DBAPPSecurity 安恒信息

西湖论剑

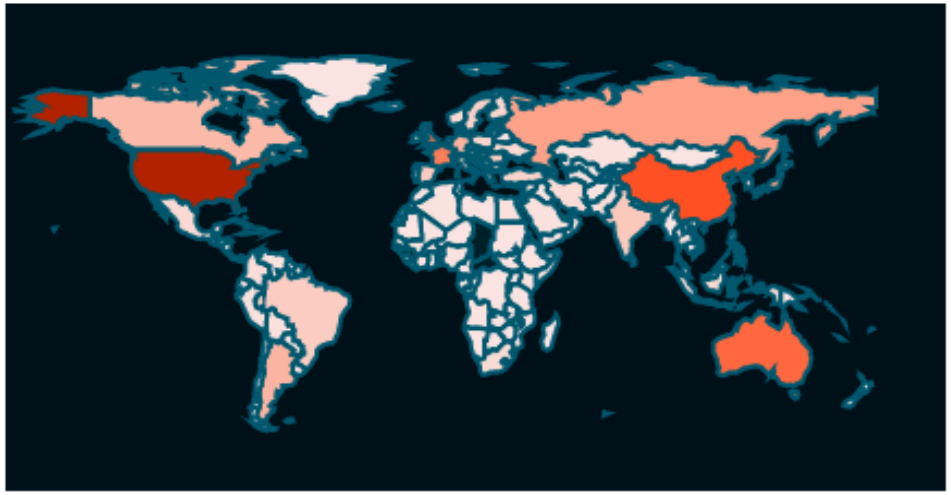
“永恒之蓝”勒索病毒应急响应工作的经验与反思

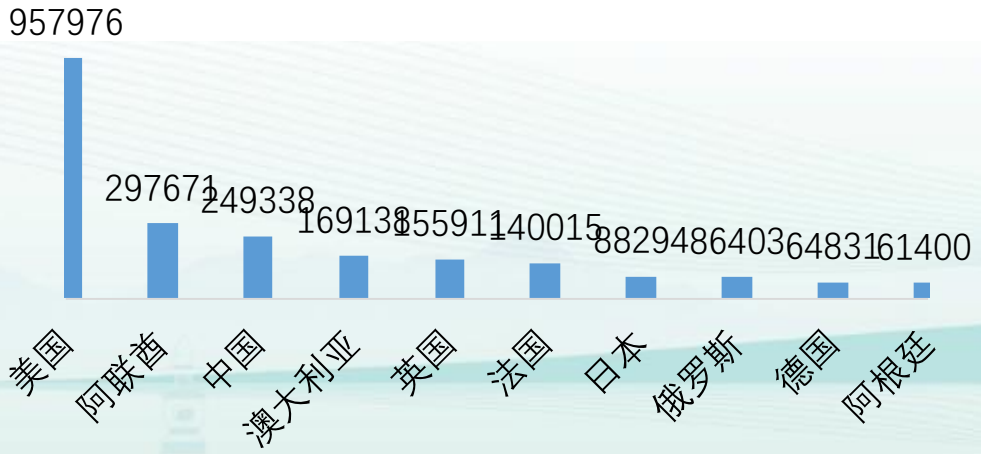
袁明坤


ALPHA
大数据智能分析平台

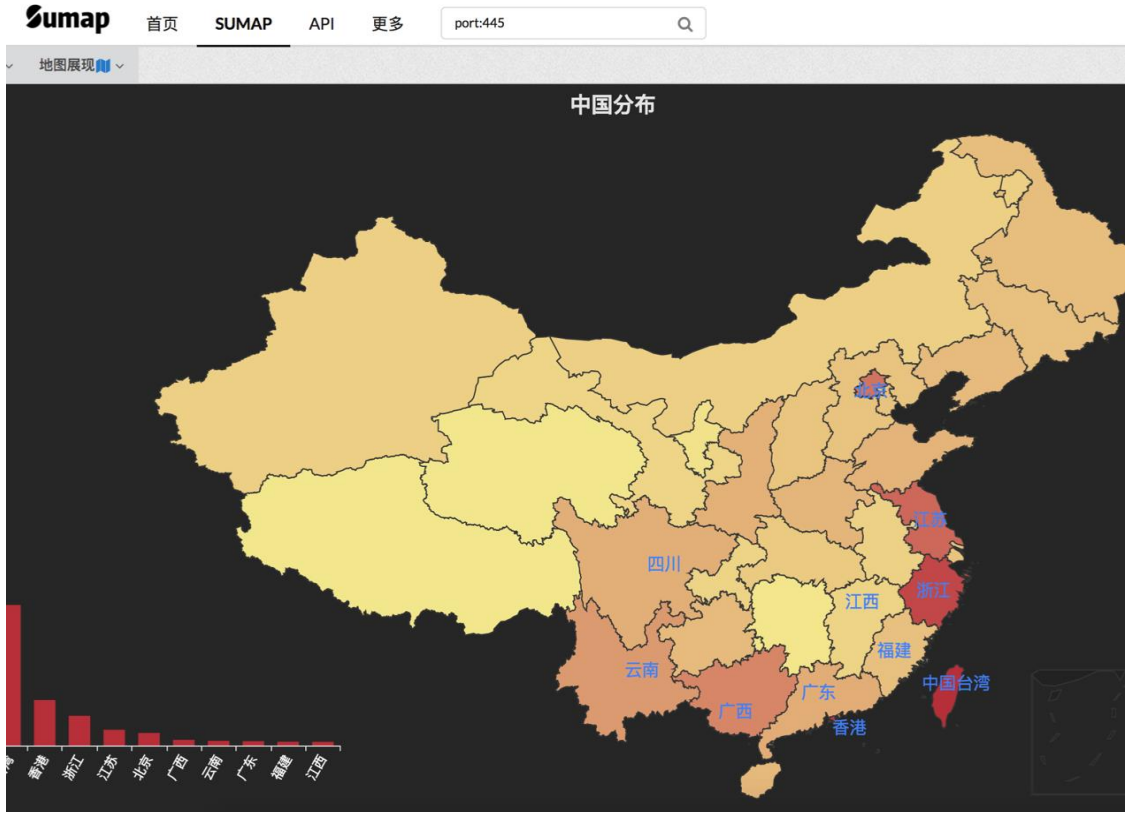

ALPHA
大数据智能分析平台

全球分布情况：





中国分布情况：



- 单日千次电话应急
- 十一份专项报告提供
- 两个专用工具推出
- 百万次下载量超过
- 全线产品全面升级

浙江、广州、深圳、北京，陆续开始接到应急响应任务

公司及应急响应中心病毒样本汇总及应急案例手册完成

全球威胁态势报告
应急响应指导手册
安恒全线产品升级

安恒专项检测工具0.1
勒索软件加固工具0.1
WannaCry勒索蠕虫FAQ

WannaCry勒索蠕虫威胁情报收集平台

安恒专项检测工GUI版本
勒索软件加固工具GUI
周一开机指南

一键式检测、加固

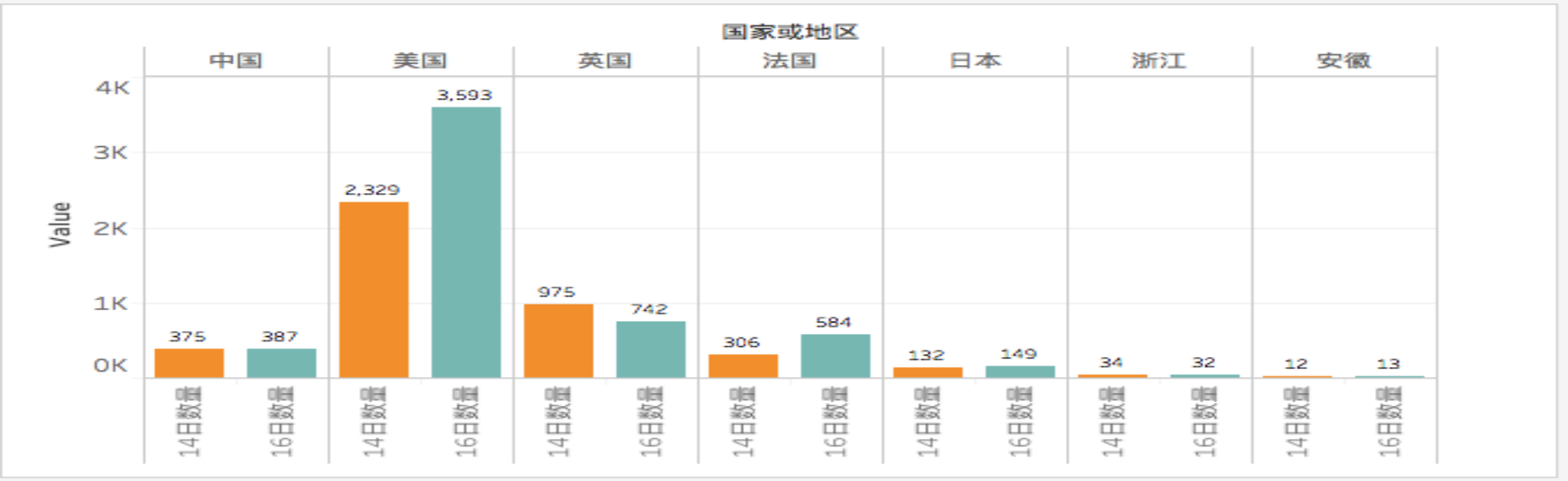
专业深度检测、分析：

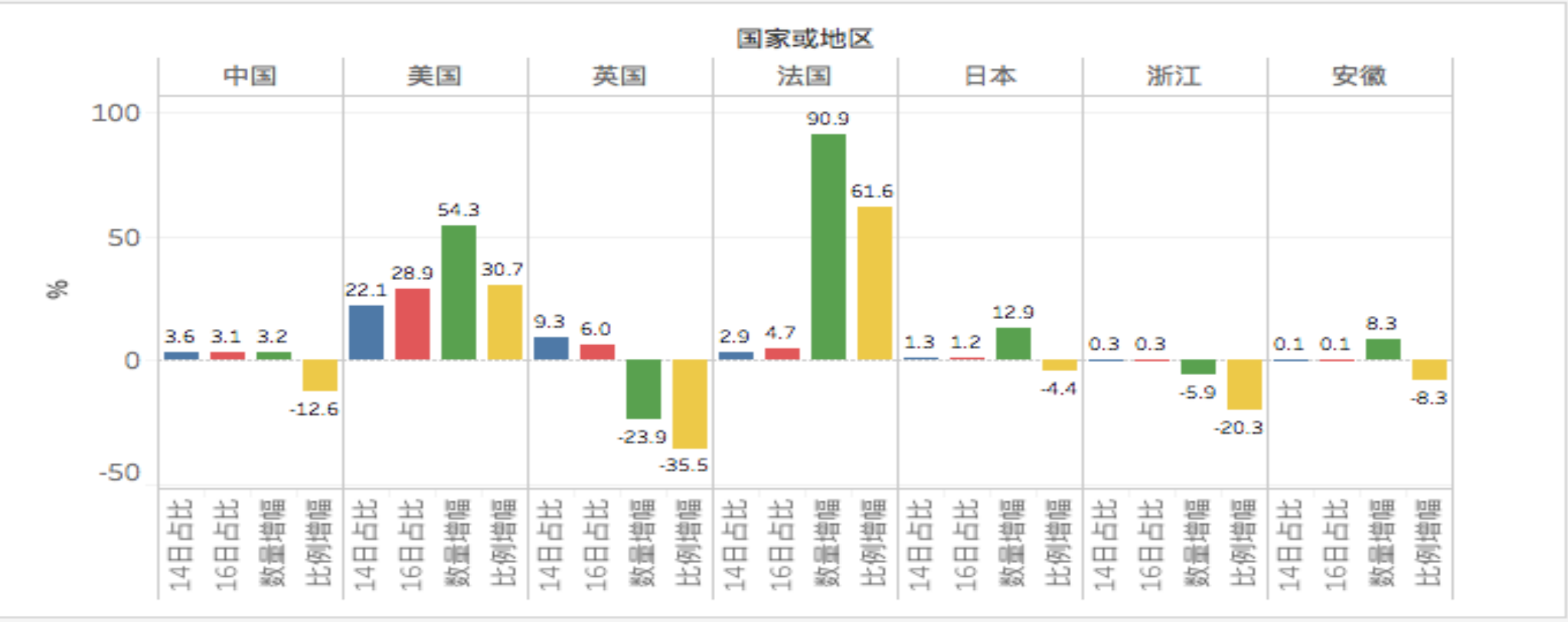
2017年5月14日

2017年5月16日

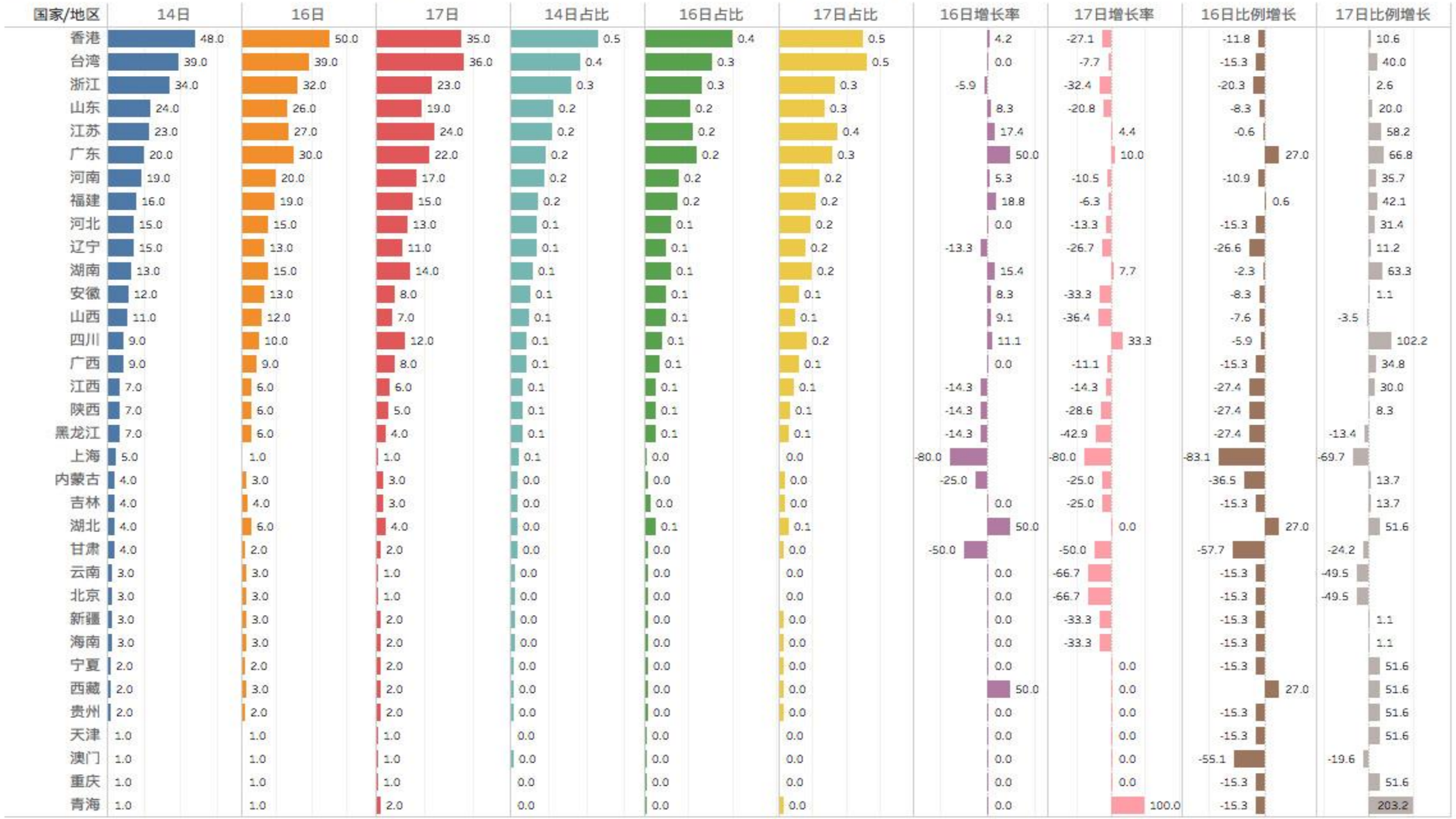
2017年5月14日

2017年5月16日


国家或地区
中国
美国
英国
法国
日本
浙江
安徽
Value
4K
3K
2K
1K
0K
375
387
2,329
3,593
975
742
306
584
132
149
34
32
12
13
14日数量
16日数量
Measure Names
14日数量
16日数量

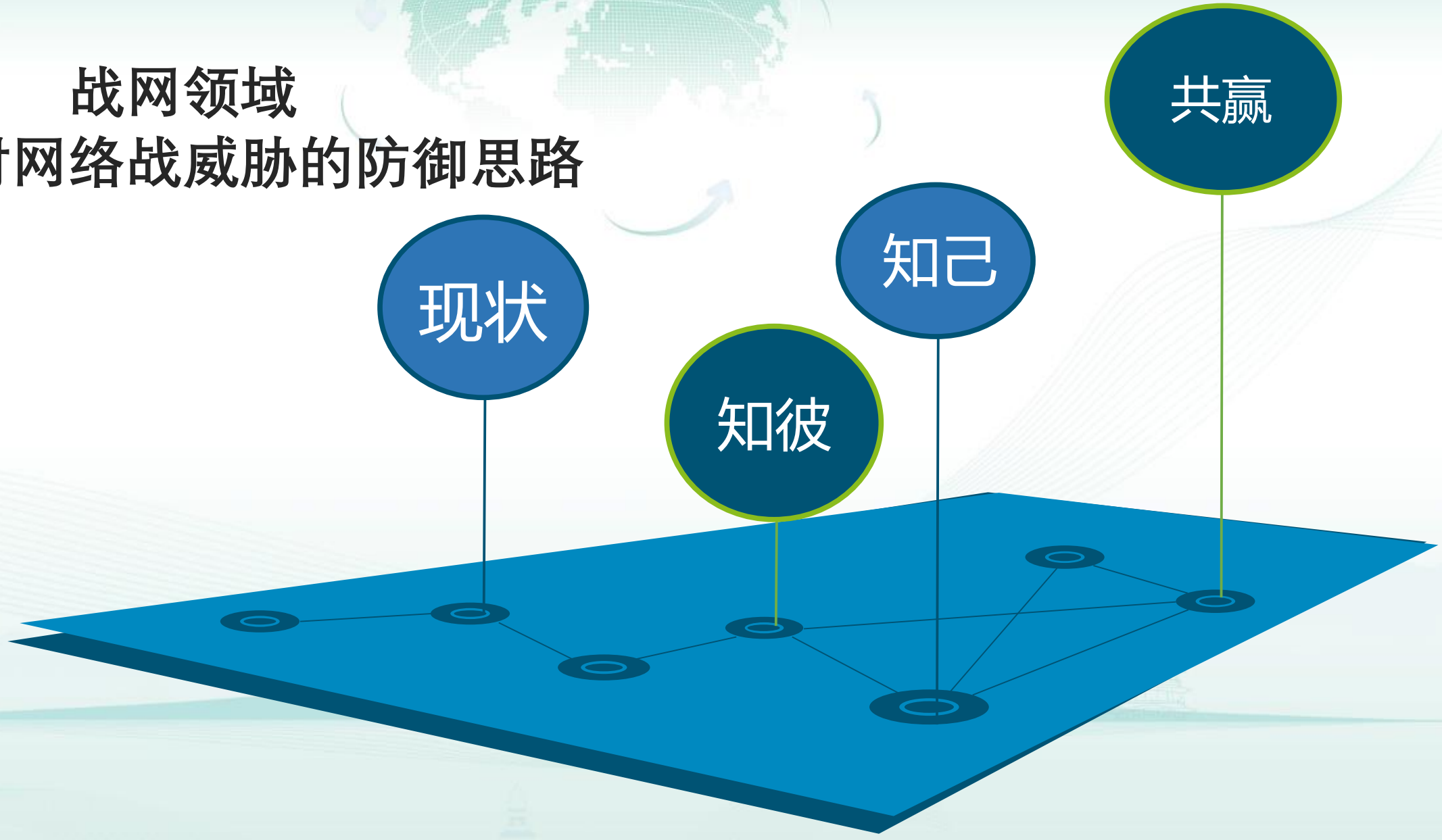

国家或地区
中国
美国
英国
法国
日本
浙江
安徽
%
100
50
0
-50
3.6
3.1
3.2
-12.6
22.1
28.9
54.3
30.7
9.3
6.0
-23.9
-35.5
2.9
4.7
90.9
61.6
1.3
1.2
12.9
-4.4
0.3
0.3
-5.9
-20.3
0.1
0.1
8.3
-8.3
14日占比
16日占比
数量增幅
比例增幅
Measure Names
14日占比
16日占比
数量增幅
比例增幅

杭州安恒AILPHA大数据实验室 - “永恒之蓝”勒索病毒感染威胁态势 - 各省份变化趋势




Shadow Brokers
The NSA Hackers Are Back!

战网领域
主动应对网络战威胁的防御思路



SRC威胁情报事件响应平台

受攻击区域排行

1 广州1,323,456
2 北京22,351
3 苏州2,222
4 济南1,135
5 杭州256

统计内容

基线情况
基线运行41,873次
基线变化433次
人为变化326次
合规变化59次

情报查询
情报查询18,735次
自产情报235次
有效利用情报323次

文件系统
文件系统变化2,141,823次
WEB目录文件变化1,050,411次
敏感目录变化变化326次
启动项变化32次

攻击方法统计

工单处理速度耗时排行

处置人员工作内容统计

扫描web 45 次，发现漏洞 844 个，其中高危 19 个，中危 620 个，低危 205 个，修复 810 个，未修复 34 个。白盒代码扫描 12 次

发现漏洞 2388 个，其中高危 89 个，中危 1877 个，低危 422 个，修复 265 个，未修复 2123 个。

扫描
处置
病毒
DDOS

事件 | 处置状态 | 详情

高危	中危	高危	高危	中危	紧急
处理完	处理中	处理中	未处理	处理中	处理完
SQL注入漏洞 CRM 192.168.58.11	CSRF跨站请求伪造 SDCMS 192.168.58.121	永恒之蓝蠕虫感染主机处置 业务支撑 192.168.38.155	远程命令执行漏洞	永恒之蓝蠕虫排查 192.168.11.135	XSS跨站脚本漏洞 OA 192.168.48.184

AI 控制指挥中心

战术行动 Tactical action

迷网	SOC	EDR	NDR	态势感知
事件数：5 已处置：4 知识库：28	事件数：1,456 已处置：324 知识库：0	事件数：2,503,456 已处置：1 知识库：55	事件数：3,456 已处置：24 知识库：1,257	事件数：156 已处置：132 知识库：8

战略框架 Strategic framework

安恒通	漏洞提交平台	外部情报	通报预警
情报数：357 知识库：25	情报数：35 知识库：20	情报数：3,856 知识库：10	情报数：256 知识库：35

DBAPPSecurity 安恒信息

西湖论剑

感谢您的聆听

祝您有个美好一天

安恒官网

安恒通

E安全

电话：400-6059-110

网址：www.dbappsecurity.com.cn

邮箱：cain.yuan@dbappsecurity.com.cn