安全态势感知工具

演讲者：鲁冰洁

00
自我介绍

鲁冰洁

在读计算机科学与技术学生，东北大学信息安全实验室成员，NEUQ-ACM俱乐部第五届常务副会长。

在校期间参加多项科创比赛，第八届全国大学生电子商务“创新、创意及创业”挑战赛省赛二等奖，数学建模美赛三等奖。现在主要研究方向为硬件安全。

CONTENTS
目录

01
漏洞案例

WannaCry
Heartbleed

01

漏洞案例

WannaCry

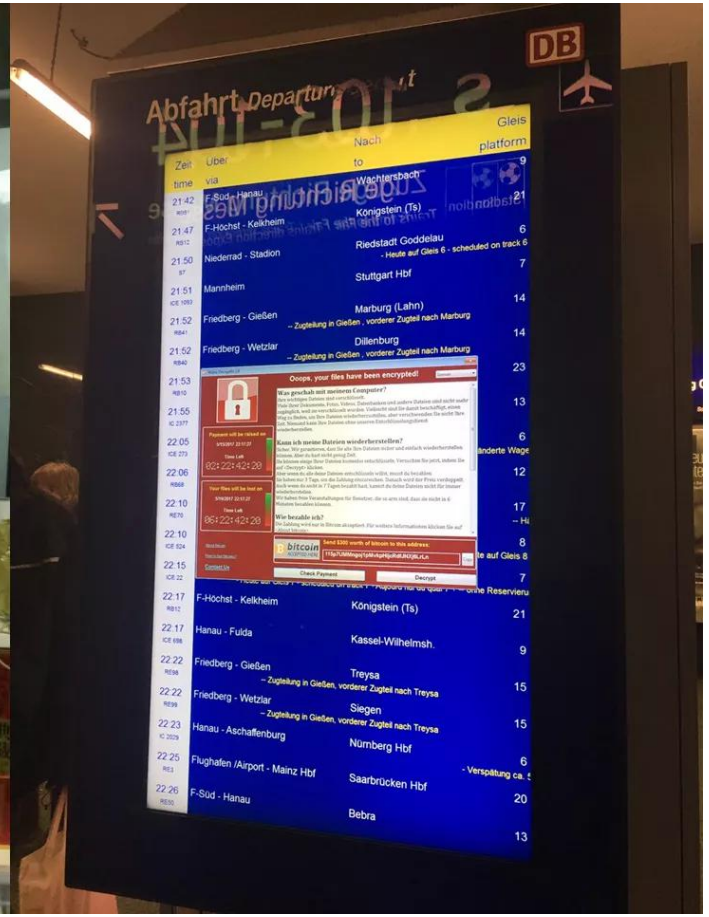
加密型勒索软件兼蠕虫病毒

01

漏洞案例

WannaCry

加密型勒索软件兼蠕虫病毒

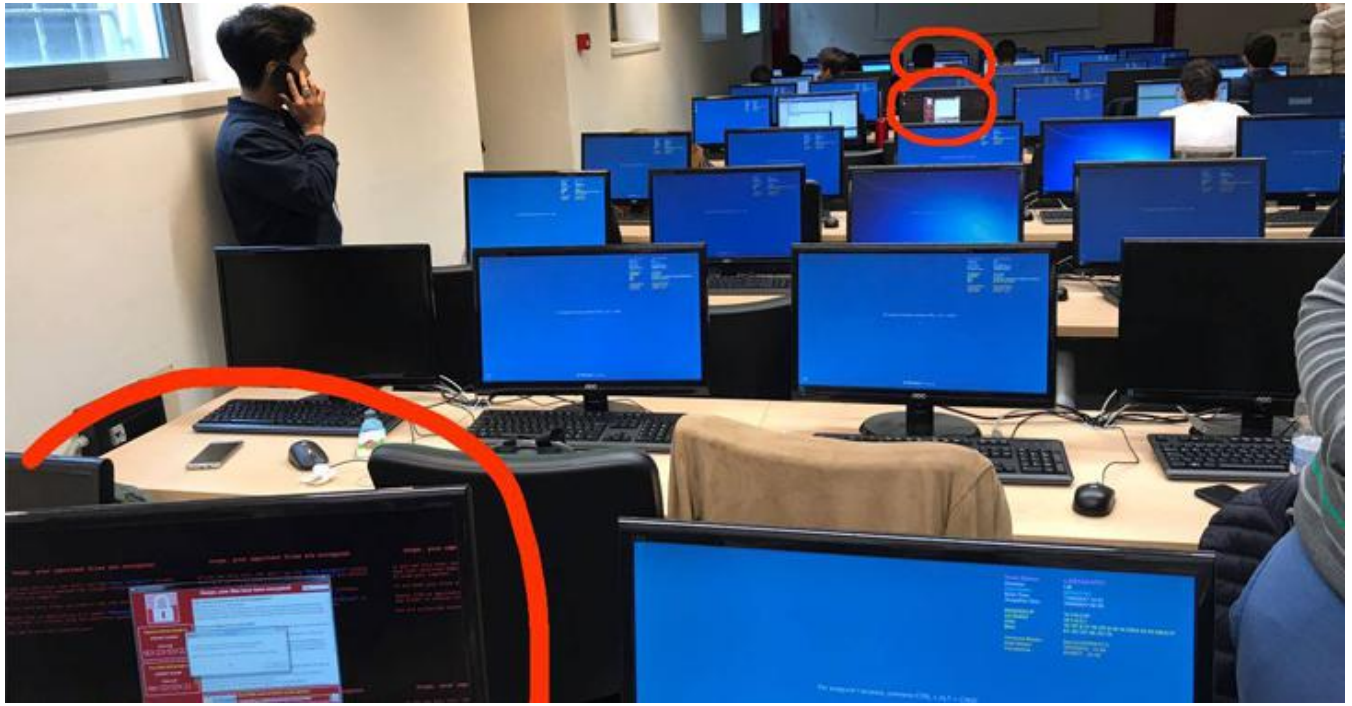


01

漏洞案例

WannaCry

加密型勒索软件兼蠕虫病毒



01 漏洞案例


“心泣（Heartbleed）” 漏洞是怎么回事
（就是这两天你到处都看到的那个OpenSSL漏洞啦）
原作 xkcd 汉化Ent@Gwokr
服务器，你还在吗？在的话请回复“POTATO”（6个字母）
User Meg wants these 6 letters: POTATO.
用户Meg需要这6个字母：POTATO
User Meg wants these 6 letters: POTATO.
POTATO
服务器，你还在吗？在的话请回复“BIRD”（4个字母）
these 4 letters: BIRD.
用户Meg需要这4个字母：BIRD

01 漏洞案例


嗯……
User Meg wants these 4 letters: BIRD.
BIRD
服务器，你还在吗？在的话请回复"HAT"（500个字母）
User Meg wants these 500 letters: HAT.
用户Meg需要这500个字母：HAT
HAT。卢卡斯请求"连接丢失"页面。伊芙（管理员）希望将服务器主密钥设为14835038534。伊莎贝尔请求关于"不太长的蛇"的页面。用户卡伦请求把账户密码改为……
User Meg wants these 500 letters: HAT.
yesky 天极网

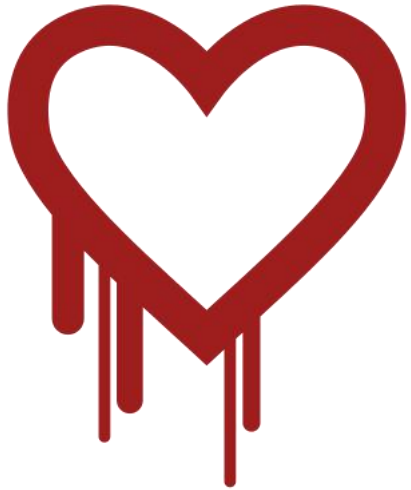
01

漏洞案例

Heartbleed

OpenSSL

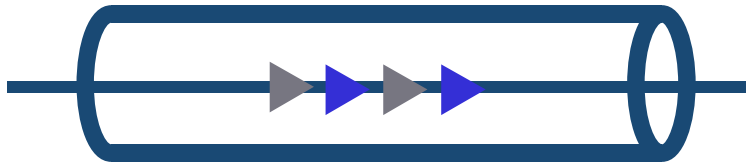
- 加拿大税务局
- 英国育儿网站Mumsnet
- 美国第二大营利性连锁医院



02
实现思路

设备探测
数据抓取
数据清洗
数据存储
数据搜索
数据交互

02
实现
思路

Zmap  设备探测

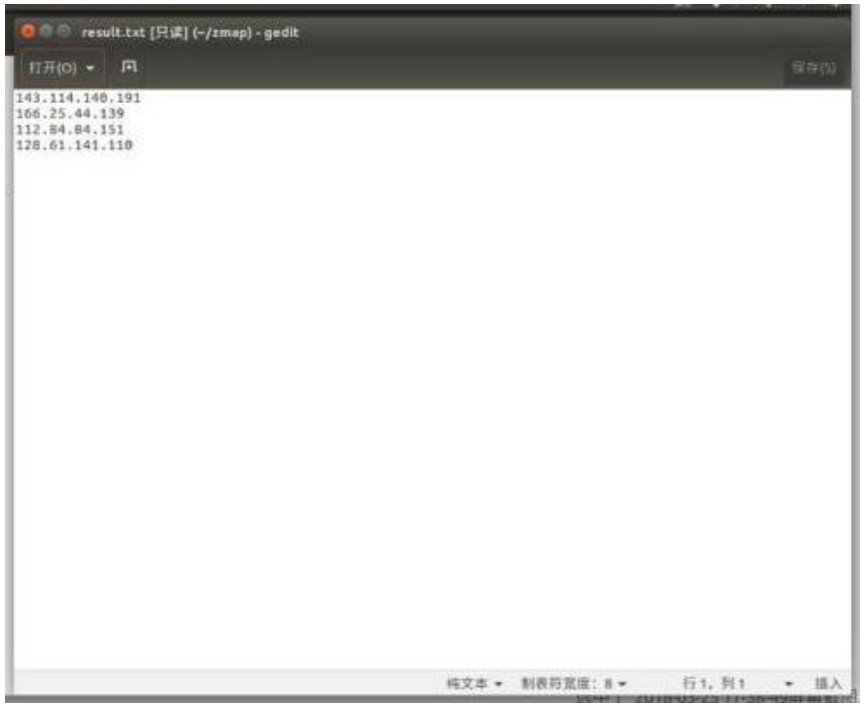
发现存活主机、开放端口，进而发现其运行的服务、操作系统等信息。

-p, --target-port=port
-o, --output-file=name
-b, --blacklist-file=path
-n, --max-targets=n
-r, --rate=pps
-B, --bandwidth=bps

02

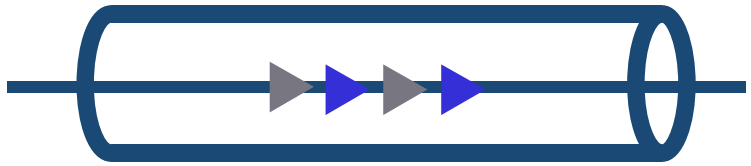
实现思路

zmap -B 10M -p 80 -n 10000 -o result.txt



02
实现
思路

Zgrab



数据抓取

获取每个IP相应的指纹信息。

02

实现思路

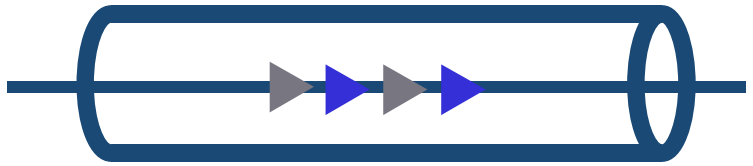
zgrab –port 80 –data http-req --output-file=banners.json


```
{
   "ip": "118.184.180.46",
   "timestamp": "2016-11-28T11:59:18-05:00",
   "data": {
      "read": "HTTP/1.1 200 OK\r\nServer: nginx/1.11.3\r\nDate: Mon, 28 Nov 2016 16:59:07 GMT\r\nContent-Type: text/html\r\nContent-Length: 612\r\nLast-Modified: Mon, 27 Jun 2016 07:56:31 GMT\r\nConnection: keep-alive\r\nETag: \"5770dc2f-264\"\r\nAccept-Ranges: bytes\r\n\r\n\u003c!DOCTYPE html\u003e\n\u003chtml\u003e\n\u003chead\u003e\n\u003ctitle\u003eWelcome to nginx!\u003c/title\u003e\n\u003cstyle\u003e\n    body {\n        width: 35em;\n        margin: 0 auto;\n        font-family: Tahoma, Verdana, Arial, sans-serif;\n    }\n\u003c/style\u003e\n\u003c/head\u003e\n\u003cbody\u003e\n\u003ch1\u003eWelcome to nginx!\u003c/h1\u003e\n\u003cp\u003eIf you see this page, the nginx web server is successfully installed and\nworking. Further configuration is required.\u003c/p\u003e\n\n\u003cp\u003eFor online documentation and support please refer to\n\u003ca href=\"http://nginx.org/\"\u003enginx.org\u003c/a\u003e.\u003cbr/\u003e\nCommercial support is available at\n\u003ca href=\"http://nginx.com/\"\u003enginx.com\u003c/a\u003e.\u003c/p\u003e\n\n\u003cp\u003e\u003cem\u003eThank you for using nginx.\u003c/em\u003e\u003c/p\u003e\n\u003c/body\u003e\n\u003c/html\u003e\n",
      "write": "GET / HTTP/1.1\r\nHost: 118.184.180.46\r\n\r\n"
   }
}
{
   "ip": "103.41.53.163",
   "timestamp": "2016-11-28T11:59:18-05:00",
   "data": {
      "read": "HTTP/1.1 200 OK\r\nDate: Mon, 28 Nov 2016 16:59:17 GMT\r\nServer: Apache/2.2.11 (Unix) DAV/2 PHP/5.2.14\r\nLast-Modified: Mon, 28 Nov 2016 07:43:48 GMT\r\nETag: \"26c00c-1b4ec-54257a1d17500\"\r\nAccept-Ranges: bytes\r\nContent-Length: 111852\r\nMS-Author-Via: DAV\r\nConnection: close\r\nContent-Type: text/html\r\n\r\n",
      "write": "GET / HTTP/1.1\r\nHost: 103.41.53.163\r\n\r\n"
   }
}
```

02

实现思路

分割数据的脚本工具

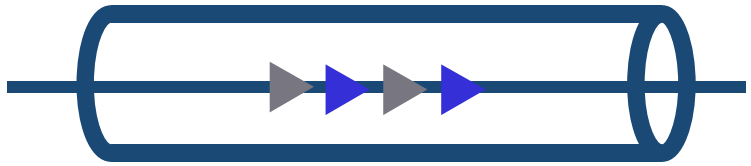


数据清洗

由于抓取到的指纹信息存在畸形格式和无法响应的IP，收集到的数据格式混乱，所以需要对这些数据进行预处理。数据预处理包括数据的分割和去除畸形格式两部分。

02
实现
思路

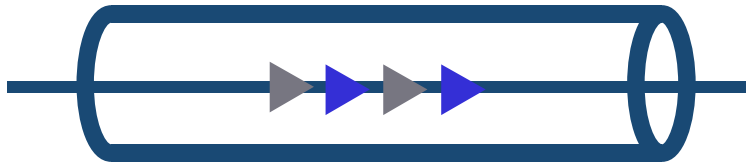
MongoDB



数据储存

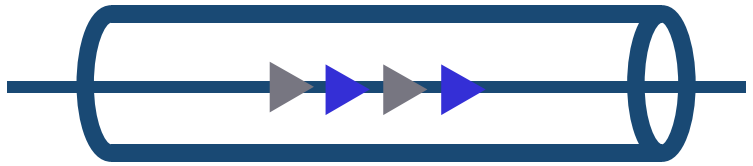
既可以满足数据的存储结构化，又可以存储较为复杂的数据类型，具有高性能、易部署、易使用的特点。

02
实现
思路

ElasticSearch  数据搜索

用JSON作为文档序列化的格式实现数据存储，并通过减少磁盘寻道次数来提高查询性能。

02
实现
思路

Laravel  数据交互

帮助用户进行数据交互，实现搜索IP指纹数据功能。

03
实例展示

全球服务器类型
HTTPS协议普及情况
Heartbleed现状

03
实例展示

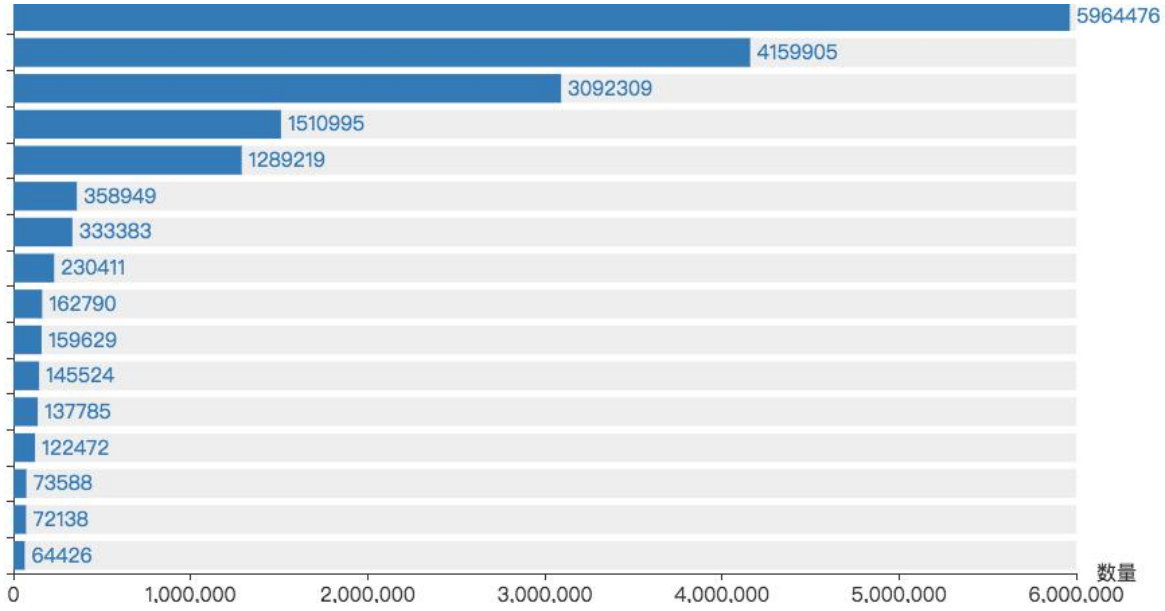

104.17.210.109
互联网空间探测系统
统计总览
全球态势
工控报告
用户手册
搜索结果
根据 104.17.210.109 搜索结果，共找到 1 条结果
104.17.210.109
[host] 104.17.210.109:80
[timestamp] 2017-11-21T02:30:28-05:00
[status] 403 Forbidden
[protocol] HTTP/1.1

03

实例展示

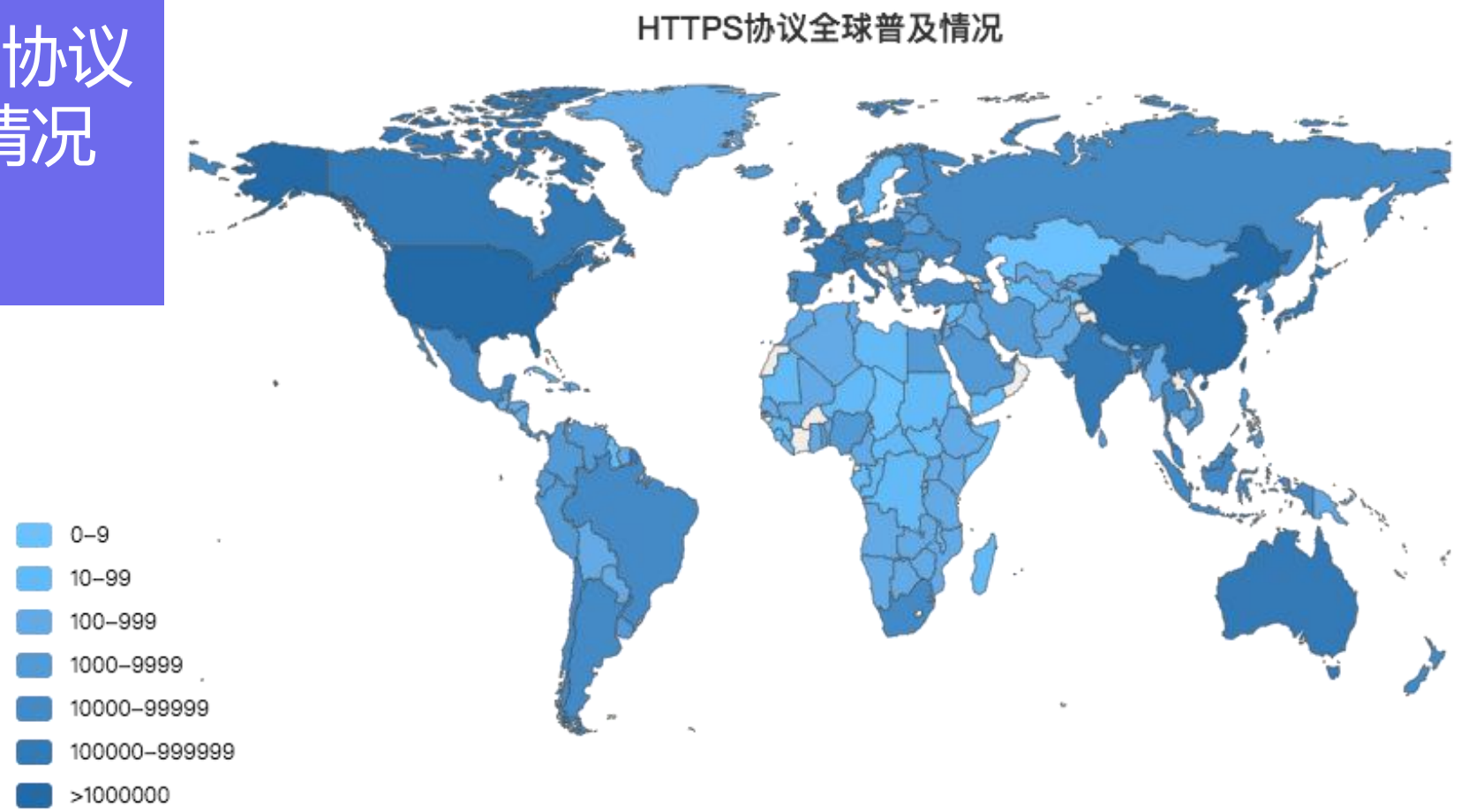
全球服务器类型

85%



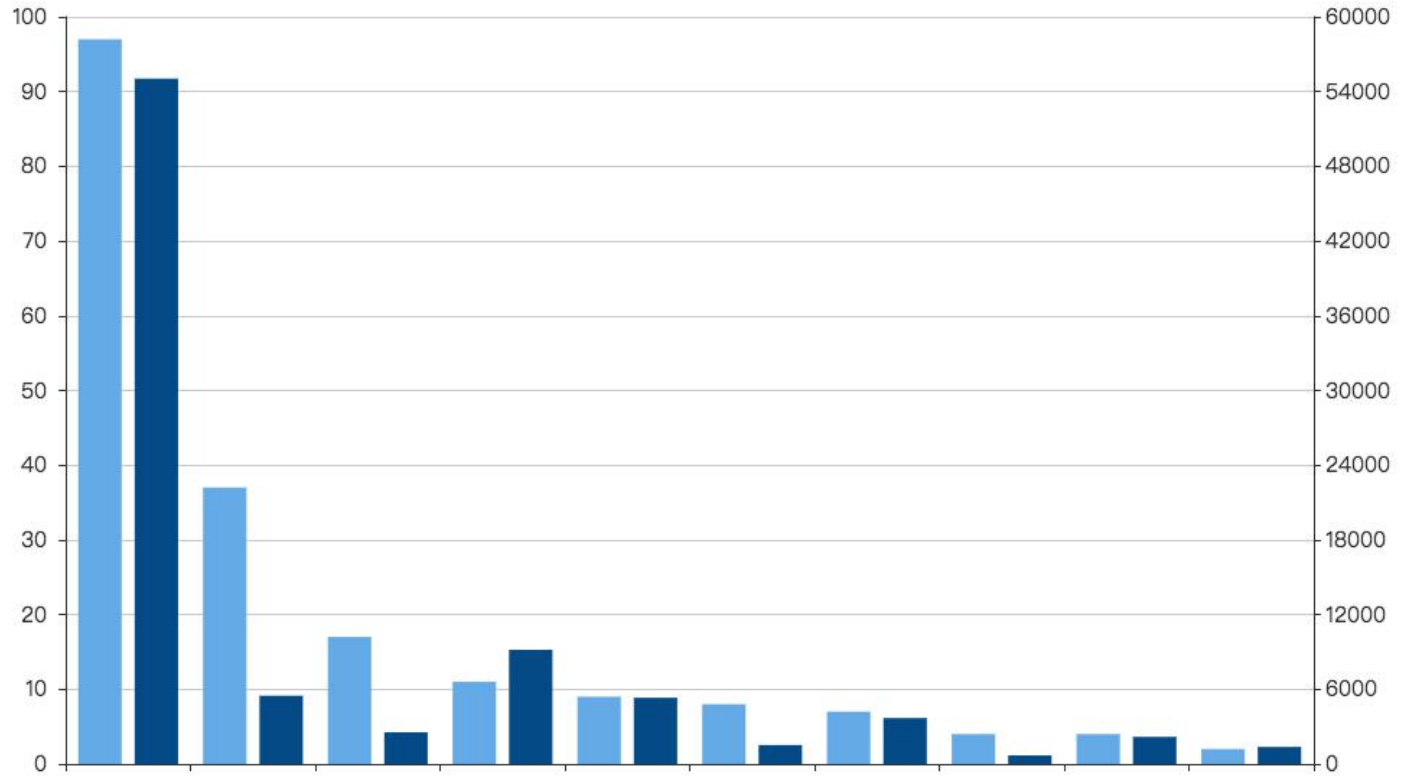
03
实例
展示

HTTPS协议普及情况



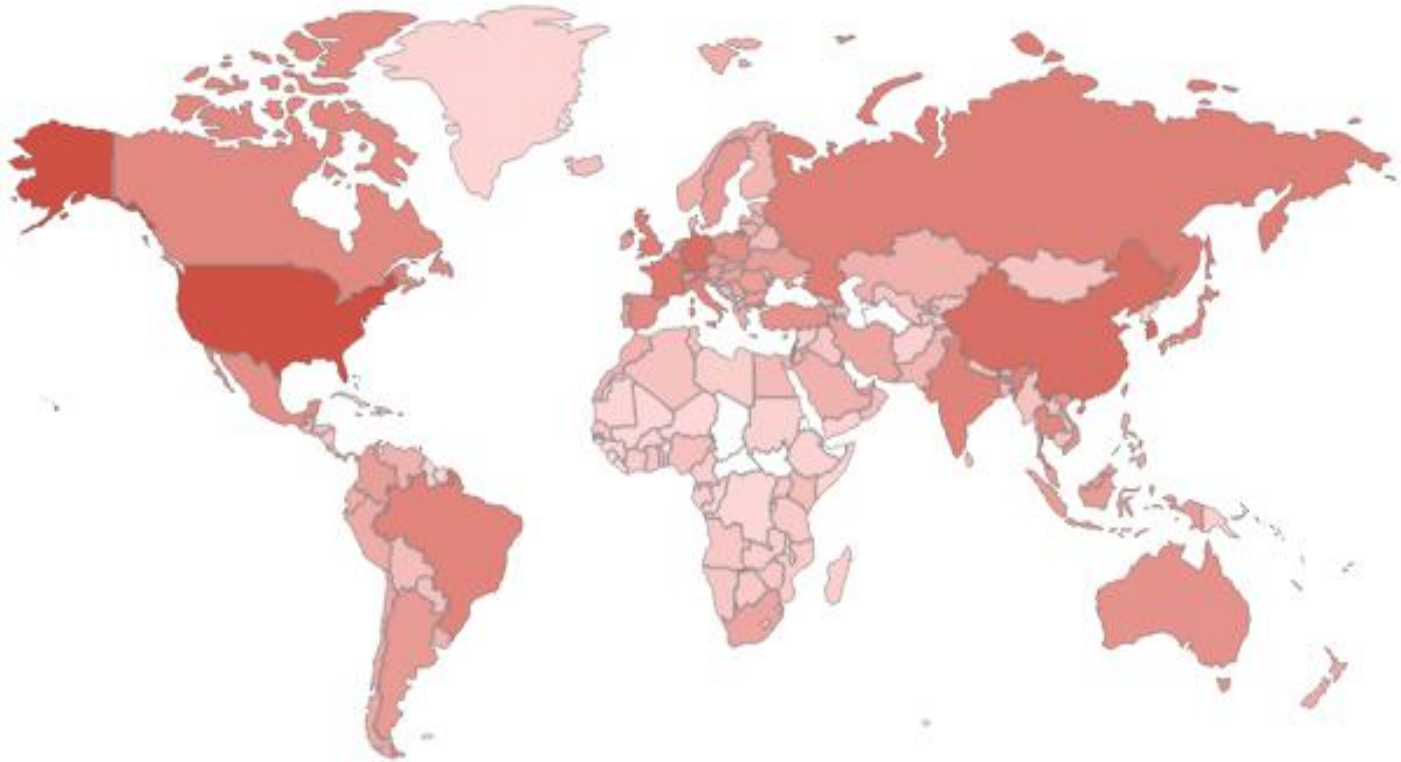
03
实例
展示

Heartbleed 现状



03
实例
展示

Heartbleed
现状



THANKS!