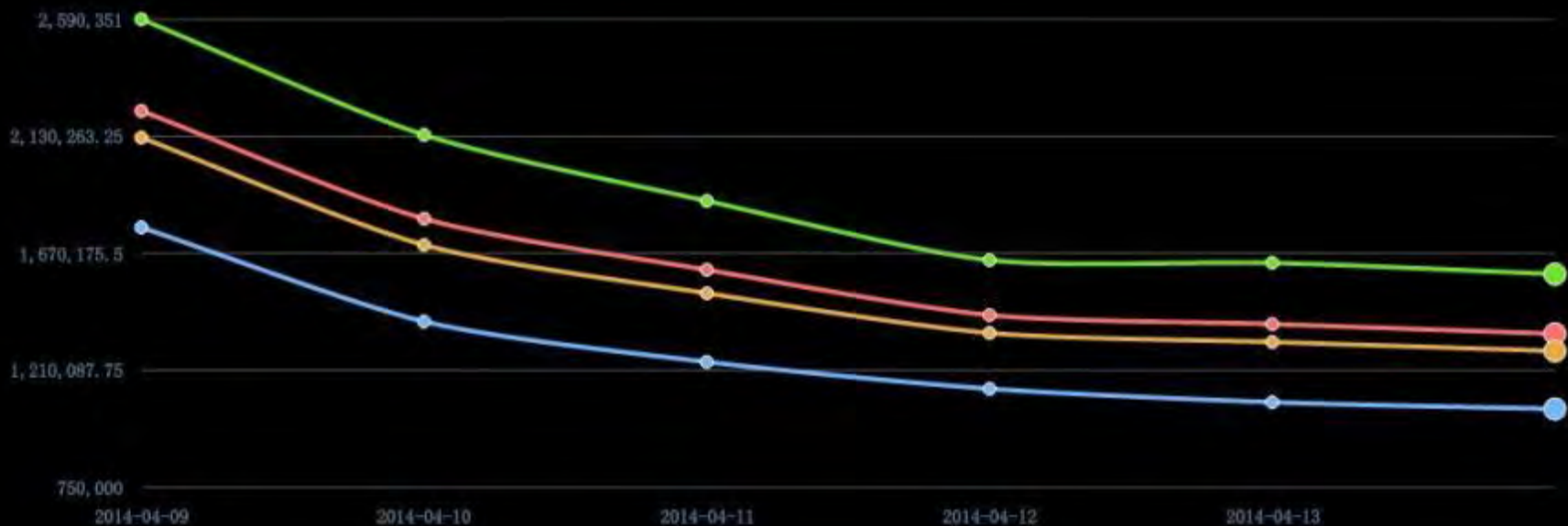
国家需要大力发展信息网络时代的基础建设

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

Trend of HeartBleed affected hosts



受影响的HTTPS、邮件系统等协议端口，一周的修复趋势

第7天全球分布

OpenSSL "心脏滴血"漏洞

443端口HTTPS服务受影响数量 **1,089,842**

465端口SMTPS服务受影响数量 **147,292**

993端口IMAP4服务受影响数量 **353,310**

995端口POP3服务受影响数量 **329,747**

本图显示全球443端口受影响服务器的分布

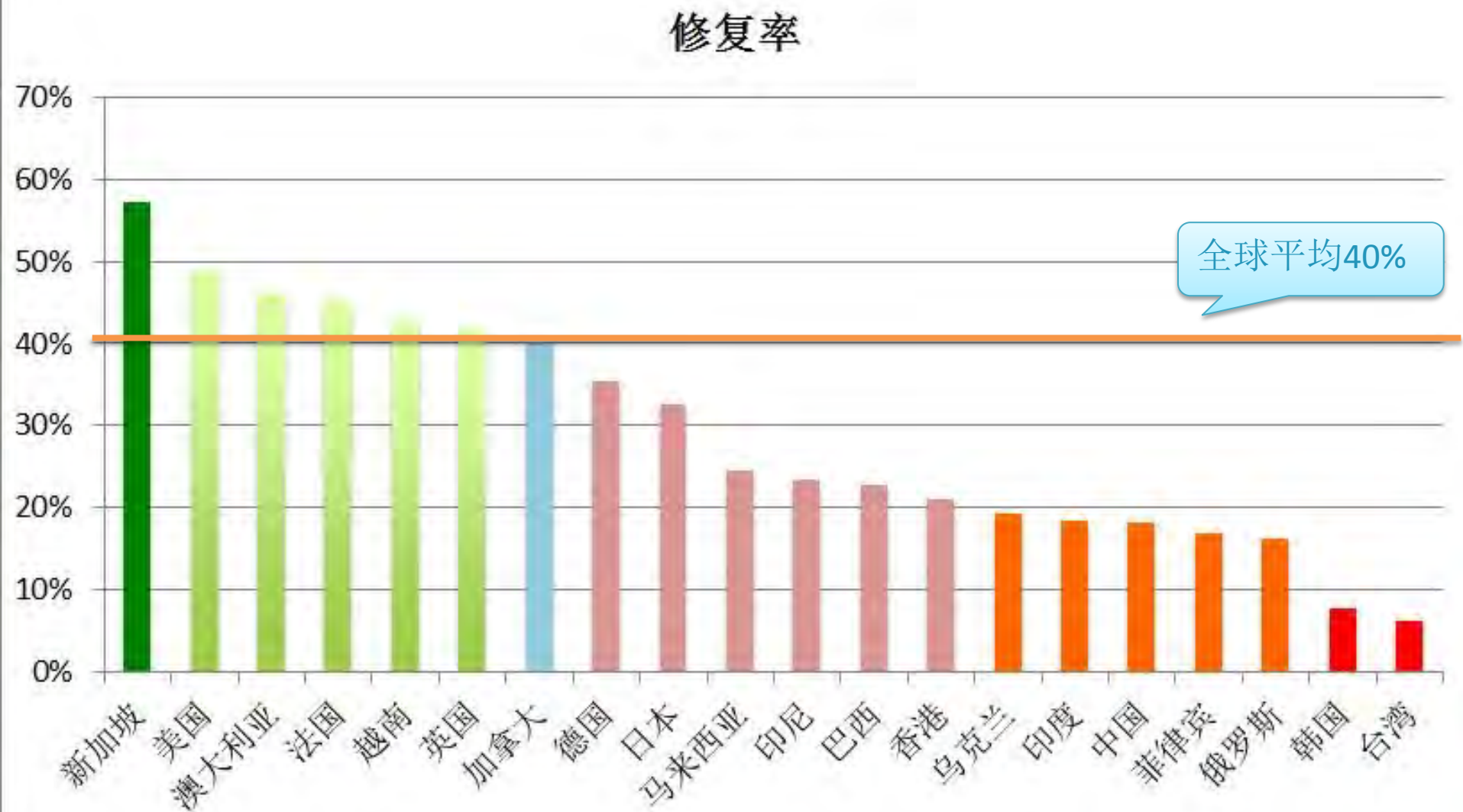


<http://zoomeye.org>

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%

三天内，周边和欧美20个国家修复率



一个星期内全球修复趋势

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%**

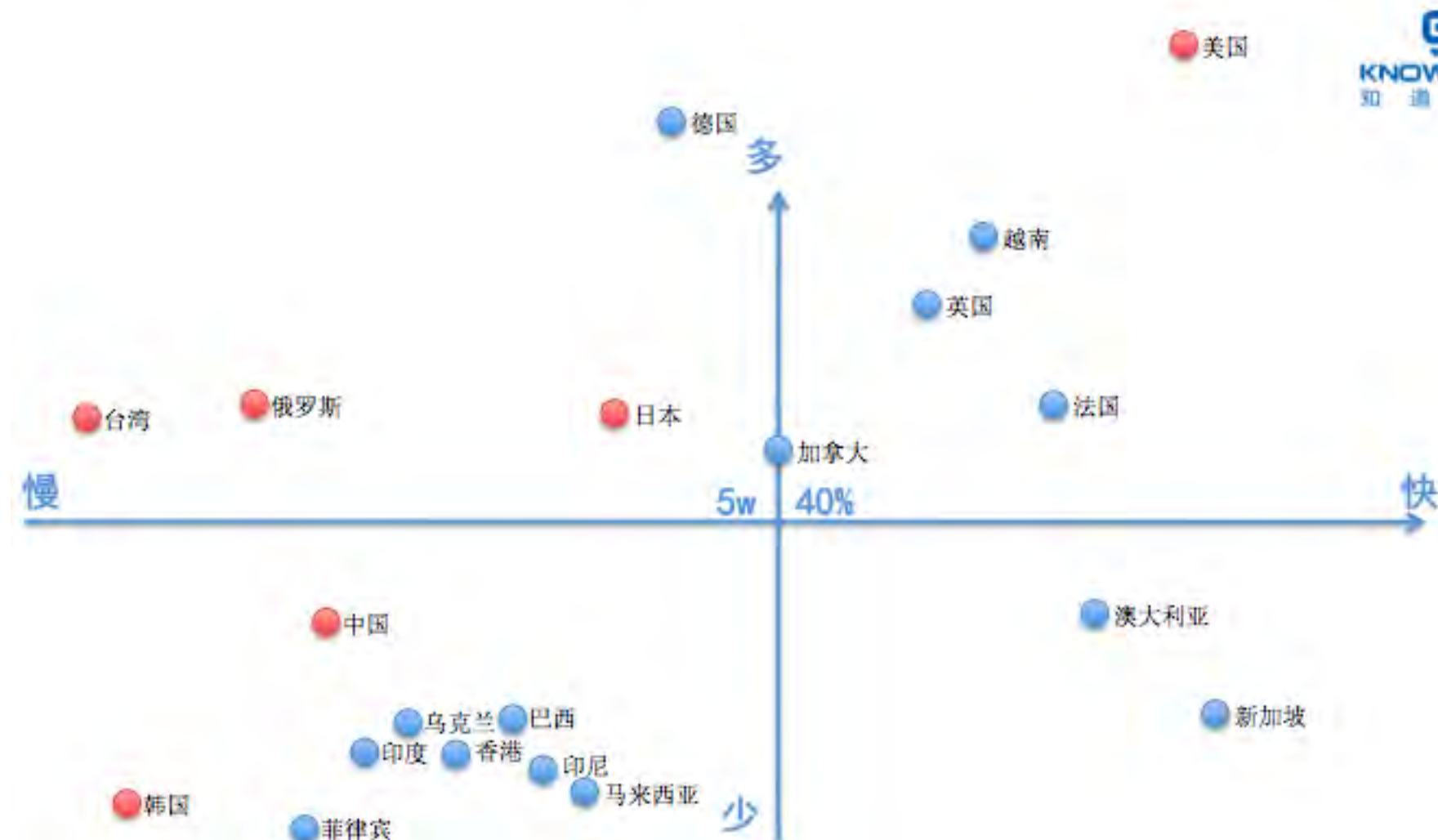
中国 **18%**

美国 **49%**

韩国 **8%**

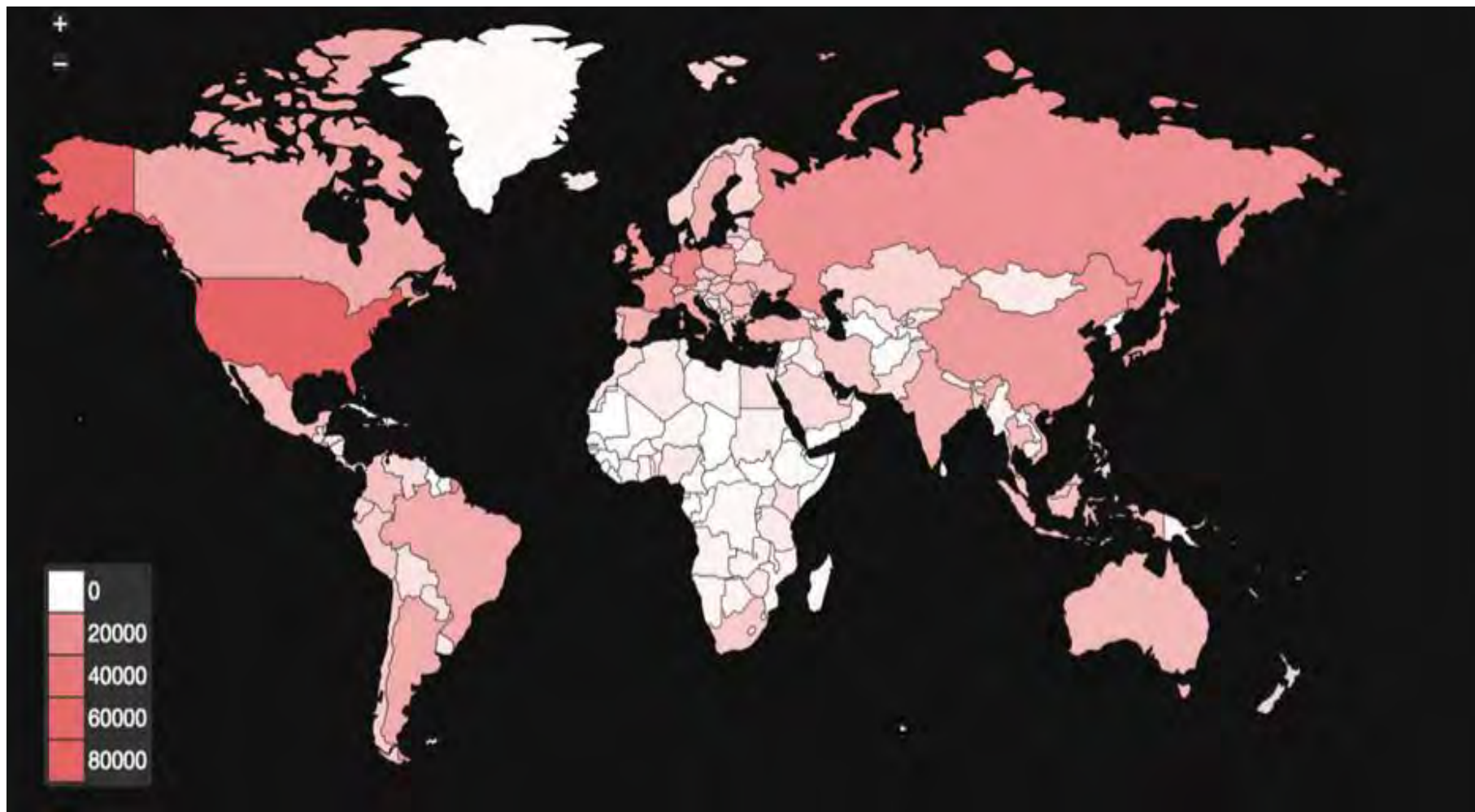
越南 **43%**

台湾 **6%**

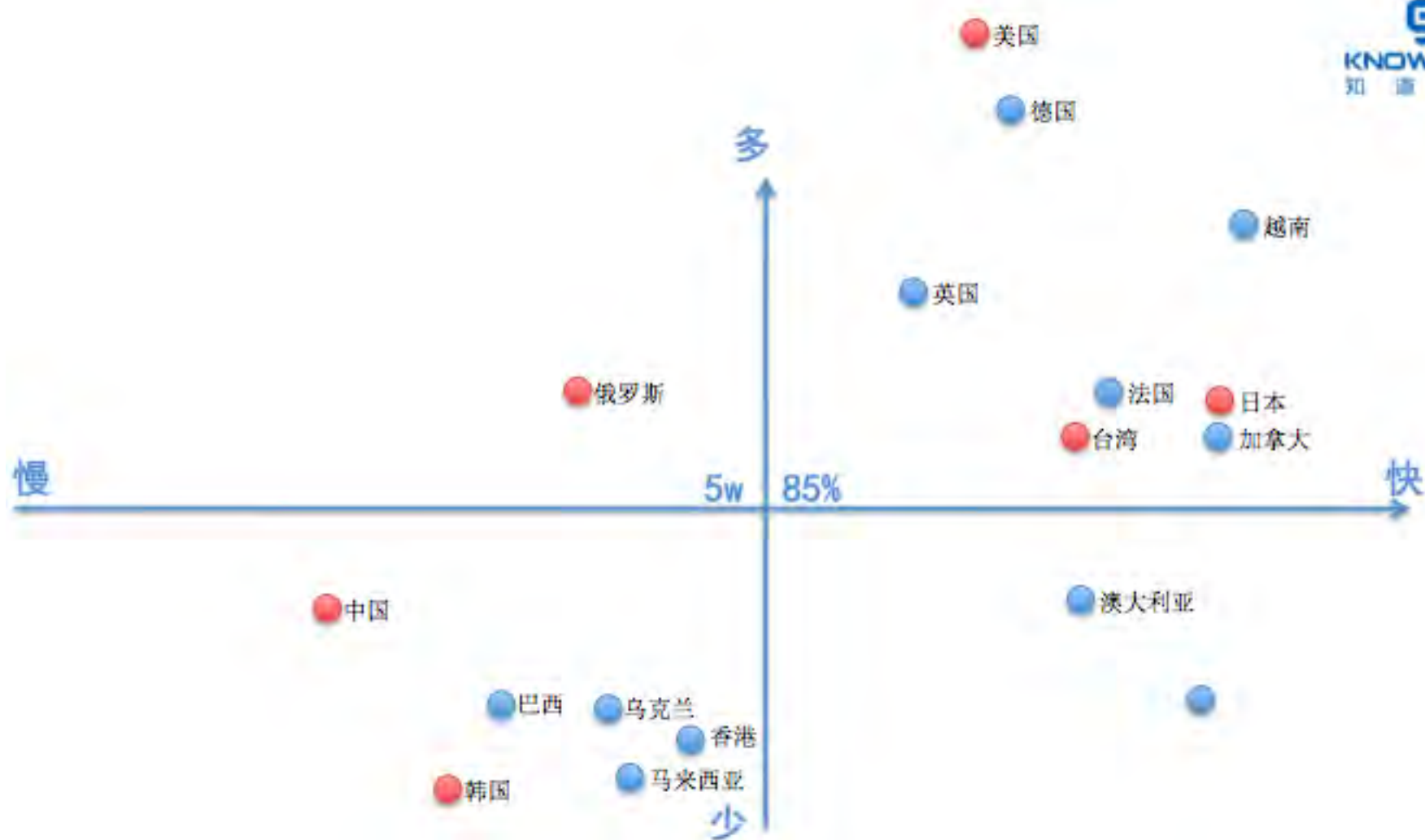


网络战应对能力，
中国全球排名**102**

第365天全球态势



一年后，全球受影响公网IP，共计：377,221，占爆发时受影响IP总量的14.6%



各国【防御能力】对比



2014年

横轴：修复速率

纵轴：被感染IP数量

2015年

谢谢！

知道创宇：杨冀龙

微信：laolaoyangyangyang