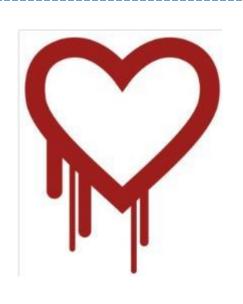
ArchSummit





从漏洞修复看各国网络战防御能力



大数据和云计算 在网络安全行业的应用



1 ZoomEye架构

- 2 数据分析
 - --从心脏出血漏洞看各国防御应急能力



ZoomEye平台架构

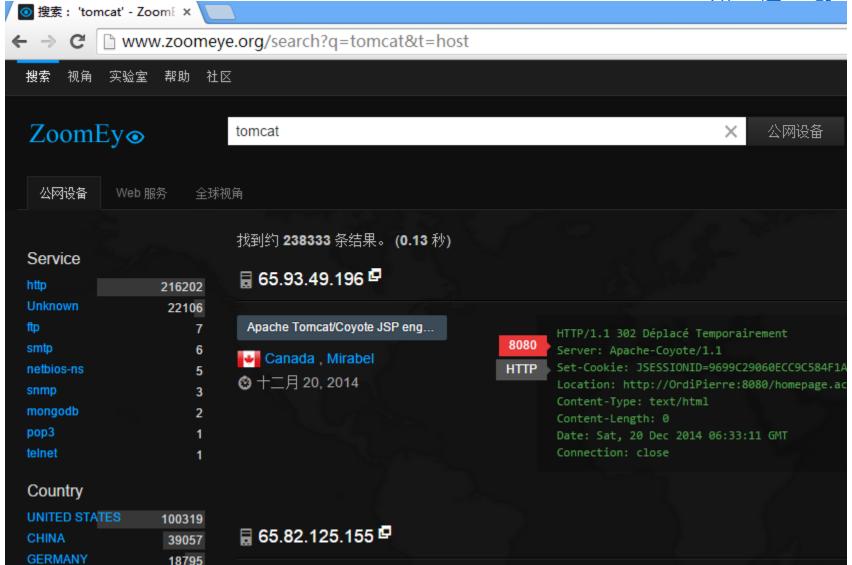
ZoomEye - 网络空间搜索引擎





ZoomEye - 网络空间搜索引擎



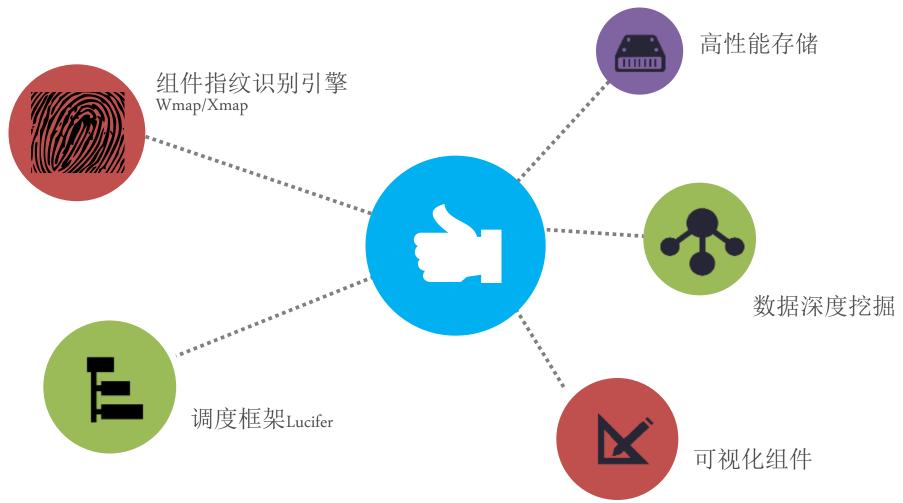


ZoomEye - 网络空间搜索引擎



- 针对全球42亿IP地址,探知资产状况
- 存活性
- 开放的端口
- 运行的服务
- 端口上的应用
- 应用的版本
- 应用的插件
- 插件的版本
- •





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
- • • •

组件指纹识别引擎

Wmap/Xmap



识别WEB服务组件

浏览器: Firefox/IE/Chrome Web前端框架: jQuery/Bootstrap/HTML5框架 Web应用: BBS/CMS/BLOG 插件 Web开发框架: Django/Rails/ThinkPHP Web服务端语言: PHP/ASP/.NET 扩展 Web容器: Apache/IIS/Nginx 存储:数据库存储/内存存储/文件存储 操作系统: Linux/Windows

组件指纹识别引擎

Wmap/Xmap



			知	迫	刨	于
www.zoomeye.org/co	omponents/	●☆				
А	advanced web stats awstat Atmail AtomicCms ASdh	p.net aspcms anymacro-mail system alpaca amanda abcms akcms addthis adobe goli is alimama ad-union aphywire.com Asp.cms AdaptCMS Archiva ArticlePublisherPRO it Ametys amirocms accessibleportal amcharts ampcms angularis acarsd acarsd httpd I alevtd for videotext pages httpd amavisd smtpd amsn apcupsd artsd authd avtech httpd ttp http proxy				
В	www.zoomeye.org/co	ter h2evolution bluecose blinty baidu adm baidu adsense bootstran bootstran bloner emponents/				Q 22
С	L	lotus-domino leadbbs lazyoms leichicms lizard-cart bscms Ipromis linezing L lepton limesurvey lancom sshd idminfod login session daemon libssh lighttpd llin lshd secure shell lukemftpd				
D	М	Mandrake Mandriva Mac OSX microsoft-iis maxems metinfo magento mymma Exchange Mambo mysql Mail2000 mantis MediaWiki Medz Framework myp2 Mojolicious mono Moodle MovableType Mura Mynetcap m0n0wall http portal mmdpop3 memcached midasd midentd minipop pop3d mifingerd mildentd mmmmpd mpd web server mpopd perl pop3d muh irc proxy mxl smtpd myigd	c mzcm nailfront sr	s moinr ntpd m	moin Ma andelbrot	exSite ftpd
E	N	NetBSD nginx netscape-enterprise newasp nweb NukeViet nucleuscms nabbi daemon netapp ftpd netqmail smtpd nginx nginx imap proxy ngirod nhttpd noht nuttcp network throughput tester				
F	0	OpenBSD oracle-application-server oecms oscomerce opencart openx openco opency ophal Osclass Octopress opennemas odmrd oftpd olsrd http info plugi				outlook
	Р	phusion phusion php play-framework phpwind pjblog php168 phpcms presta management phpidapadmin pageadmin phpdisk phpMyAdmin phpnuke plone Percussion phpDocumentor php-fusion phpsqlitecms plentymarkets punbb pdns pop3 proxy poppassd popper pop3d pppctid pppd print server print server http of httpd pwdgen pyftpd pyftpdlib pygopherd pysieved	phpBB d piden	posterou td pksp	s Piwig xy pmu	o d pop3g
ArchSummit 全班	Q	qibocms quarkmail quarkmail qhttpd qmail pop3d qmail smtpd qpopper qpop quark	per pop3d	qpsmt	pd qpsi	ntpd smtp

第一个版本



2007年: 检测一个网页是否有挂马

Qemu: 虚拟16个Windows XP每个XP运行带沙箱的32个IE6





第二个版本



2008年: 一个小集群

包含了96台服务器 一个8服务器组成的MongDB集群



第三个版本



2009年: 所有网站的技术组件感知、被黑监控

添加了:

基于Gearman做了一个调度系统

5个不同区域的机房部署了服务器

部署了一个hadoop集群,主要用于存储

使用了lucense

添加了一个mysql数据库

Mongodb继续扩容

采集器除了沙箱系统外,添加了大量的采集worker插件

第四个版本



2011年: 所有开放80口的IP, 对应的技术组件、及被黑感知

继续扩大机房建设 Hadoop开始用于分析 Lucense开始换为solr Mongodb继续扩容 继续添加服务器 继续添加worker采集插件,采集更多样化的数据 累计大约到了400 server的数量

第五个版本



2013年: 所有IP的HTTP服务(包括非80), 采集对应的技术组件、及被黑感知

继续扩大机房建设 Hadoop换为DSE的发布版本 Solr开始工作 Mongodb继续扩容 添加了一个cassandra数据库 继续添加worker采集插件,采集更多样化的数据 继续添加服务器 累计大约到了700 server的数量

第六个版本

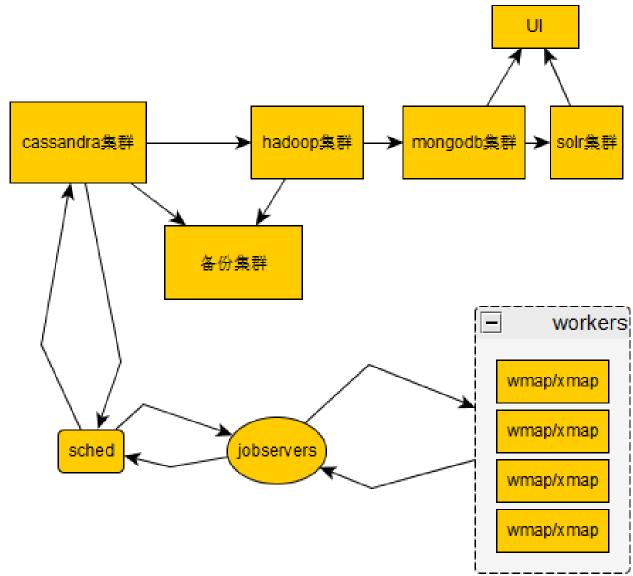


Now:漏洞响应与态势感知

累计大约到了1000 server/vmbox的数量

整体架构





调度框架 Lucifer



sender 发送器 collector 收集器 collector sender jobserver 作业调度者 jobserver recover recover 回收器 workshop workshop workshop

worker

workshop 车间

worker

worker

worker

worker 工人

worker

worker

worker

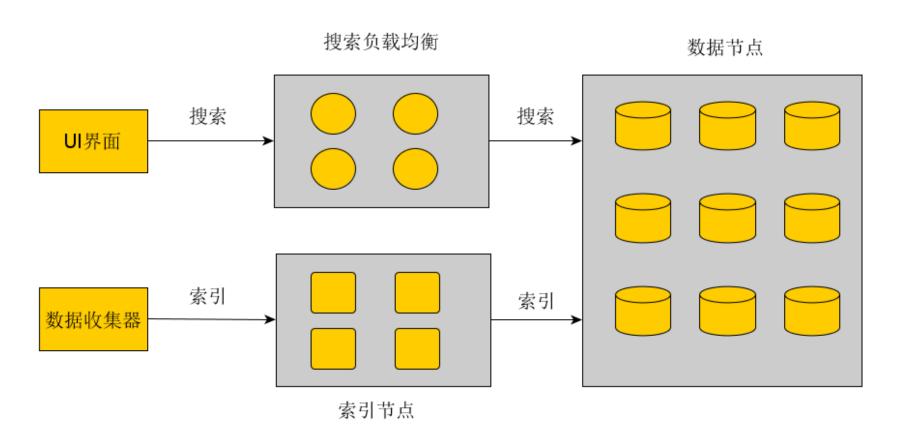
worker

worker

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。



数据分析

--从心脏出血漏洞看各国防御应急能力

历史上第一个上央视的漏洞





12306铁道购票系统



547&userDTO.pass user name= 325&confirmPa word=zhad ssWord=zha 325&userDT O.IVR_passwd= &confirmIvr_pwd &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^E604975000410177501183 031550042&train_location=B2&_json_att =&REPEAT_SUBMIT_TOKEN=1e23ac3f d0630836c67aad1dde869ca7







```
37 25 32 46 37 62 78 25 32 42 37 48 38 37 71 37
                                                       7%2F7bx%2B7H87q7
            71 54 72 74 4F 53 69 25 32 42 76 47 76 37
                                                        34qTrtOSi%2BvGv7
           6E 36 76 36 68 37 36 7A 30 76 65 58 75 75
                                                       Oan6v6h76z0veXuu
      50 7A 71 71 76 50 75 72
                              66 25
                                    32 42
                                                       PzqqvPurf%2Bh5aT
           4C 25 32 46 6D 25 32 42 61 58 39 25 32 46
2200:
                                                       h9L%2Fm%2Bax9%2F
            6B 75 76 36 25 32 46 25 32 42 65 71 68 25
                                                       Lbkuv6%2F%2Beqh%
2220:
              25
                  32
                    42 79 38 66 47 76 39 62 50 32 71
                                                       2B0%2By8fGv9bP2q
                  31 76 75 66 77 72 75 72 71 74 4F 61
                                                       %2Bb1vufwrurqt0a
      6E 25 32 46 71 4C 37 37 4C 6E 25 32 46 39 62 54
                                                       n%2FqL77Ln%2F9bT
      35 37 4C 50 39 76 75 65 6E 25 32 46 25 32
                                                       57LP9vuen%2F%2FS
2260:
              65
                     37 76 4F
                              77 34 62 25 32 46 37 75
                                                       i5Pe37vow4b%2F7u
                  33
                                                       v7r00%3D%3D&TPL_
2270:
               30
                 51 25 33 44 25 33 44 26 54 50 4C 5F
                  6E 61 6D 65 3D 62 72 61 64 65 63 61
                                                       username=bradeca
2280:
                                                       odTPL_password=
           54 50 4C 5F 70 61 73 73 77
2290:
                                       6F 72 64 3D 36
              37 39 35 6D 65 6E 67 63 61 6F 26 54 50
      33 36 30
                                                              &TP
22b0: 4C 5F 63 68 65 63 6B 63 6F 64 65 3D 6B 75 34 62
                                                       L_checkcode=ku4b
```

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/p
artner/T1ecVaXl0XXXXXXXXX","isCertified":"Y","loginId":"
                                                                            om","login
ServerTime": "2014-
                                  ',"loginToken"|"
                                            ","resultStatus":1000,"sessionId":"
memo":"操作成功。" "mobileNo":"
                                  ,"userId":"
                                                               ","userName":"
relessUser":false}, "resultStatus":1000}
{"id":0, "memo":"操作成功", "result": {"accountHomeAsset": {"freezed":false, "hidden":fa
lse, "mark": false, "opText": "0.75元" }, "bankHomeAsset": {"bankCardCount": , "freezed": fa
lse, "hidden": false, "mark": false, "opText": "共 张 "}, "bollywoodHomeAsset": {"freezed"
:false, "hidden":true, "mark":false}, "charityHomeAsset":{ "freezed":false, "hidden":fal
se, "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,
```





	0250:	6C	3A	20	бE	6F	2D	63	61	63	68	65	0D	0A	43	6F	6F	l: no-cacheCoo
	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	бE	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:																	3lzaWQ+Mzwvc3lza
	02f0:																	WQ+PHBlcnNvbnV1a
	0300:																	WQ+MDAwMDAwMDAwM
	0310:																	DAWMDAWMDAWM
	0320:																	DAWMDAWMDAYMDk8L
	0330:																	3BlcnNvbnV1aWQ+P
	0340:																	G5vZGU+UjFGcmFtZ
	0350:																	Xdvcms0LjEuMDwvb
	0360:																	m9kZT48L0xUUEFUb
	0370:																	2tlbj4=iR
	0380:																	S+.\$jlD
	0390:															4C		AwMDAwMDAyMDk8L3
	03a0:																	BlcnNvbnV1aWQ+PG
4	0350:	35	76	SA	4/	55	2B	55	6A	46	47	63	6D	46	/4	SA	58	5v7GU+UiFGcmFt7X

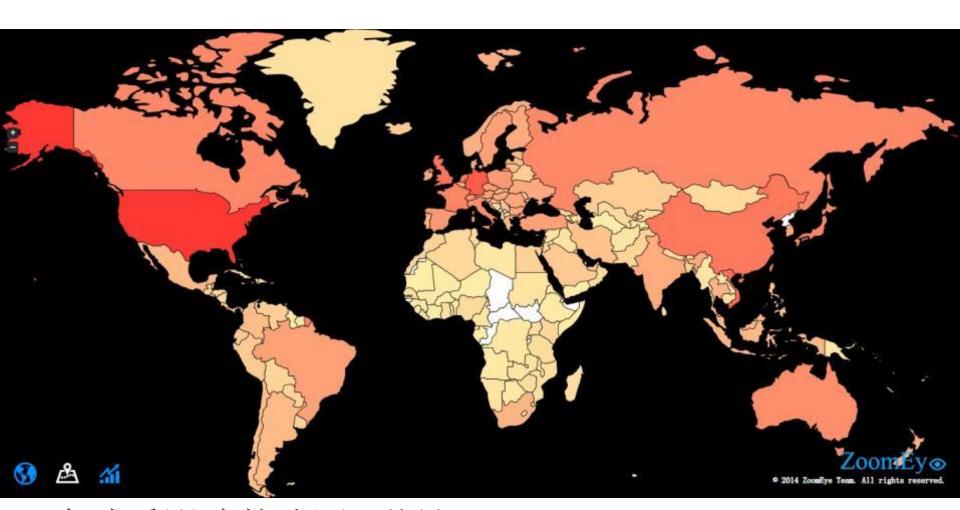
中华电信hinet邮箱



1	用户名	密码
2963	jaki.cpu	ak 20 7
2964	jamehou	ir i 3 3
2965	james45.lee	a es 4 05
2966	james.bk3689	PIAA L I
2967	james.frun	j19300 91
2968	james.lorenz	54 7 5582
2969	jameswa	ilii
2970	jamin.nee	1120h
2971	jan1121	D2. D4
2972	jan97322	2 ukuduk
2973	jane.kelly	6 iD 4
2974	janelee.puzco	g Illon
2975	janelu	m m : n
2976	jane. one	5 5 5 6
2977	janes. judy	W r 7 7
2978	janet104	2 g a di
2979	janet99.lu	9 0 1
2980	janet. jaja	g a et ar 66
2981	janewei	g a e ar 56 J H 6 1
2982	janeyiru	ei 155
2983	jang. dt	Olcal min
2984	jang.hsin	24711
2985	jangshin	9 8 4 6
2986	jang. yi cheng	5 6 8
2987	janice.t48	59600
_≨ 2988	jan.minj	e st oh s t

全球态势





全球受影响的公网IP共计: 2,433,550

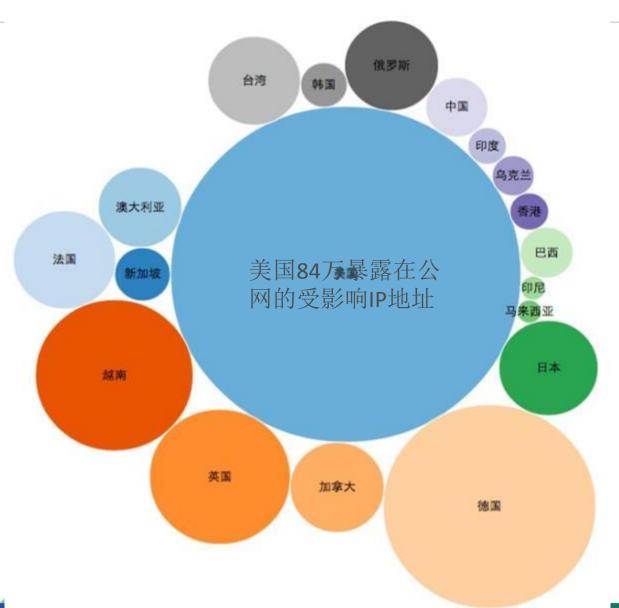
全球可被攻破对象暴露面TOP35



美国84万暴露在公 网的受影响IP地址 德国 澳大利亚 意大利 台湾 越南 土耳其 奥地利 瑞士 匈牙利 芬兰 加拿大 波兰 瑞典 乌克兰爱尔兰保加利亚 西班牙 俄罗斯 新加坡 英国 中国 捷克 日本 荷兰 法国

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个地区可被攻破暴露面

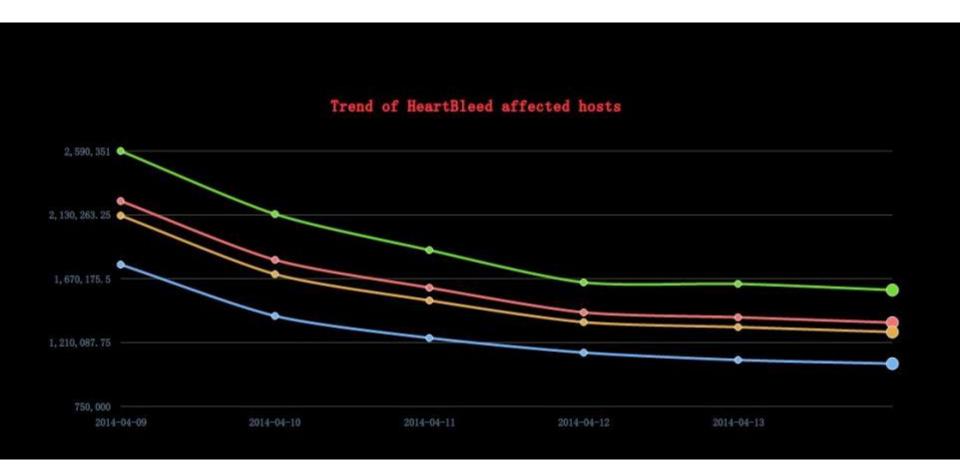


美国	838526
德国	309303
越南	170235
英国	136075
法国	71975
日本	67458
俄罗斯	60629
加拿大	60608
台湾	58770
澳大利亚	48012
中国	26621
新加坡	21408
巴西	19545
韩国	14965
乌克兰	12207
香港	10358
印度	10193
印尼	4325
马来西亚	4081
菲律宾	1715

美国占全球34%,中国仅占1%

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

中国問边和欧美20个国家修复率NOWNSEC

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%
ArchSummit 全球架 <mark>全球</mark>	2433550	1468022	40%

Powered by InfoQ

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%

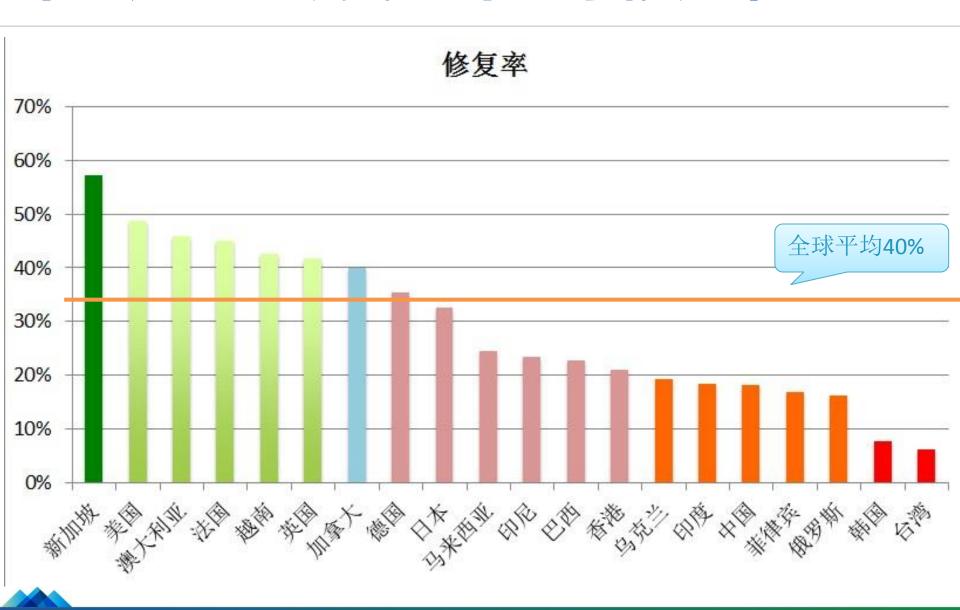
韩国 8%

越南 43%

台湾 6%

中国全球排名102

中国周边和欧美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 石油承包商和服务公司(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

高雄市政府教育局 高雄市立社會教育館 教育機構防洩漏個資掃瞄平台

中華電信hicloud雲端服務 中華電信hinet網頁郵件服務 南荣科技大学网络认证系统 树德科技大学网络认证系统 中壹科技大学VPN系统 建国科技大学VPN系统 国立东华大学VPN系统 中山大学VPN系统

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

大東銀行 日本注册会计师协会 日本sunoco石油公司 日本kohan/kogyo鋼鈑工業公司 総研フィールド公司 独占赛马会

筑波大学 大阪大学 山梨大学 横浜国立大学

TIPS:第一天中国修复情况

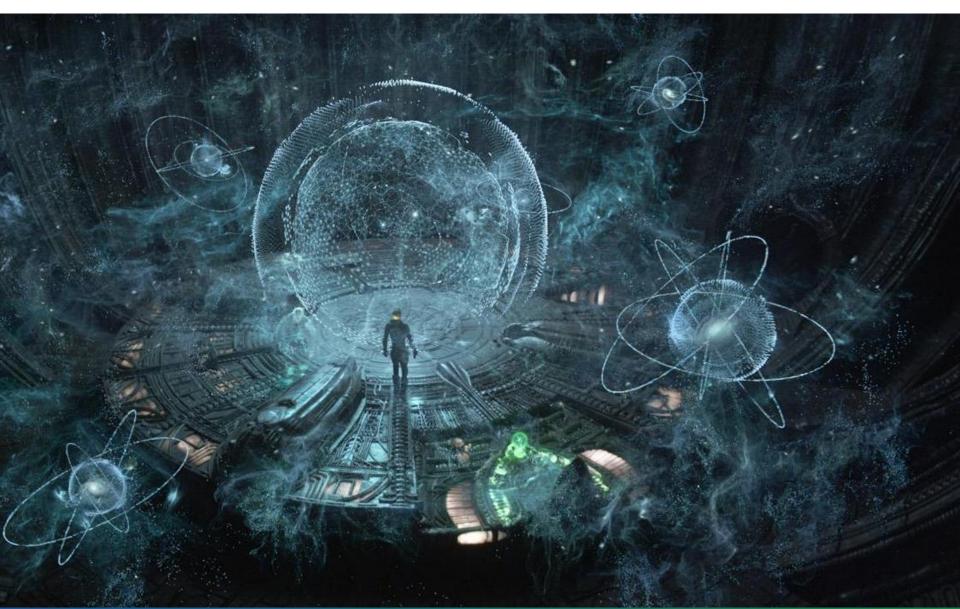
中国

阿里腾讯百度

数据对比发现:

中国基础行业对安全重视急需提高

大数据为网络安全行业开启了新篇章



ArchSummit

谢谢!

知道创宇: 杨冀龙

微信: laolaoyangyangyang



Thanks!

