2017 年网络空间威胁与展望

知道创宇 404 实验室

版本	时间	描述
第一版	2018 年 3 月 19 日	完成《2017 年网络空间威胁与展望》第一版

目录

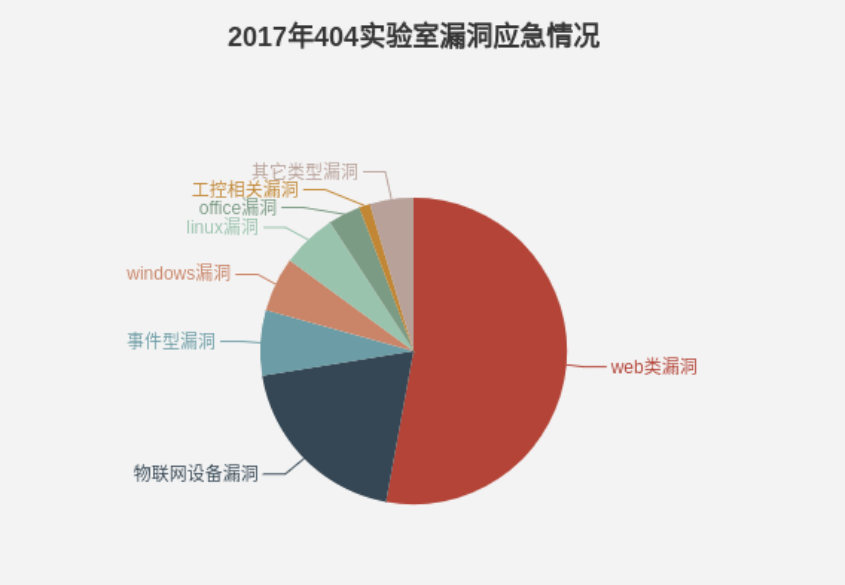
一．2017 年网络安全总体形势

1.1 2017 年网络安全总体形势

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施。网络安全被真正写入法律并实施，为国家从整体推动保障体系建设提供法律依据。一个全新的时代已经到来，时代将赋予了安全从业者更多的责任，推动他们作出更多的贡献。

随着媒体的不断曝光，普通大众也逐渐意识到我们身边存在各种各样的威胁，摄像头，路由器都可能被入侵、生活可能被监控。在这个万物互联的时代，各式各样的漏洞也随之而来，网络空间将面临给多的挑战。这也意味着安全防御已不是一隅之地，安全从业者的知识要有足够的深度和广度，才能够应对新出现的各种威胁。

2017 年，知道创宇 404 实验室(以下简称 404 实验室)一共应急了 91 个漏洞， Seebug 漏洞平台收录了 1394 个漏洞，涉及各操作系统、工控设备、网络摄像头、路由器、打印机等多个方面，其中各漏洞占比情况如下：



回顾这些漏洞，结合公司其他部门的相关数据，我们谨慎地提出以下观点：

2016 年公开的 Mirai 源码深远地影响了僵尸网络的发展。在 2017 年被曝光的僵尸网络中，我们看到了不少 Mirai 的影子，部分僵尸网络仅仅修改了 Mirai 源码中的攻击代码就在网络空间中传播。由于只需编写攻击代码就可以在网络空间中形成一个新的僵尸网络，所以漏

洞从被披露到被僵尸网络利用的时间也在不断缩减，这也意味着需要更加高效的安全应急响应才能保障网络空间的安全。

2017 年勒索软件造成的破坏不容小觑。WannaCry 勒索病毒在永恒之蓝漏洞的助攻下，席卷全球。大量未打补丁的 Windows 主机被感染，后续还出现了 NotPetya 以及 Bad Rabbit 等类似的勒索软件。这些勒索软件不仅仅对被攻击的电脑造成了损失，还在民众中引起了不小的恐慌。从勒索软件的应急结果来看，依然有部分民众网络安全意识薄弱，相关勒索软件仍然可能会卷土重来，公众的网络安全意识仍待加强。

随着物联网的发展，网络空间中的 IoT 设备数量仍在不断上涨，随之而来的安全问题不断涌现。从 2017 年应急的漏洞看来，目前被曝光的物联网设备的漏洞甚至可以追溯到十年之前，并且相似的问题在近几年也持续出现。各大 IoT 设备厂商急切地需要提升安全开发意识、积极修补漏洞、推动存在漏洞设备的固件补丁升级。但由于已有的 IoT 设备缺乏有效的更新机制，所以部分漏洞可能会在网络空间持续存在长达几年甚至几十年。

伴随着虚拟货币的热潮，挖矿行业逐渐兴起。从 2017 年下半年开始，网络空间的对抗的重点逐渐从僵尸网络转到与挖矿之间的斗争。攻防的对抗也促进了挖矿手法的进步，Coinhive.js、Satori 僵尸网络变种等都具有一定的代表性。控制目标主机不再是攻击者的最终目标，如何获取到更大的计算能力才是重点。可以预见的是：一旦虚拟货币热潮衰减或价值下降，挖矿行业会趋于低调。但新出现的各种挖矿手法都会被延用。

随着物联网的普及，网络空间安全的范围将会不断扩张。IPV6 网络也将逐渐走进人们的生活，万物互联的时代正在缓慢到来。这是机遇也是新的挑战。网络的范围在变大，可能的被攻击面也在增加。如何有效地在发展和安全中寻求平衡，需要所有人共同努力。

相较于已有的大型报告而言，该报告未必能将网络空间所有的威胁都有所体现。但我们仍将尽我们最大的努力，将 2017 年网络空间安全展现给大家。

1.2 年度安全漏洞或事件

2017 年 Seebug 漏洞平台一共收录了 1439 个漏洞，404 实验室应急了其中的 91 个漏洞。结合 2017 年网络空间相关事件，我们总结出年度安全漏洞或事件，有的是具有典型特

征的一类漏洞，有的是影响广泛的单个漏洞，我们亦希望通过这十个漏洞或事件来总结 2017 年网络空间的整体态势。

1.2.1 永恒之蓝

2017 年 4 月 13 日，永恒之蓝漏洞被曝光，随之曝光的还有十几个相关漏洞，但由于永恒之蓝漏洞最为大众所熟知，所以本小节标题为永恒之蓝。在该漏洞曝光后的一个月，5 月 12 日，臭名昭著的勒索软件 WannaCry 借其传遍全球，造成超过 80 亿美元的损失。在之后的半年的报道中，通过该漏洞传播勒索软件的事件(NotPetya、Bad Rabbit 等)不断涌现，甚至僵尸网络和挖矿行业也开始利用该漏洞传播其恶意程序。

1.2.2 GoAhead 摄像头漏洞

2017 年 3 月，Seebug 漏洞平台收录了多款网络摄像头的多个漏洞，后经证明，该漏洞存在于二次开发的 GoAhead 程序中。该漏洞在曝光后一个月内就被 HTTP81 僵尸网络使用，在短短的两天时间内，感染了大量摄像头。更有甚者，借助相关摄像头漏洞，通过非法侵犯他人家庭摄像头获利。在之后的网络空间中，该漏洞依然被其他僵尸网络使用(详情见 4.1.1：81 端口 GoAhead 摄像头已成为新僵尸网络传播的温床)。

1.2.3 华为 HG532 系列远程命令执行漏洞

该漏洞早在多年前就已经被华为修复，相关漏洞攻击代码并未流出。但由于修复时未发布相应的漏洞公告，互联网上仍然存在大量存在漏洞的路由器。Satori 僵尸网络就是利用该漏洞，迅速在互联网上传播。因此 Satori 僵尸网络可以说是 2017 年使用“0day”攻击形成的僵尸网络

1.2.4 Struts2 系列漏洞

Struts2 系列漏洞在安全届具有很高的人气，Struts2 框架被广泛使用，经常因为各种原因造成漏洞，可以用很简单的攻击方式拿到很高的权限，都是让它被广泛关注的原因。2017 年 Struts2 一共曝出多个漏洞，其中 s2-045、s2-052、s2-053、s2-054、s2-055 均可以实现远程命令执行。

1.2.5 Samba 远程命令执行漏洞

2017 年 5 月 24 日，Samba 官方发布安全公告，修复了一个严重的远程命令执行漏洞（CVE-2017-7494）。永恒之蓝漏洞影响了众多 Windows 主机，而该漏洞则影响了大量的

Linux 主机，由于该漏洞披露时间在 WannaCry 勒索软件爆发之后，故此该漏洞也被称为 SambaCry 。

1.2.6 fastjson 远程代码执行漏洞

2017 年 3 月，Java 三大 json 解析库之一的 fastjson 曝出存在远程命令执行漏洞。2017 年 12 月，fastjson 修复中的黑名单再次被绕过。相较于之前的 Java 序列化与反序列化漏洞，fastjson，Jackson 等更多的是由 Java 自身的反序列化漏洞造成的。

1.2.7 Python Package 钓鱼以及各种源污染

2017 年 06 月 02 日，paper.seebug.org 收录了 fate0 的一篇《Package 钓鱼》，通过上传伪造的第三方库就实现了 Python Package 钓鱼。更令人惊叹的是，国内国外大量政府互联网公司均有中招。在后期的跟踪中，我们发现 Python Package 钓鱼还实现了恶意代码的隐藏和进化。从单纯的收集被感染用户的主机名到具有一定混淆和隐藏性质的 Package 钓鱼，真令人防不胜防。与之类似的，npm 钓鱼，Vscode Extension 钓鱼等也存在同样的问题。

1.2.8 路由器漏洞系列

除却 3 中提到的华为 HG532E 系列路由器漏洞外，2017 年 404 实验室还应急了 16 个路由器漏洞，涉及 TP-LINK 、D-LINK 、NETGEAR 等多个品牌，相比于 2016 年，路由器漏洞增长明显。这些路由器漏洞，部分已经被用于传播僵尸网络，例如 D-LINK 的远程命令执行漏洞，NETGEAR 的远程命令执行漏洞等。可以预见的是，路由器漏洞仍会不断出现，在多层次威胁公共安全。需要厂商及时修复漏洞，用户及时更新固件，多方面努力消除威胁。

1.2.9 摄像头漏洞系列

除却 2 中提到的 GoAhead 系列摄像头以外，大华、Netwave 系列摄像头均出现过一定程度的漏洞，这些漏洞部分已经被用于传播僵尸网络，还有一部分漏洞被用于满足恶意攻击者的偷窥欲。相关报道在焦点访谈，财经等多处都有报道。由于摄像头和路由器都与大众生活息息相关，所以需要引起重视。

1.2.10 Java 反序列化漏洞

Java 反序列化漏洞在近几年不断兴起，2017 年 OWASP 排名中，Java 反序列化等不安全的序列化方式名列第八，由于该漏洞可以在存在漏洞的主机上执行任意命令，所以 Java 反序列化漏洞也被大量利用。通过 404 内部“炼妖壶”蜜罐项目可以观察到，Java 反序列化漏洞已经被黑产用于传播挖矿软件（详情见 5.1.3 和 5.1.4）。

二．2017 年网络空间大事记

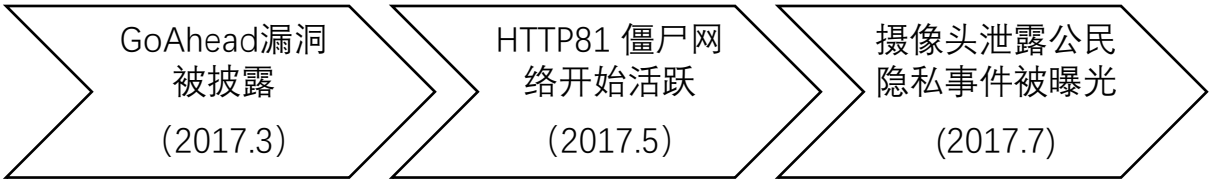
2.1 IoT 基础 Web 组件 GoAhead 漏洞事件

2.1.1 从隐私泄露到僵尸网络

2016 年 10 月的 Mirai 的出现为 IoT 安全带来了新的挑战，人们逐渐开始关注 IoT 设备的安全问题。2017 年 3 月，韩国安全研究者发布了一个有关 GoAhead 以及其他 OEM 摄像头的脆弱性分析报告，由于作为 Web 服务器的 GoAhead 普遍被使用在 IoT 设备中，此次报告波及多个厂商超过 1250 个不同型号的设备。

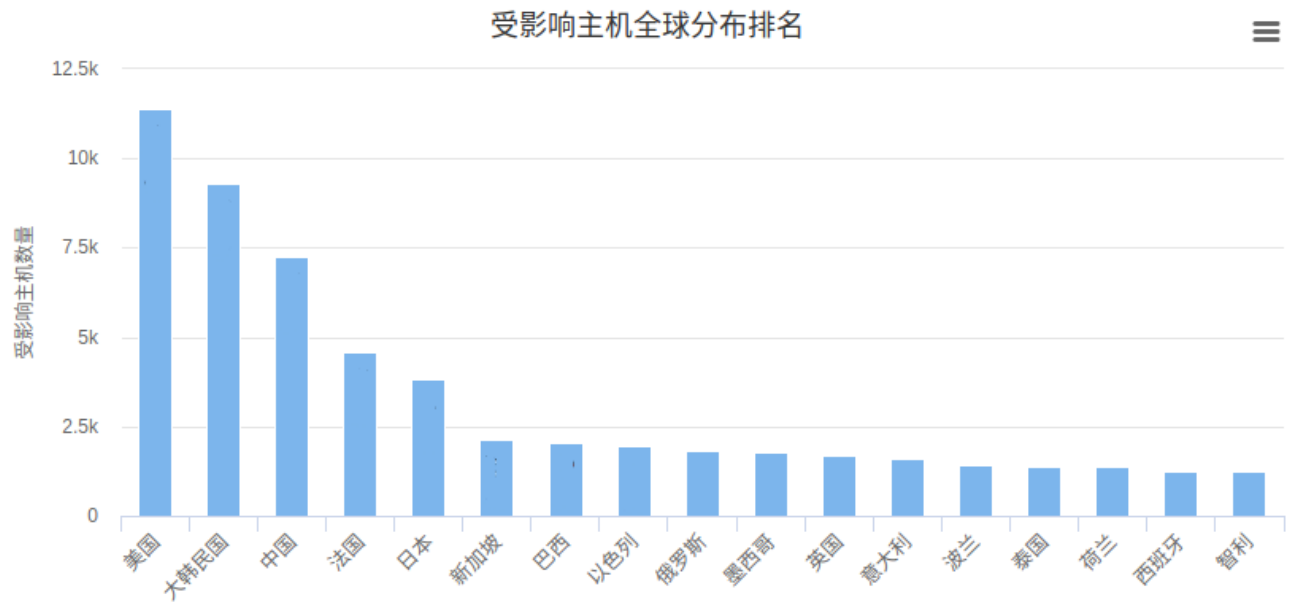
随后，地下从业者立马将其转化为生产力。2017 年 4 月，一款利用 HTTP 81 端口的僵尸网络异常活跃，控制超过 50000 台摄像头；2017 年 7 月，央视报道大量家用摄像头泄漏公民隐私——被“直播”。

相关时间线如下：

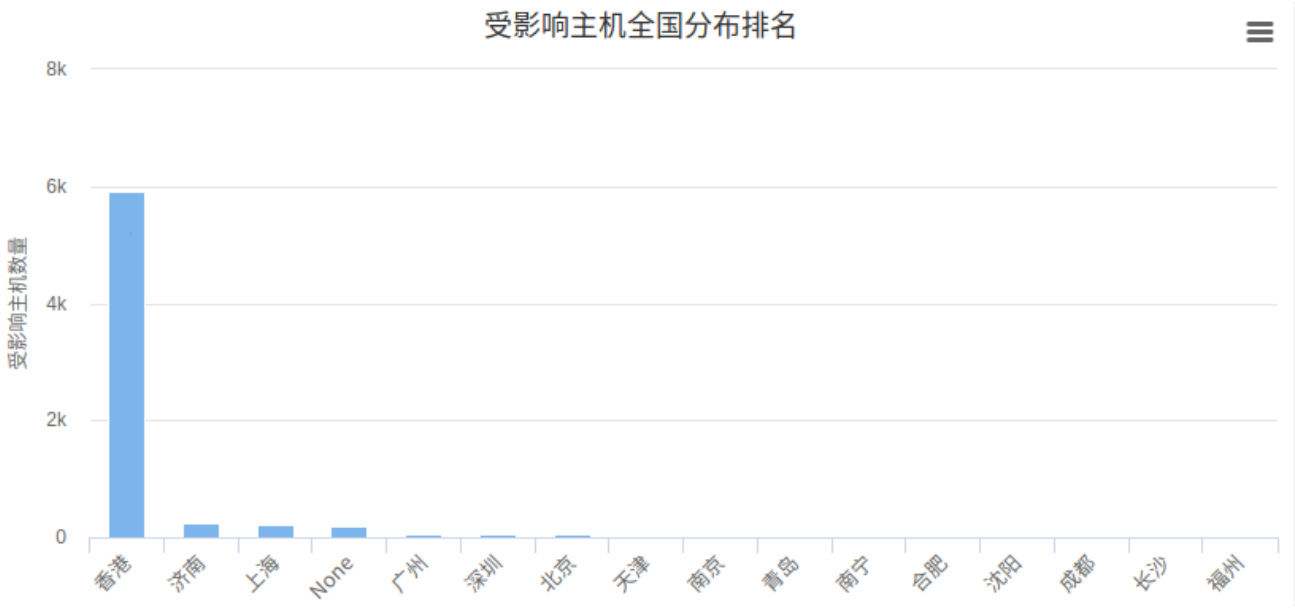


2.1.2 GoAhead 分布情况

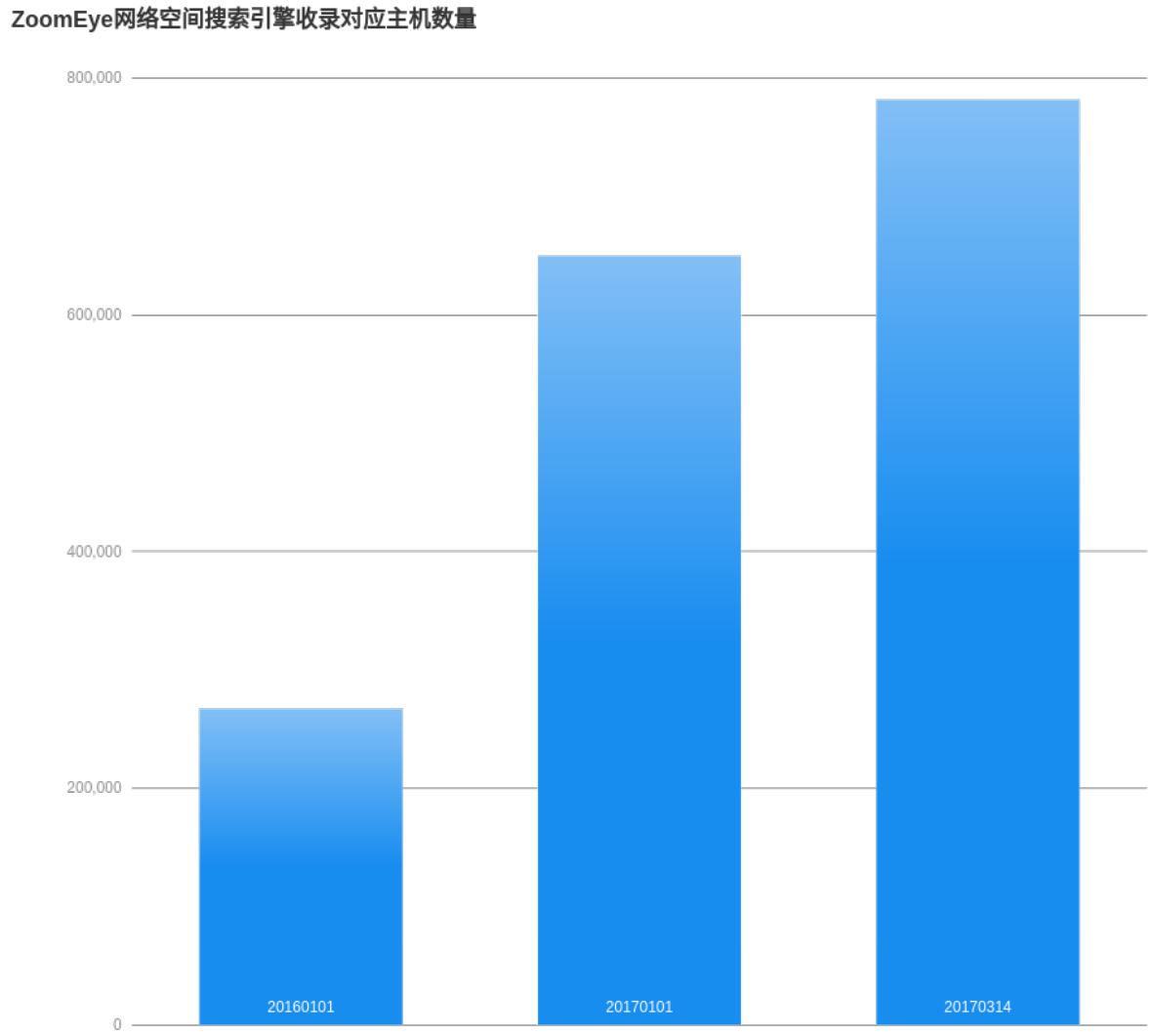
ZoomEye 网络空间探测引擎探测结果显示，在全球范围存在 7 万 GoAhead 设备存在被入侵的风险，其中美国、中国、韩国、法国、日本属于重灾区：



我国一共有 7000 多台设备可能被入侵，其中近 6000 台位于香港：



根据 ZoomEye 网络空间探测引擎探测的历史结果，我们分析出 GoAhead 设备增长速度极快，在 2016 年 1 月 1 日、2017 年 1 月 1 日和 2017 年 3 月 14 日收录包含 GoAhead 5ccc069c403ebaf9f0171e9517f40e41 的 banner 的设备数目分别是：26 万台，65 万台，78 万台。其中存在漏洞的版本也有类似的增长速度：



2.2 核弹级漏洞 永恒之蓝等泄漏

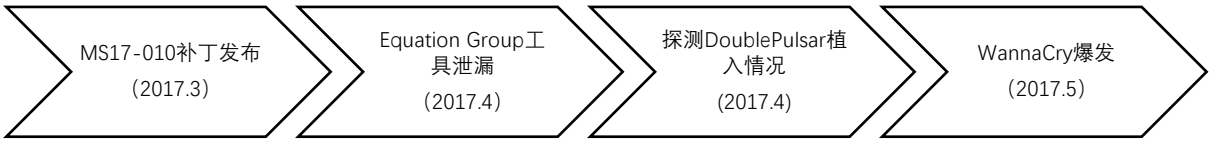
2.2.1 MS17-010 时间线

2017 年 4 月 14 日，Shadow Brokers 组织公布了此前窃取的部分方程式（Equation Group）组织的机密文件，其中包含多个黑客工具以及可用于攻击 包括 Windows 在内的多个系统漏洞，其中 "永恒之蓝"(Eternalblue) 无疑是一枚具有核弹威力的攻击模块。

在泄漏的文件中还包含一个 DoublePulsar 后门程序，配合 Eternalblue 可在 Windows XP，Windows Server 2003，Windows 7 和 8 以及 Windows 2012 上运行；

永恒之蓝利用 SMB 服务器的漏洞 MS17-010，而该漏洞实际在 2017 年 3 月已经由微软发布了更新补丁，但由于种种原因未能及时更新，导致 2017 年 5 月 12 日 WannaCry 的爆发，影响了超过 150 个国家，造成的经济损失高达 80 亿美元。

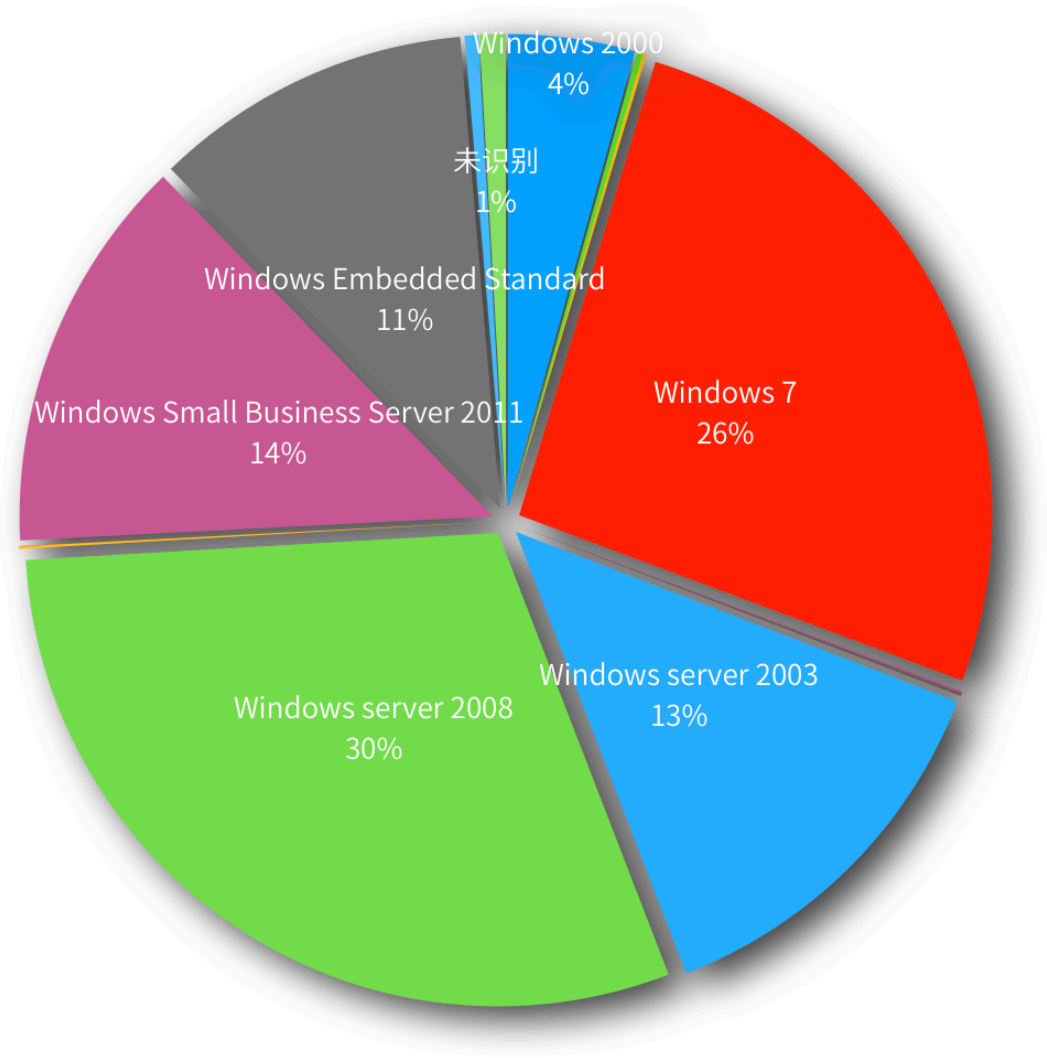
相关时间线如下：



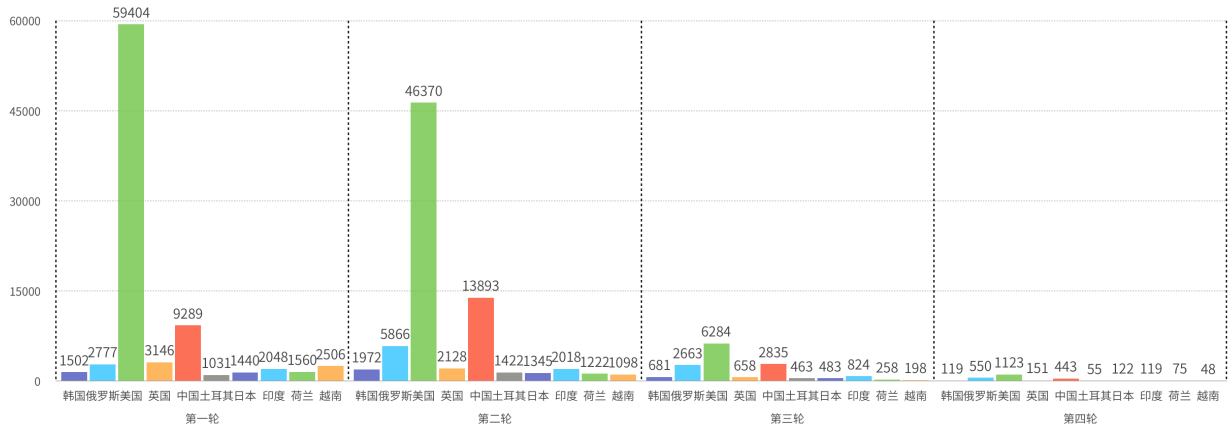
2.2.2 Doublepulsa 后门植入以及修复情况

ZoomEye 网络空间探测引擎在 2017 年 04 月 24 日，2017 年 05 月 02 日，2017 年 05 月 07 日，2017 年 5 月 18 日 对 Doublepulsa 后门植入情况进行共 4 轮探测。

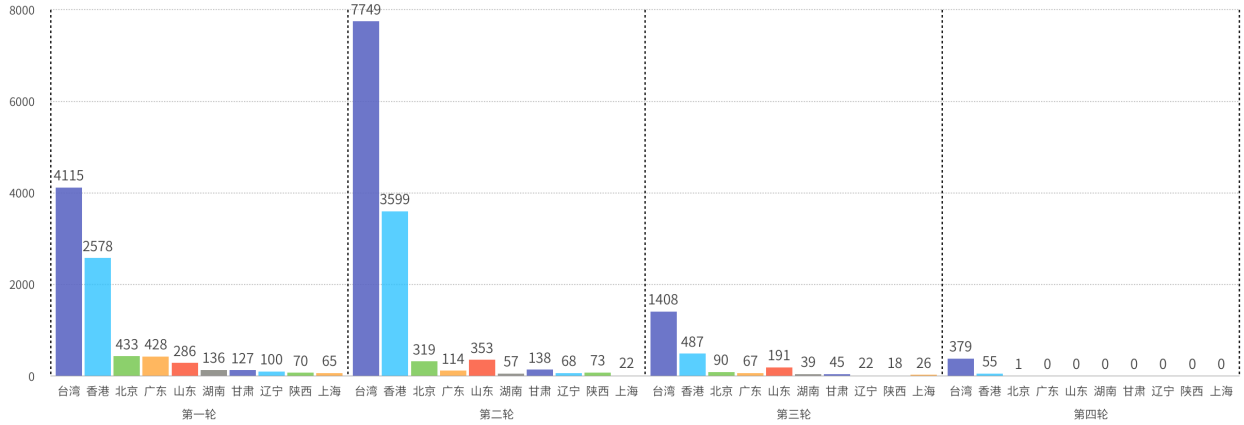
在第 3 轮探测中，我们尝试获取被植入 Doublepulsa 后门主机的系统信息，其中我们成功获得了 12017 台主机的系统信息。通过对收集的信息进行分析，我们可以发现 Windows 2008 和 Windows 7 是主要被感染的系统，而 Windows 8/8.1 仅有 7 台、Windows 10 仅 12 台 、Windows Server 2012 仅 10 台 和 Windows Server 2016 仅 2 台。这也从侧面解释了 WannaCry 肆虐时被感染的主机大多是 Windows7 和 Windows Server 2008 的原因。



通过分析 4 轮探测的数据，可以发现各国都非常重视 Doublepulsa 后门的清理情况，下面是 4 轮探测 Doublepulsa 植入情况柱状图：



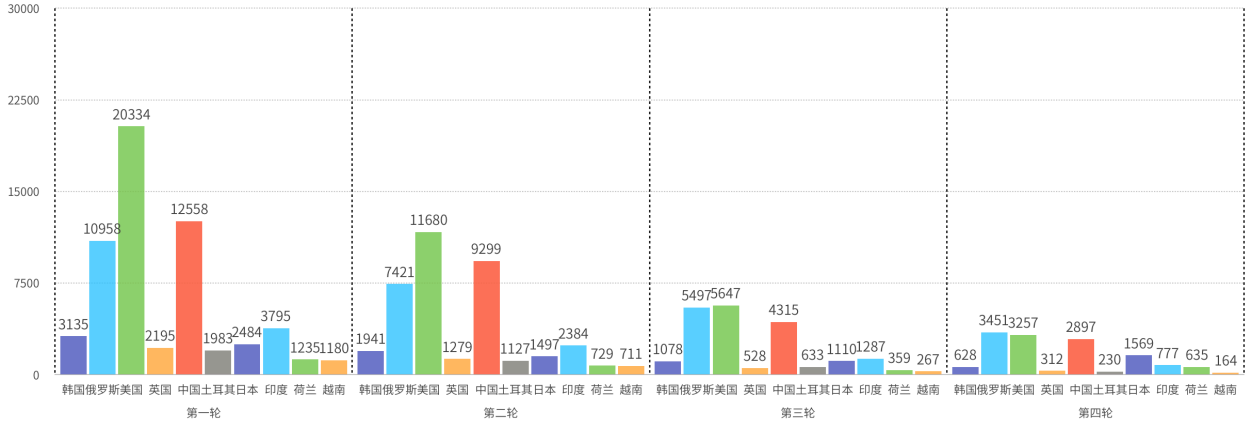
国内 Doublepulsa 后门被植入最多的是台湾省，这可能和大陆限制 445 端口通信有关系，下面是国内 4 轮探测 Doublepulsa 植入情况柱状图:



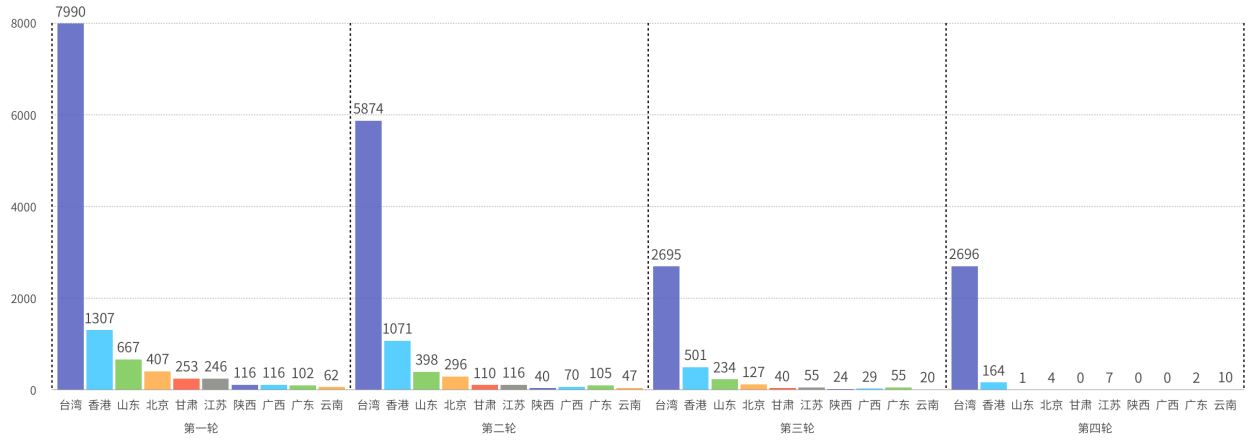
2.2.3 MS17-010 修复情况分析

与此同时，ZoomEye 网络空间探测引擎也对 MS17-010 进行了四轮探测。通过分析 4 轮探测的数据，MS17-010 的修复情况和 Doublepulsa 后门的清理情况相似，也是在不断的减少；但由于 WannaCry 勒索病毒的爆发促进了 MS17-010 漏洞的修复，所以 MS17-010 修复情况要优于 Doublepulsa 后门的清理情况。

全球 MS17-010 SMB 系列远程命令执行漏洞主机柱状图：



国内 MS17-010 SMB 系列远程命令执行漏洞主机柱状图：



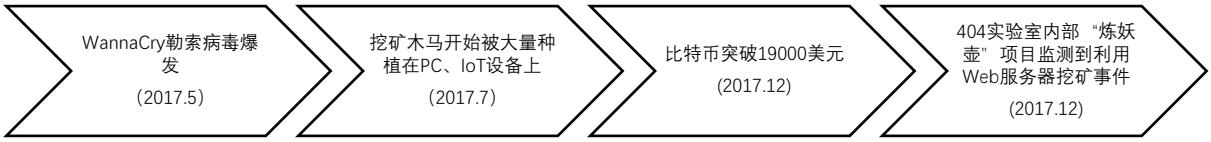
2.3 数字货币热潮

2.3.1 数字货币爆炸式增值

2017 年，数字货币掀起了一股 "炒币" 热潮，大量数字货币都呈爆炸性的增长趋势，其中升值最疯狂是比特币，在 2017 年 12 月突破了 19000 美元。由于数字货币的匿名性，WannaCry ，NotPetya ，Bad Rabbit 等勒索软件都将比特币作为支付方式。

在数字货币增长的热潮中，地下从业者也看到了商机，纷纷投入到挖矿事业中。挖矿的技术也是不断的更新，地下从业者从广撒网投放挖矿木马的方式，逐步转向一些高性能的 Web 服务器设备。

相关时间线如下：



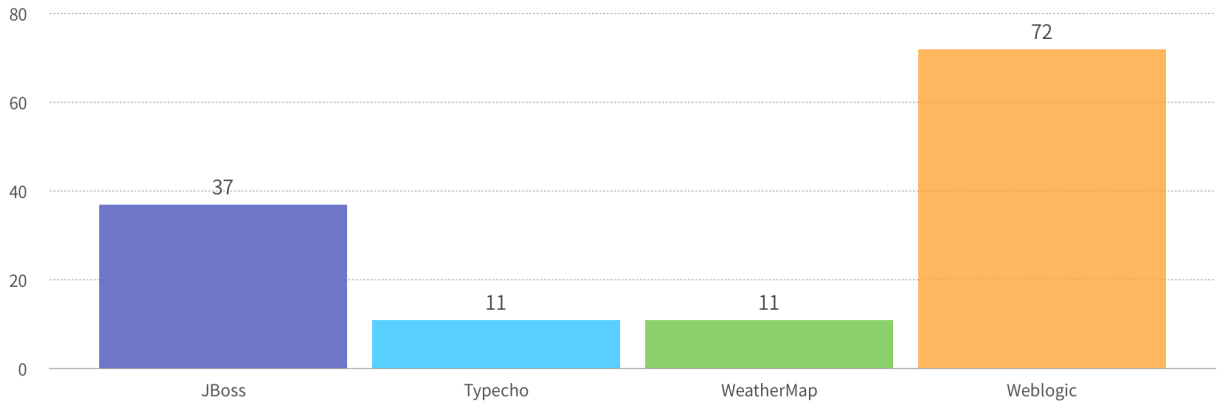
2.3.2 勒索软件推动比特币一路走高

随着勒索软件的爆发，直接促进了数字货币的增值，比特币更以指数型的速度在增长；从 2017 年初的 1000 美元，增长到 2017 年 12 月的 19000 美元，增值近乎 20 倍：

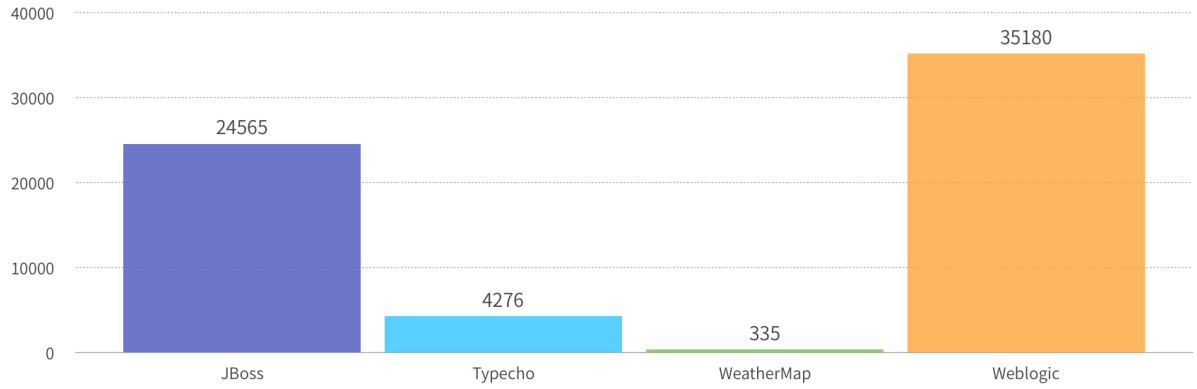
2.3.3 挖矿新技巧：多种利用服务器挖矿手法介绍

2017 年，404 实验室监测到多种新型的挖矿方式，2017 年 4 月，在对 Mesos 框架进行研究的过程中，我们发现相关容器管理平台资源已经被用于挖矿。2017 年 11 月，DNN 远程命令执行漏洞被用于感染挖矿程序，被感染主机继续通过永恒之蓝漏洞在内网感染。2017 年 12 月，在利用 Weblogic 漏洞挖矿事件后，通过内部 "炼妖壶"项目捕捉到的流量，我们还发现利用多种漏洞交叉感染的挖矿手法（具体内容在 5.1 节：职业选手和临时工中有具体介绍）。

关于交叉感染的挖矿行为，我们通过捕获流量分析出受到影响的组件包括： JBoss，Typecho，WebLogic，WeatherMap，其中 WebLogic 受影响最为严重，捕获到的攻击流量占总量的 50%。



就捕获的流量来看，目前这种挖矿方式正属于萌芽阶段，但互联网上仍然存在着大量受影响的主机，通过 ZoomEye 网络空间搜索引擎探测发现，JBoss 和 WebLogic 数量较多，分别是 24565 台和 35180 台，需要引起相关的重视。



三．物联网安全

3.1 物联网安全总体趋势

据 IT 研究与顾问咨询公司 Gartner 年初预测，2017 年全球物联网设备数量将达到 84 亿，比 2016 年的 64 亿增长 31%，而全球人口数量为 75 亿。2020 年物联网设备数量将达到 204 亿。

2017 年物联网设备总数将首次超过全球人口总数。可以说，这是物联网井喷式发展的一年。

而与如此快的发展速度相对应的，物联网的安全问题也是日趋凸显，尤其是网络摄像头、路由器、打印机、NAS（网络存储）等，频频被曝出漏洞。

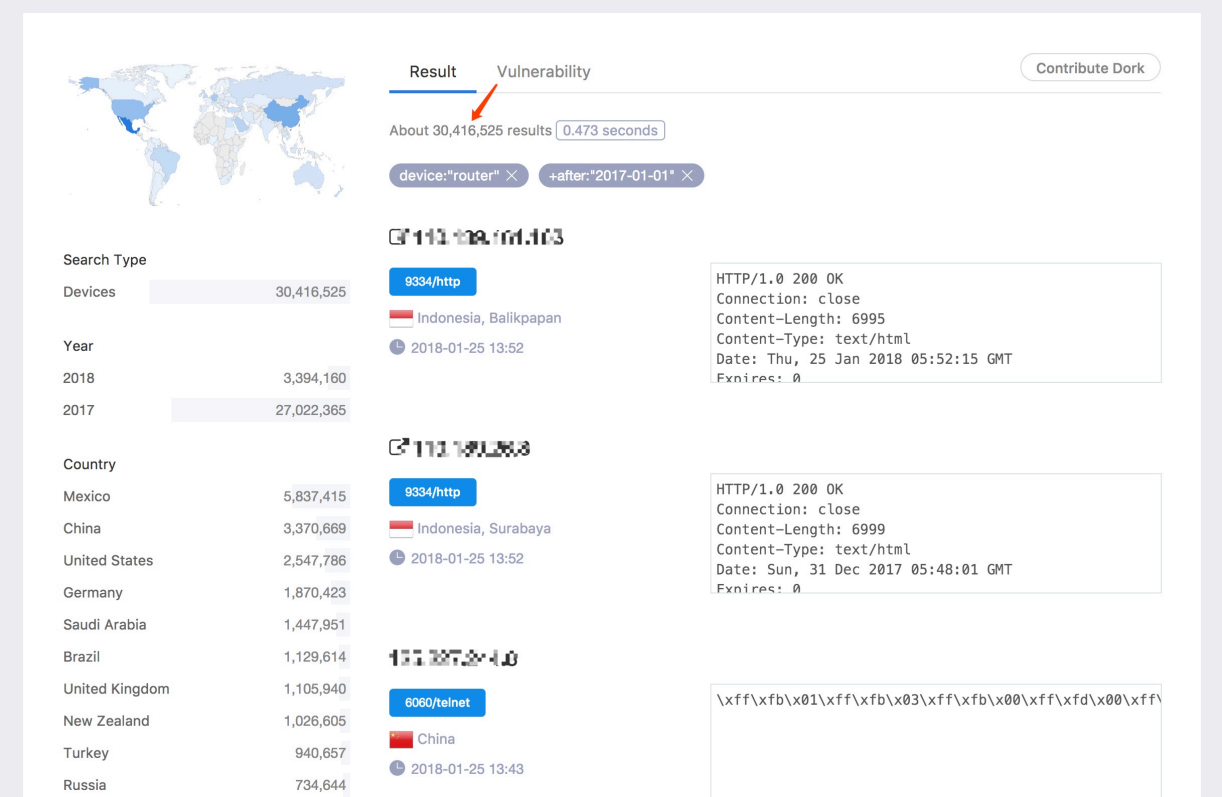
3.2 常见设备公网暴露情况

3.2.1 路由器

路由器是互联网络的枢纽，遍及整个网络。

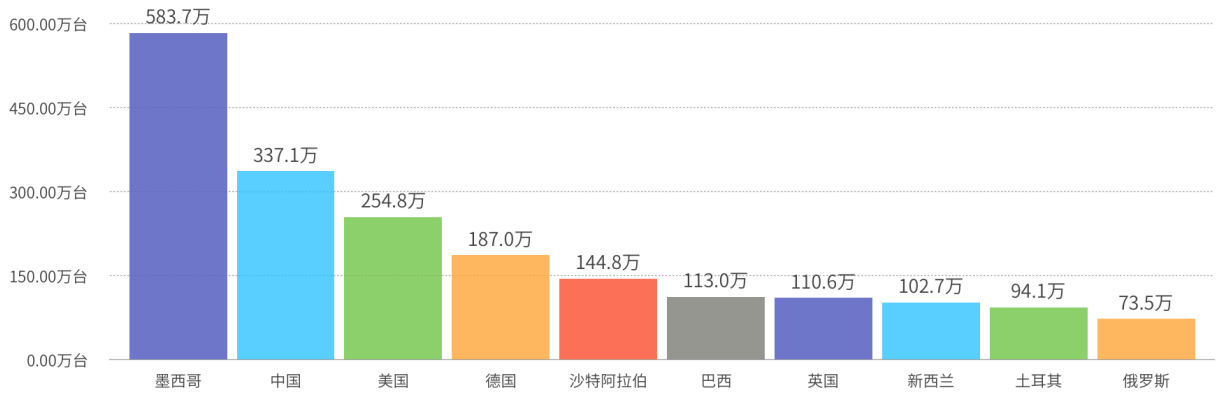
设备总量：

数量：30,416,525（台）



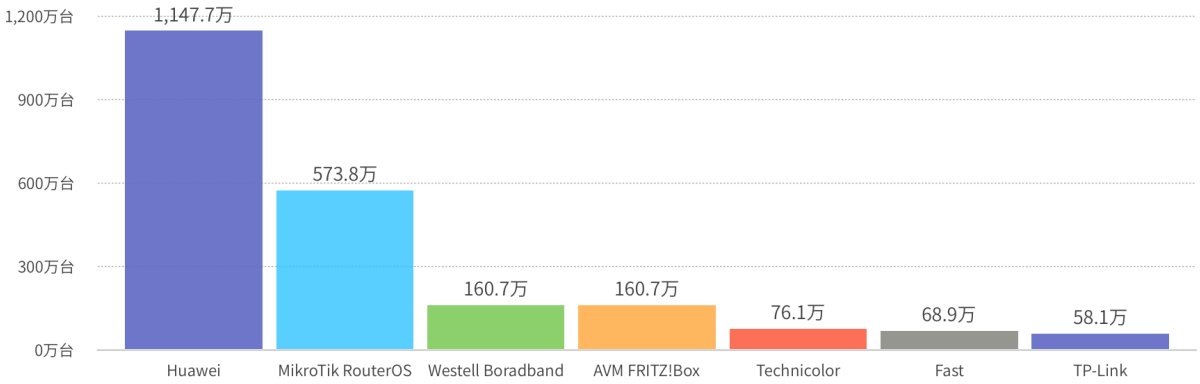
国家分布

数量前三的国家依次为：墨西哥、中国、美国。



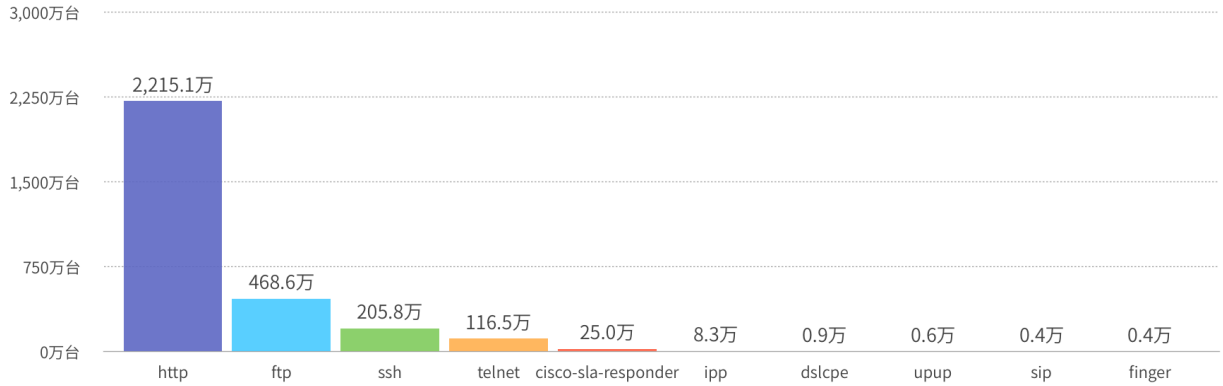
厂商分布

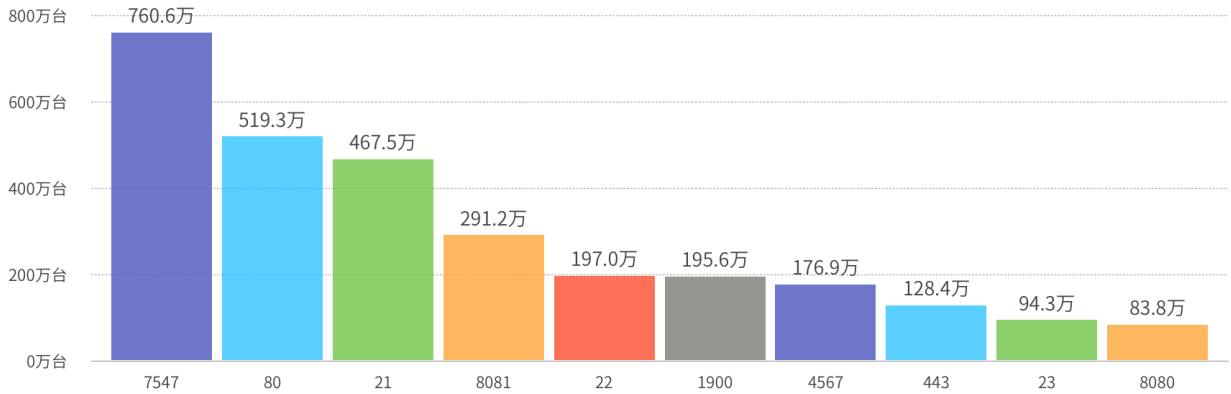
数量最多的依然是华为路由器设备，数量达到了惊人的 1100 万，约占互联网路由器总量的 1/3。其次是 RouterOS，MikroTik 旗下的 RouterOS 是一种路由操作系统，并通过该软件将标准的 PC 电脑变成专业路由器，公网数量约 573 万。此外，Westell 路由器和 AVM FRITZ!Box 路由器均达到了 160 万的量。



服务及端口分布

暴露最多的依然是 HTTP 服务，主要服务在 80 和 7547 端口。值得一提的是，约有 760 万路由器开放了 7547 端口，该端口多次被曝出漏洞，是一个攻击者经常利用的“热门”端口，通过发送基于 TR-069 或 TR-064 协议的指令对路由器发起攻击。其次依次是 FTP 服务（21 端口）、SSH 服务（22 端口）、TELNET 服务（23 端口）。



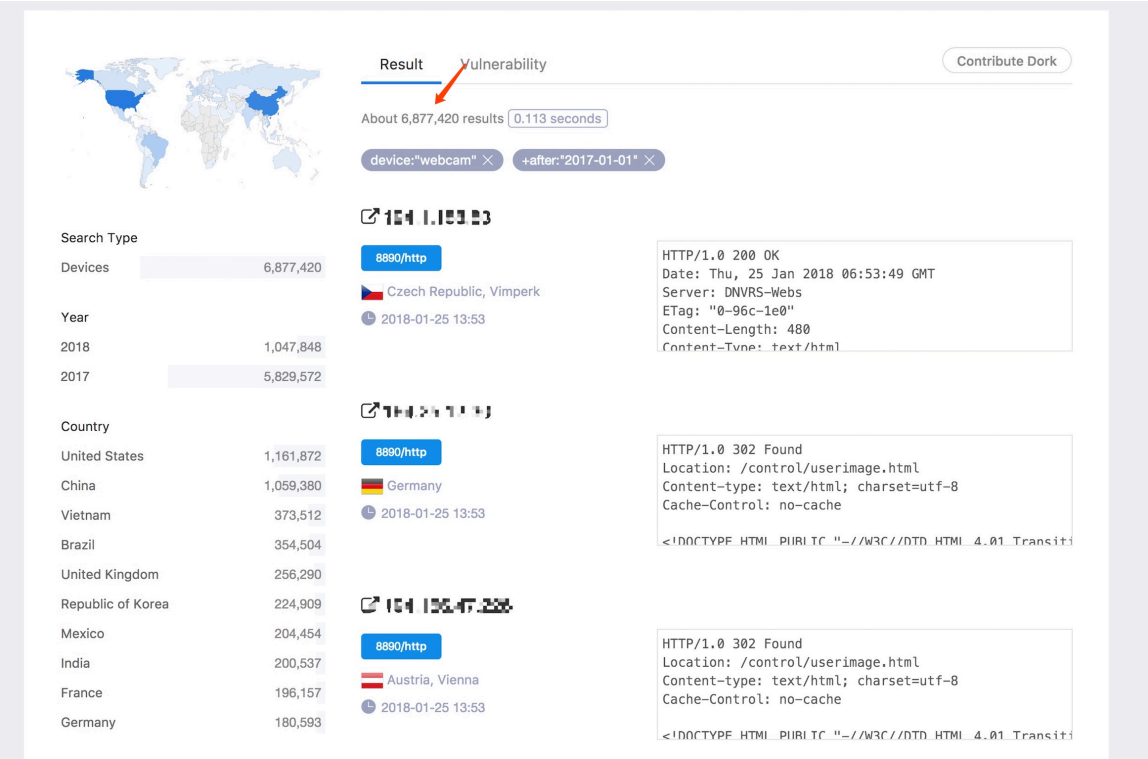


3.2.2 视频监控类设备

随着网络技术的发展，远程观看的网络监控摄像头已经逐渐取代了传统的模拟监控摄像头。越来越多的摄像头暴露在公网上，在方便了用户的同时，也成为一个新的攻击面。

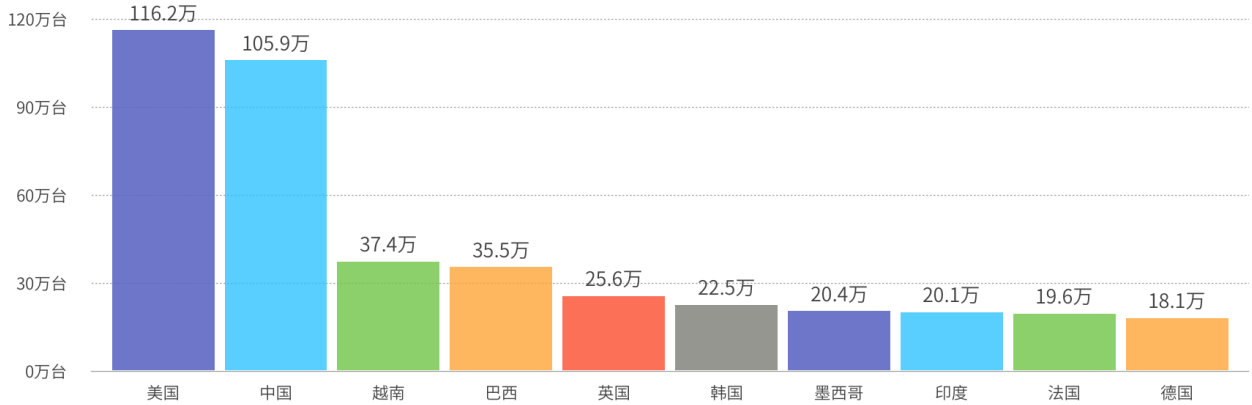
设备总量

数量：6,877,420（台）



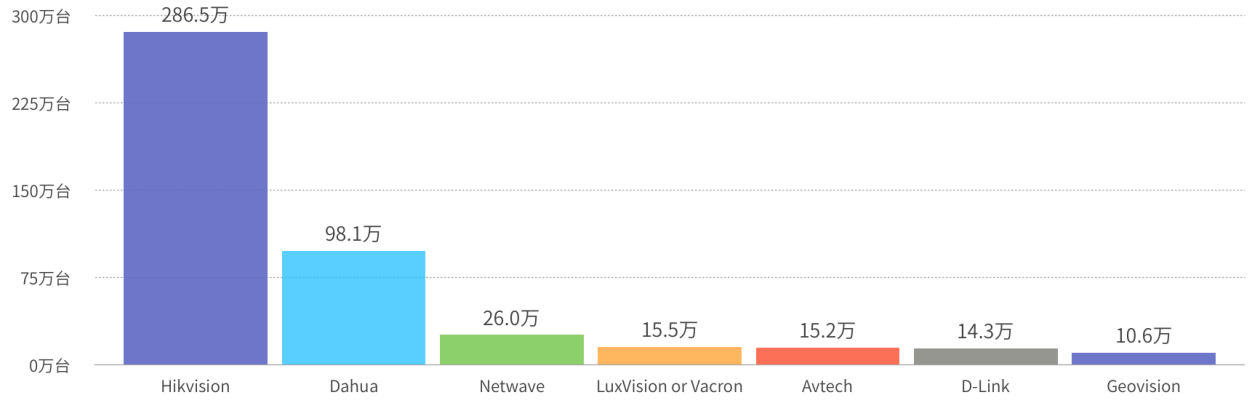
国家分布

美国、中国的数量最多，均超过了 100 万台。



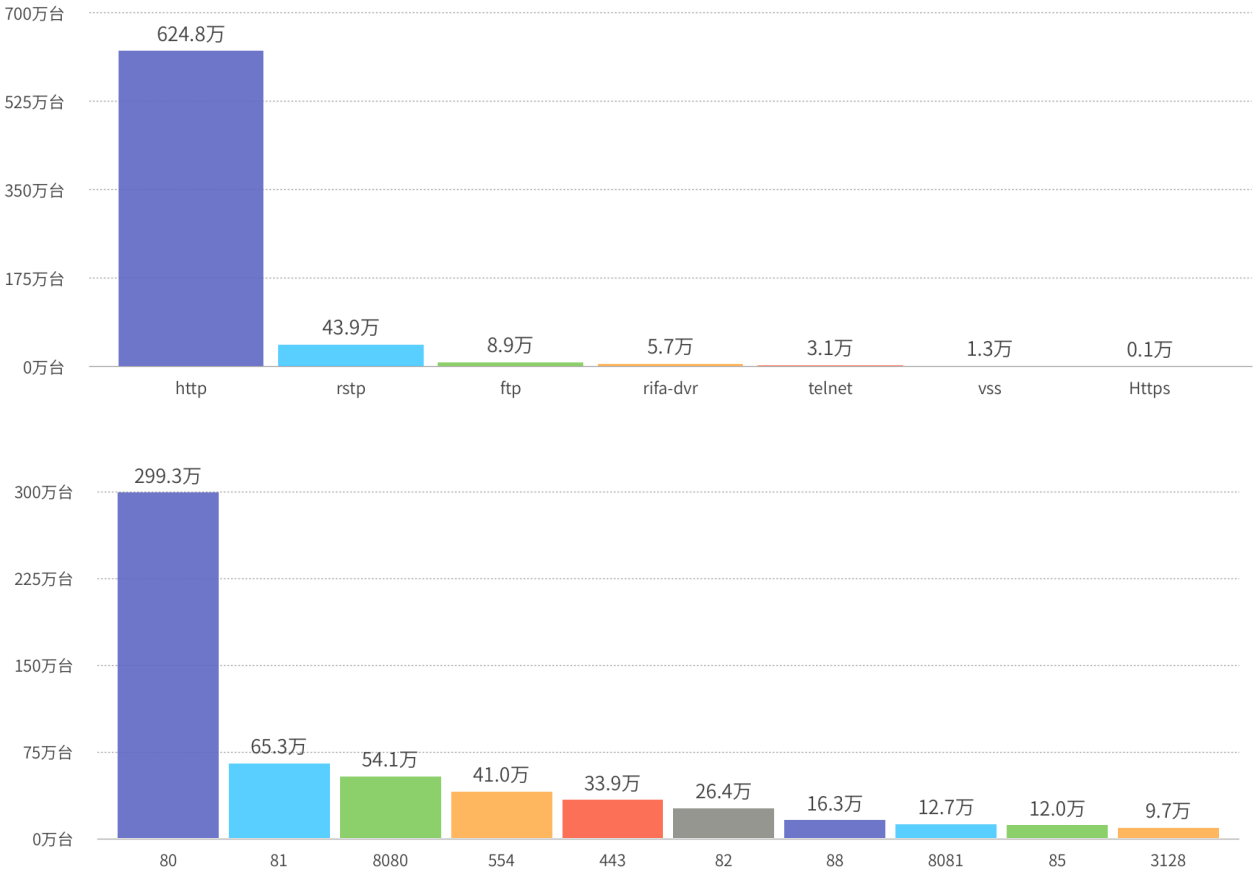
厂商分布

海康威视稳坐头把交椅，数量为 286 万台，约占 40% 的市场份额。其次为大华，数量约为 98 万台。



服务及端口分布

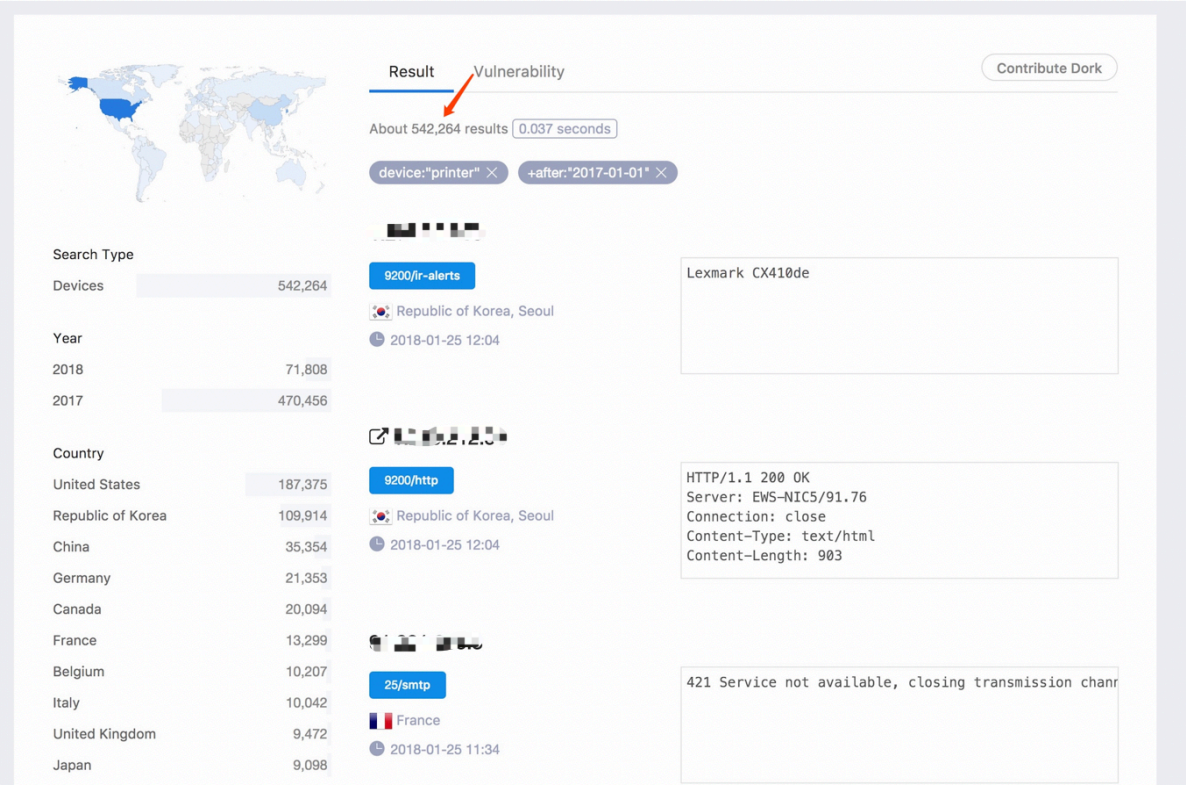
暴露在公网的绝大多数为 HTTP 服务，服务于 80 端口。



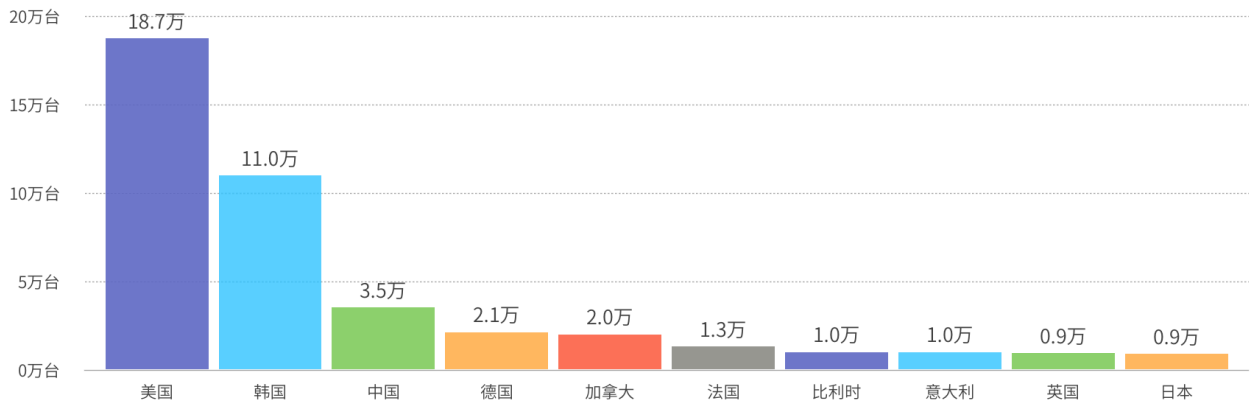
3.2.3 打印机

设备总量

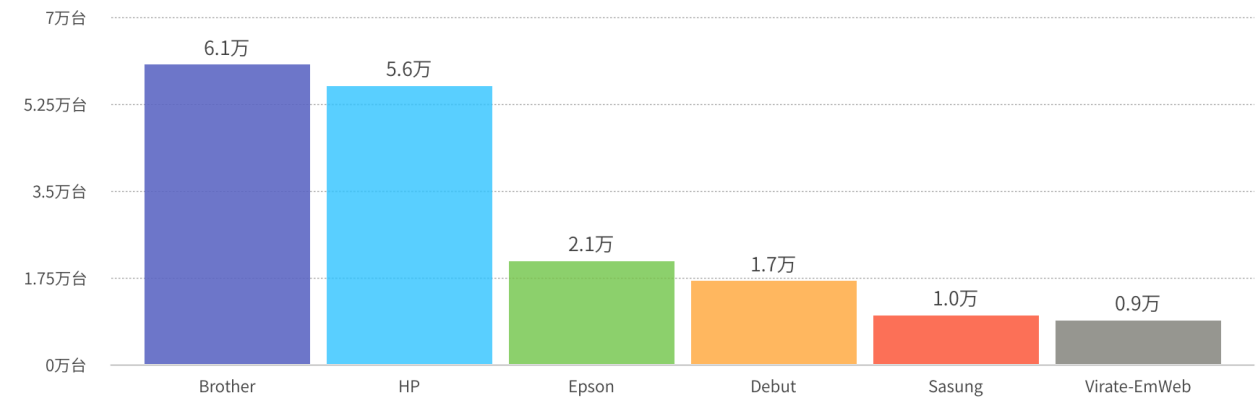
数量：542,264（台）



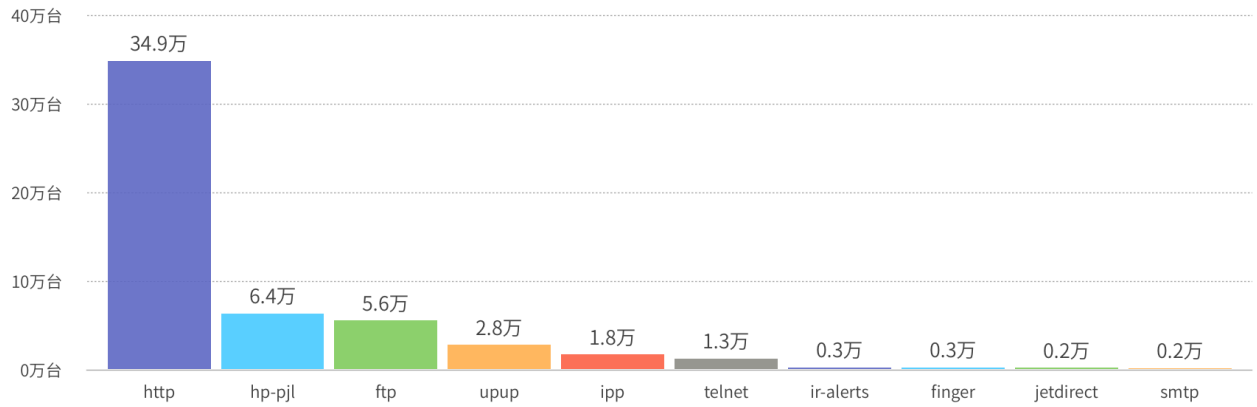
国家分布

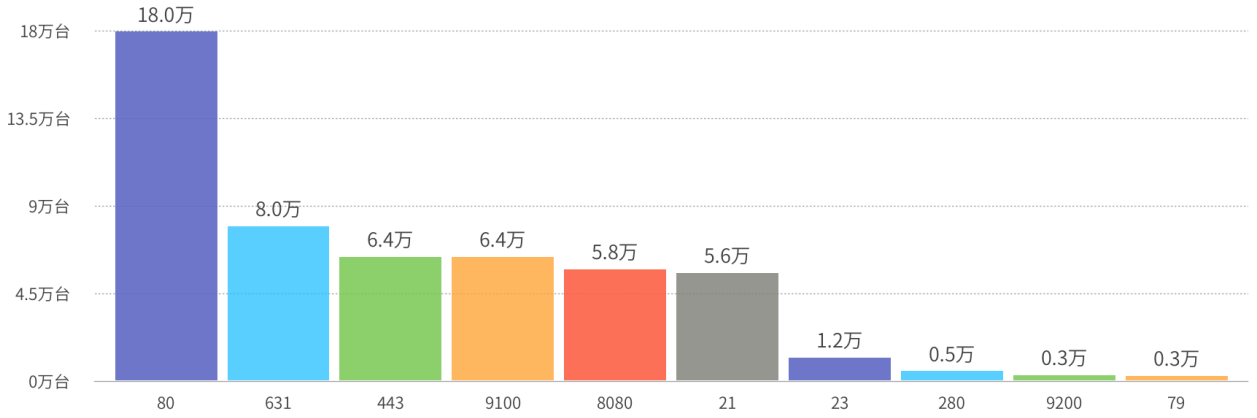


厂商分布



服务和端口分布

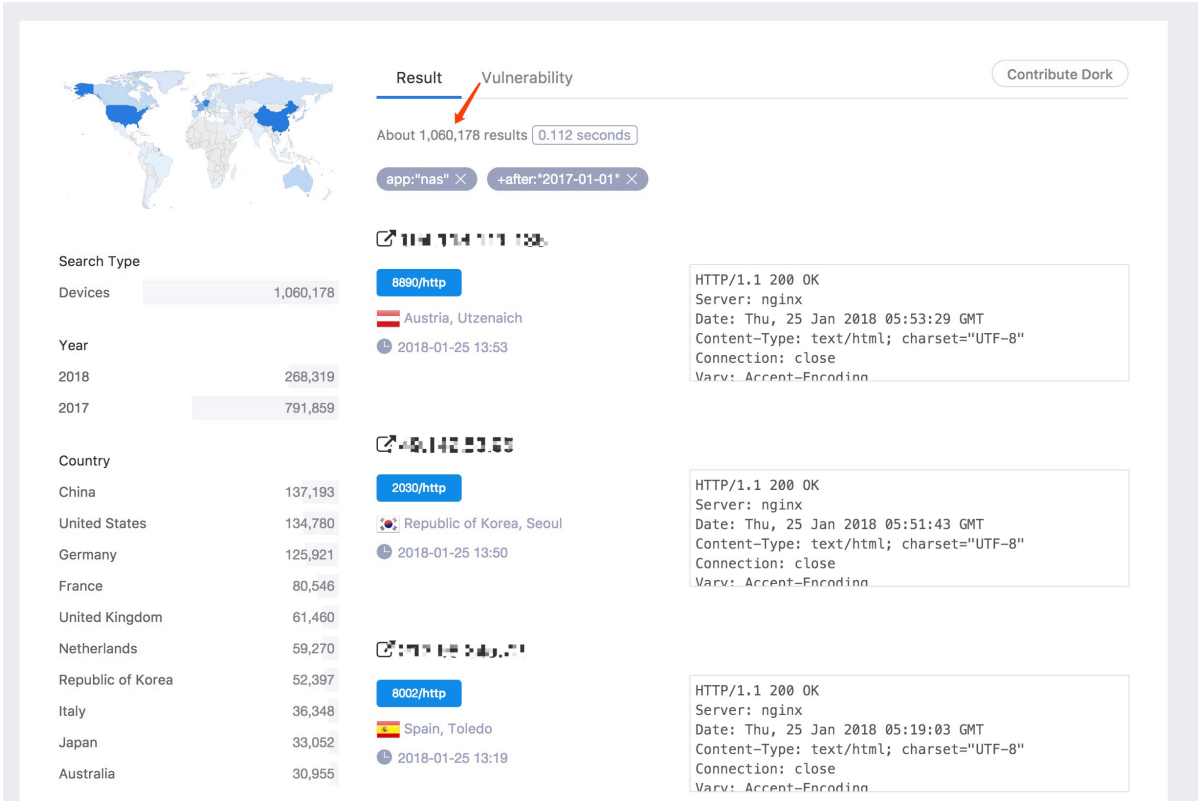




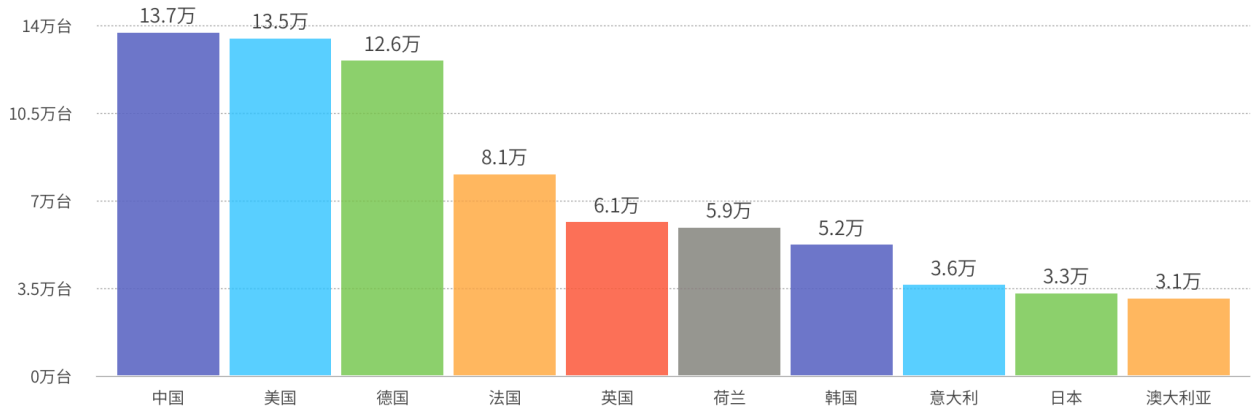
3.2.4 网络存储设备（NAS）

设备总量

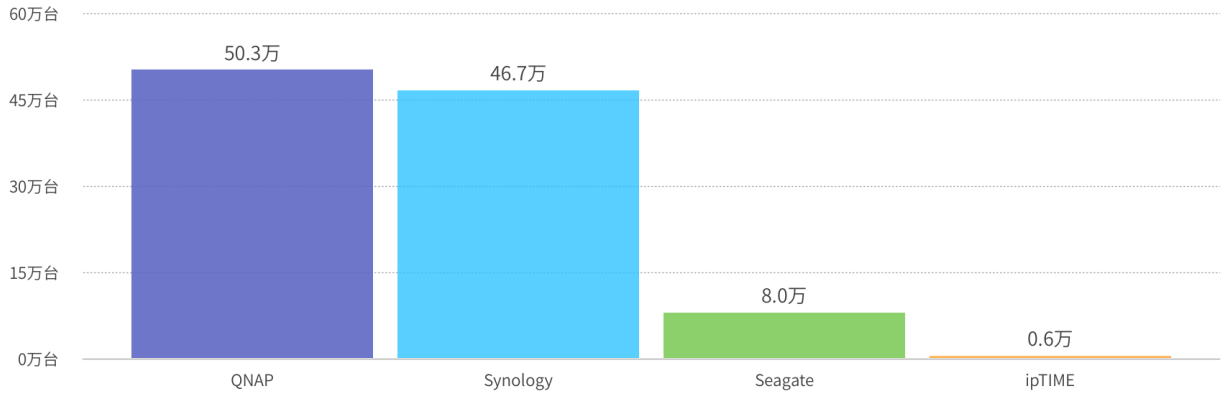
数量：1,060,178


Result
Vulnerability
Contribute Dork
About 1,060,178 results
0.112 seconds
app:"nas"
+after:"2017-01-01"
Search Type
Devices 1,060,178
Year
2018 268,319
2017 791,859
Country
China 137,193
United States 134,780
Germany 125,921
France 80,546
United Kingdom 61,460
Netherlands 59,270
Republic of Korea 52,397
Italy 36,348
Japan 33,052
Australia 30,955
8890/http
Austria, Utzenaich
2018-01-25 13:53
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 25 Jan 2018 05:53:29 GMT
Content-Type: text/html; charset="UTF-8"
Connection: close
2030/http
Republic of Korea, Seoul
2018-01-25 13:50
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 25 Jan 2018 05:51:43 GMT
Content-Type: text/html; charset="UTF-8"
Connection: close
8002/http
Spain, Toledo
2018-01-25 13:19
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 25 Jan 2018 05:19:03 GMT
Content-Type: text/html; charset="UTF-8"
Connection: close

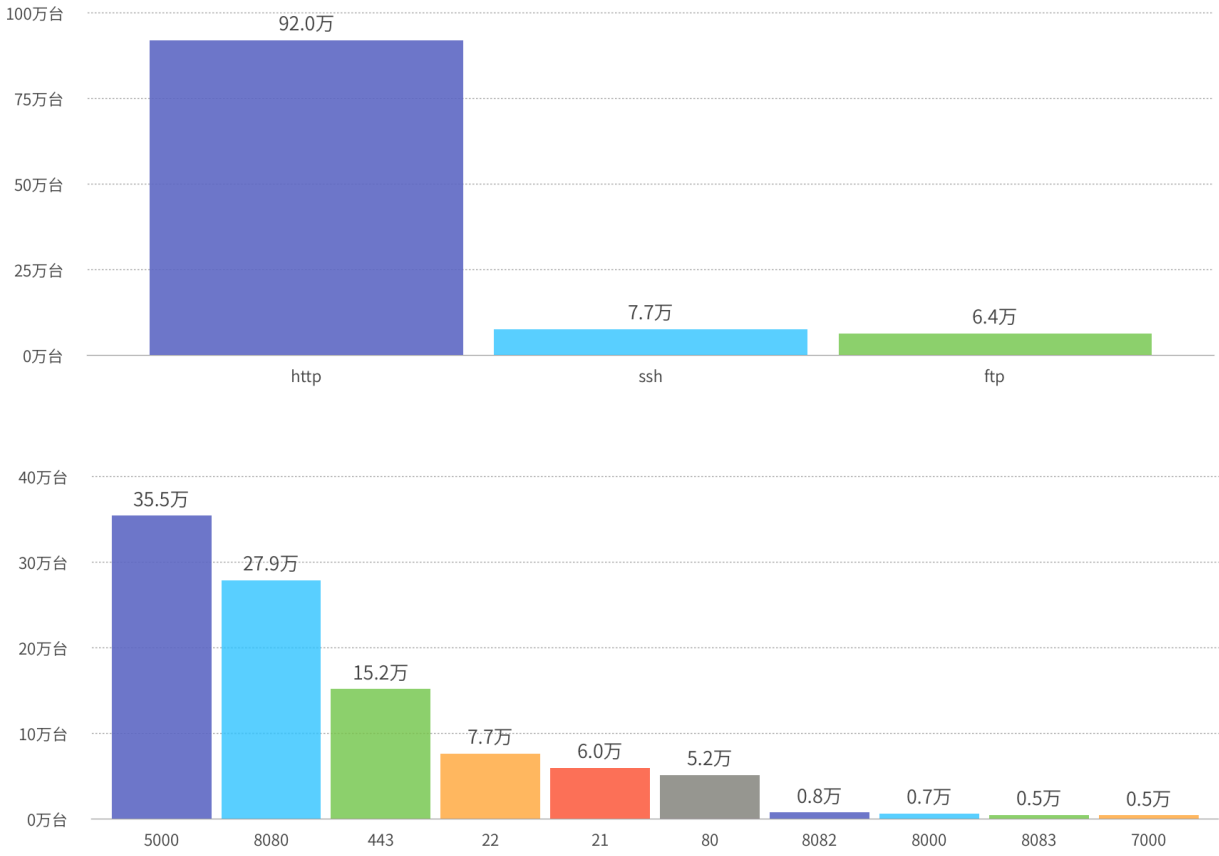
国家分布


14万台
10.5万台
7万台
3.5万台
0万台
13.7万
13.5万
12.6万
8.1万
6.1万
5.9万
5.2万
3.6万
3.3万
3.1万
中国
美国
德国
法国
英国
荷兰
韩国
意大利
日本
澳大利亚

厂商分布



服务和端口分布



3.3 物联网设备存在的问题

3.3.1 开发过程不够规范，存在很多“低级”漏洞

例一：某厂商路由器允许未授权访问特定页面，该页面源代码中包含 Web 管理界面的登陆凭证。

```
(python2.7) ➜ ~ proxychains4 -q curl http://[redacted]:8080/BSW_wsw_summary.htm | grep "CA" -A10

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2785  100  2785    0     0   2785      0  0:00:01 --:--:--  0:00:01  4042
<!-- CA1.63_3.4
<tr>
        <td width="50%"><b>  Admin Username(case sensitive):</b></td>
        <td width="50%">admin</td>
</tr>
<tr>
        <td width="50%"><b>  Admin Password(case sensitive):</b></td>
        <td width="50%">flywheel</td>
</tr>
```

例二：某厂商 NVR 设备，由于后台未做充分过滤，而将用户的输入直接拼接到命令中执行，导致恶意攻击者可执行任意命令。该漏洞影响该厂 NVR 全版本。

```
if ( v11 == 1 )
{
  if ( !v2[5] )
  {
    snprintf(
      &s,
      0x96u,
      "tcpdump -i %s  -p -nn -s 1520 -B 4096 port %d  -vv -C %d -z exittcpdump.sh -w /tmp/packetcapture.pcap 1>/dev/null 2>&1 &",
      v6[4],
      v4[5],
      v10);
    system(&s);
    return 0;
  }
LABEL_31:
  if ( v2[5] == 1 )
  {
    snprintf(
      &s,
      0x96u,
      "tcpdump -i %s  -p -nn -s 1520 -B 4096  -vv -C %d -z exittcpdump.sh -w /tmp/packetcapture.pcap 1>/dev/null 2>&1 &",
      v6[4],
      v10);
    system(&s);
    return 0;
  }
  return 0;
}
if ( v11 == 1 )
  goto LABEL_31;
return 0;
}
```

例三：某厂商多种型号摄像头设备，由于不正确的使用 strncpy() 函数，当攻击者发送的 HTTP 请求中 Content-Length 头字段超出长度限制，会导致缓冲区溢出，进一步可以做到远程代码执行。

```
.text:00018504 ; ---------------------------------------------------------------------------
.text:00018504
.text:00018504 loc_18504                               ; CODE XREF: sub_17F80+1B8↑j
.text:00018504                 LDR     R0, [SP,#0x50+haystack] ; haystack
.text:00018508                 LDR     R1, =aContentLength_0 ; "Content-Length"
.text:0001850C                 BL      strstr
.text:00018510                 MOV     R1, #0xA        ; c
.text:00018514                 MOV     R7, R0
.text:00018518                 BL      strchr
.text:0001851C                 MOV     R1, #0x3A ; ':' ; c
.text:00018520                 MOV     R6, R0
.text:00018524                 MOV     R0, R7          ; s
.text:00018528                 BL      strchr
.text:0001852C                 ADD     R1, R0, #1      ; src
.text:00018530                 RSB     R2, R1, R6
.text:00018534                 ADD     R0, SP, #0x50+dest ; dest
.text:00018538                 BL      strncpy
.text:0001853C                 B       loc_1813C
```

3.3.2 组件重用

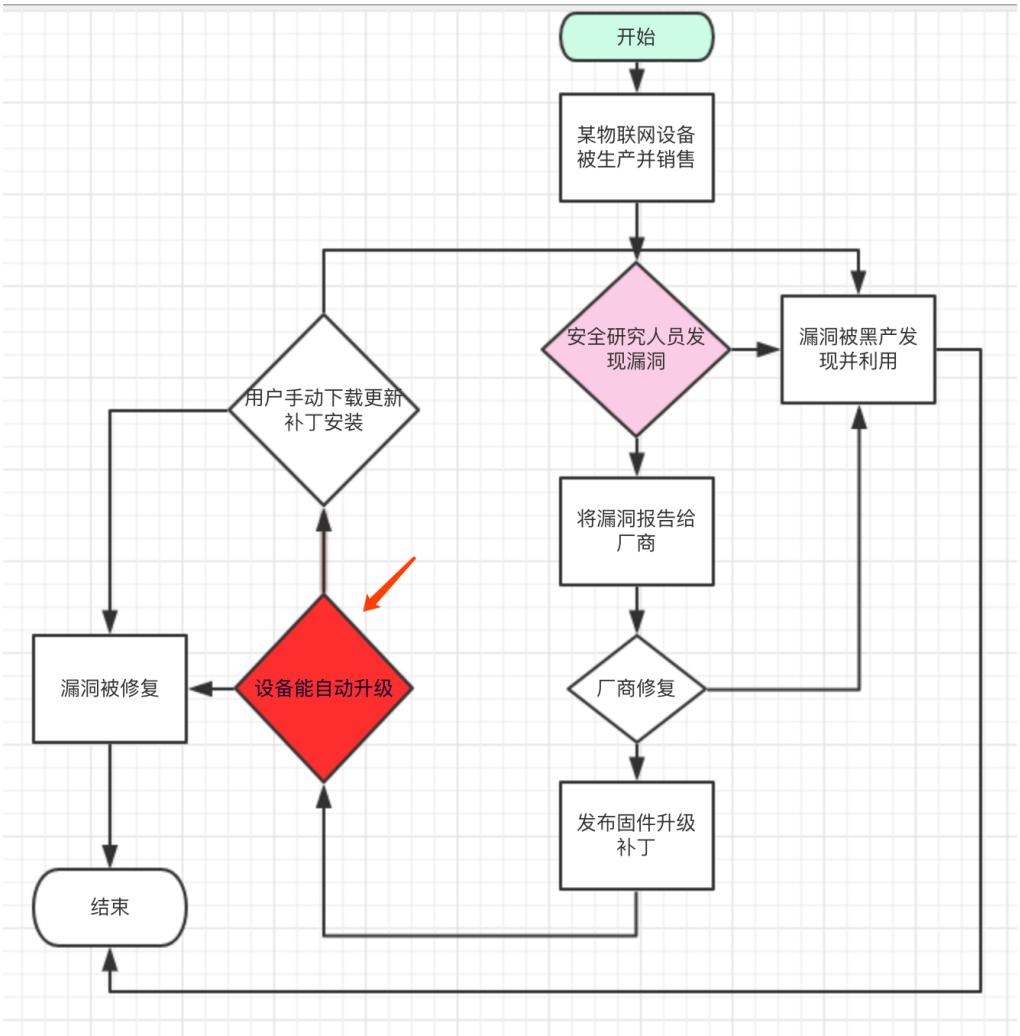
嵌入式设备固件开发过程中可能会使用第三方的开源工具或通用软件，这些通用软件又通常由某一特定厂商研发，这就导致很多设备固件存在同源性，不同品牌的设备可能运行相同或者类似的固件以及包含相同的第三方库，一个漏洞可能同时影响多家厂商。

例如：

GoAhead 作为世界上最受欢迎的嵌入式 Web 服务器被部署在数亿台设备中，是各种嵌入式设备与应用的理想选择。当然，各厂商也会根据不同产品需求对其进行一定程度的二次开发。 2017 年 3 月 7 日，Seebug 漏洞平台收录了一篇基于 GoAhead 系列摄像头的多个漏洞。该漏洞为 Pierre Kim 在博客上发表的一篇文章，披露了存在于 1250 多个摄像头型号的多个通用型漏洞。事后证明，该漏洞是由于厂商二次开发 GoAhead 服务器产生的。利用该漏洞可以成功获取摄像头的最高权限。

3.3.3 无法自动更新

我们可以用流程图大致描绘一个物联网设备的安全链如下。



物联网设备不同于手机、笔记本等，对于普通用户来说，几乎是“无感”的存在，往往在设备出现故障无法工作时才会留意到。对于日常频繁曝出的漏洞，即使是厂商发布了固件更新补丁，由于大多数设备缺少自动升级机制，漏洞往往不能及时修复。

针对这种情况，我们发现了一些有趣的事情：

1. 部分厂商在开发时留下“后门”，可以在设备售出后对设备进行维护或其它目的，但往往这些后门也会被黑产发现并用于其它用途。
2. 网络空间上存在大量的含漏洞的路由器、摄像头等 IoT 设备。一方面，这些设备不断被黑产用来组建僵尸网络，用于 DDoS、挖矿等各种恶意目的。另一方面，我们发现有人用设备本身存在的漏洞对网络空间上的设备进行修复，也有利用漏洞让设备变砖，以引起用户的关注。一定程度上有效降低了这些设备被恶意利用的风险。

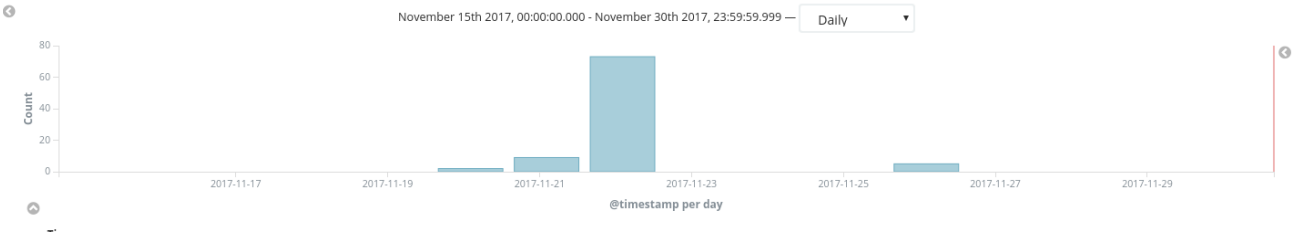
物联网设备是否含有自动升级机制，是整个安全链条中至关重要的一环。

四．僵尸网络与 DDoS 规模

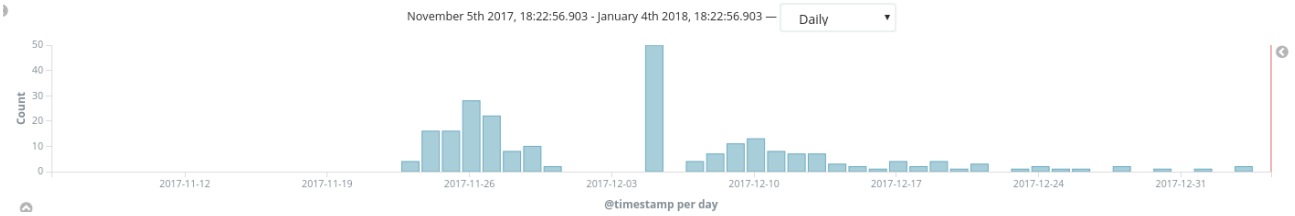
4.1 僵尸网络新特性

4.1.1 81 端口 GoAhead 摄像头已经成为新僵尸网络传播的温床

通过 404 内部蜜罐项目“炼妖壶”中，我们发现在 2017 年 11 月 Satori 僵尸网络传播的开始阶段，相关的样本就已经在 81 端口上传播。



如上图，在 11 月 20 日至 11 月 22 日之间，我们部署在 81 端口的蜜罐被频繁扫中，紧接着 11 月 23 日 Satori 开始正式爆发。



在事后的分析中，由于该样本与 Satori 感染脚本类似，具有相同的 23/2323 端口爆破行为以及相同的 C&C 端，故我们认定该样本为 Satori 的早期样本。

感染 81 端口的摄像头成本低廉，只需要对全网的 IP 发送经过构造的 payload 即可，故通过先感染数万台摄像头的方式可以在短时间内形成庞大的僵尸网络。大大提升了僵尸网络的成形速度。

4.1.2 僵尸网络利用新漏洞的能力不断增强

2017 年，物联网设备 0day 漏洞被曝光到被利用的周期在不断变短，历史上未被曝光的 Nday 有被潜在利用的可能性。GoAhead 摄像头相关漏洞从被曝光到利用用了两周的时间，Vacron NVR 远程利用漏洞仅仅两天的时间就被 IoT_reaper 僵尸网络所利用。一方面，这是 Mirai 源码公开所造成的影响之一(由于 Mirai 源码被公开，攻击者仅仅只需要修改攻击部分就可以很容易组成一个新的僵尸网络)，另一方面，这也说明更及时的安全情报曝光，更有效的安全应急响应的必要性。

4.1.3 僵尸网络漏洞的利用呈现复杂化的趋势

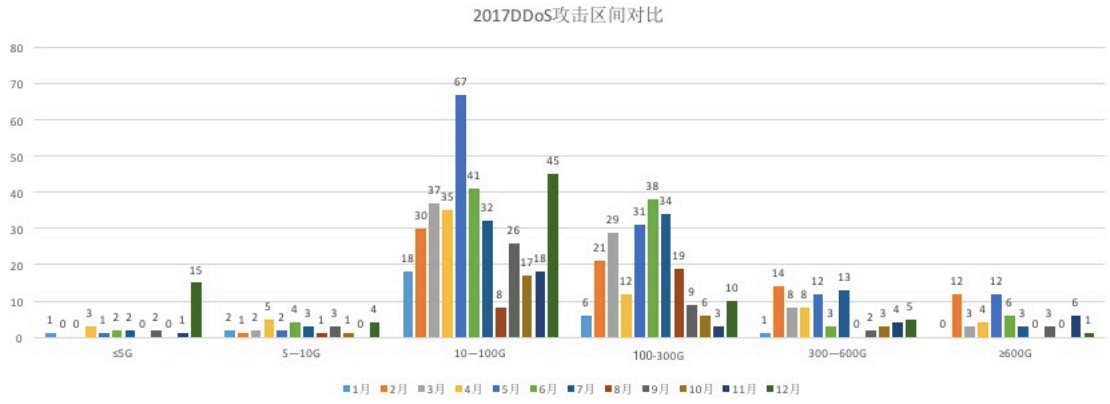
2017 年 9 月，新的僵尸网络 IOT_reaper 在其内部集成了 lua 的执行环境，这也就意味着其支持通过 lua 脚本编写复杂的攻击指令，由于可以自定义相关攻击脚本，所以未来是否可能会发生复杂化的攻击方式？由于部分僵尸网络会使用 DGA 的方式躲避被屏蔽的命运，所以那些未被使用的 DGA 域名是否会被他人注册，从而使相关拥有 lua 执行环境的僵尸网络被他人截胡呢？让我们拭目以待。

4.2 DDoS 规模

4.2.1 2017 年抗 D 宝防御数据

下图是我司的 DDoS 攻击防御产品--抗 D 宝提供的 2017 年度数据

峰值区间	≤5G	5—10G	10—100G	100-300G	300—600G	≥600G
1月	1	2	18	6	1	0
2月	0	1	30	21	14	12
3月	0	2	37	29	8	3
4月	3	5	35	12	8	4
5月	1	2	67	31	12	12
6月	2	4	41	38	3	6
7月	2	3	32	34	13	3
8月	0	1	8	19	0	0
9月	2	3	26	9	2	3
10月	0	1	17	6	3	0
11月	1	0	18	3	4	6
12月	15	4	45	10	5	1



通过图表我们可以看出：

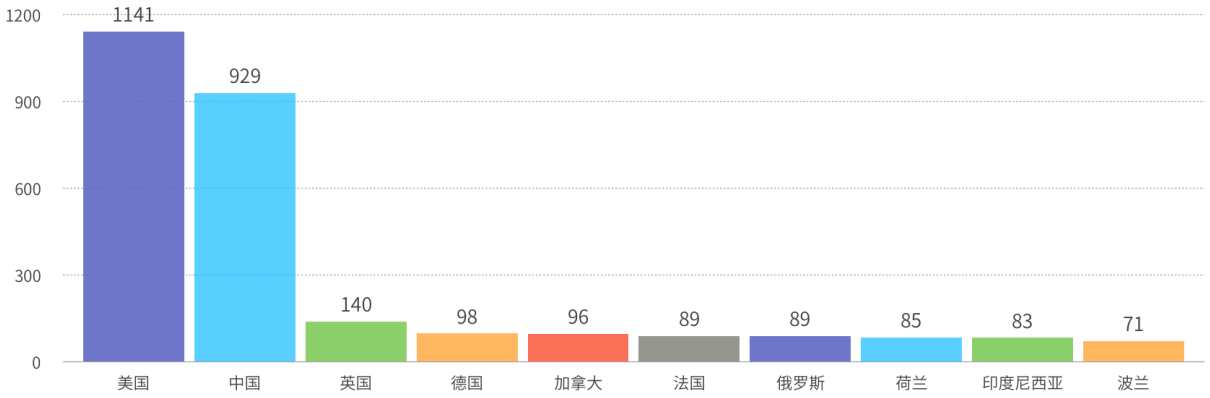
1. 流量在 10G 到 100G 区间的攻击次数是最多的，其次是 100G 到 300G 区间的攻击次数。大于 300G 甚至大于 600G 的超大流量 DDoS 攻击次数也不占少数。结合往年的数据足以说明 DDoS 的攻击能力逐年提升。

2. 攻击流量在 2017 年的月份上也有一定的规律可循：2 月，3 月，5 月，6 月，7 月，12 月的大流量攻击事件比较多。集中在年中和年末两个时间段。

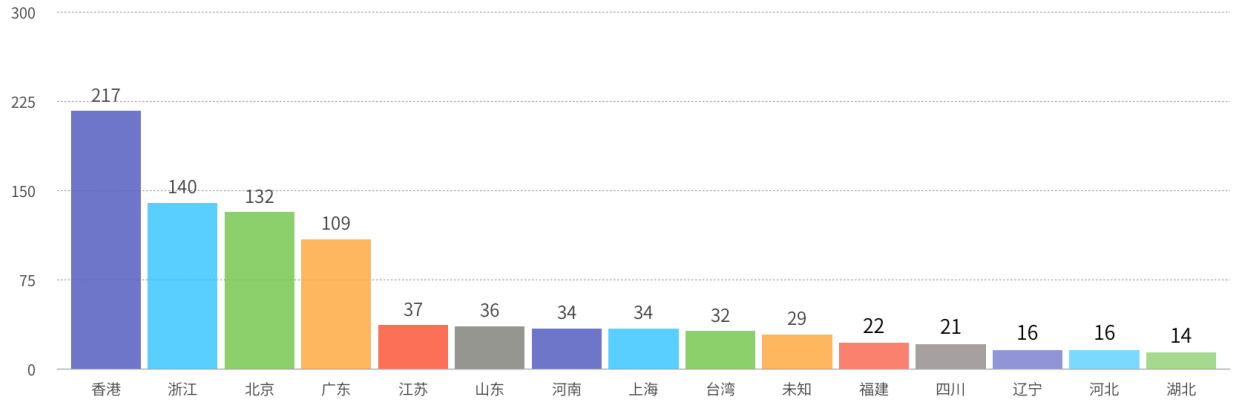
4.2.2 DDoS 攻击目标研究

2017 年 404 实验室内部“炼妖壶”项目捕获到众多 DDoS 被攻击目标，对每个月数据进行去重和筛选后，得到 3705 个重点受攻击目标的服务器信息。

如下图所示，从地理位置上分析，全球重点受攻击 IP 主要集中在中美两国。其他 IP 主要分布在一些欧洲及北美的发达国家。

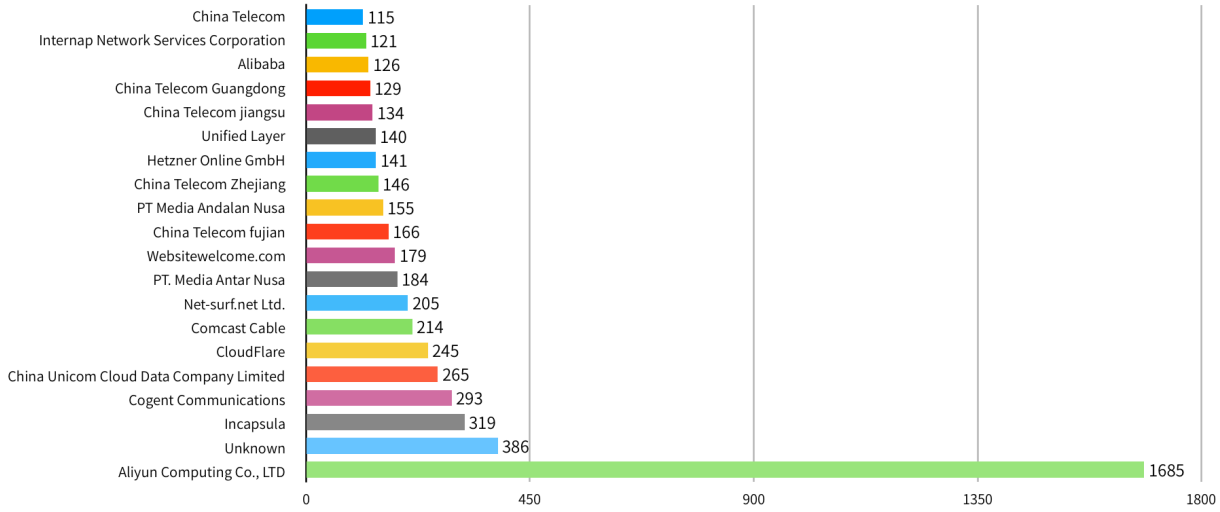


国内的受攻击 IP 分布则主要集中于香港、浙江、北京和广东：

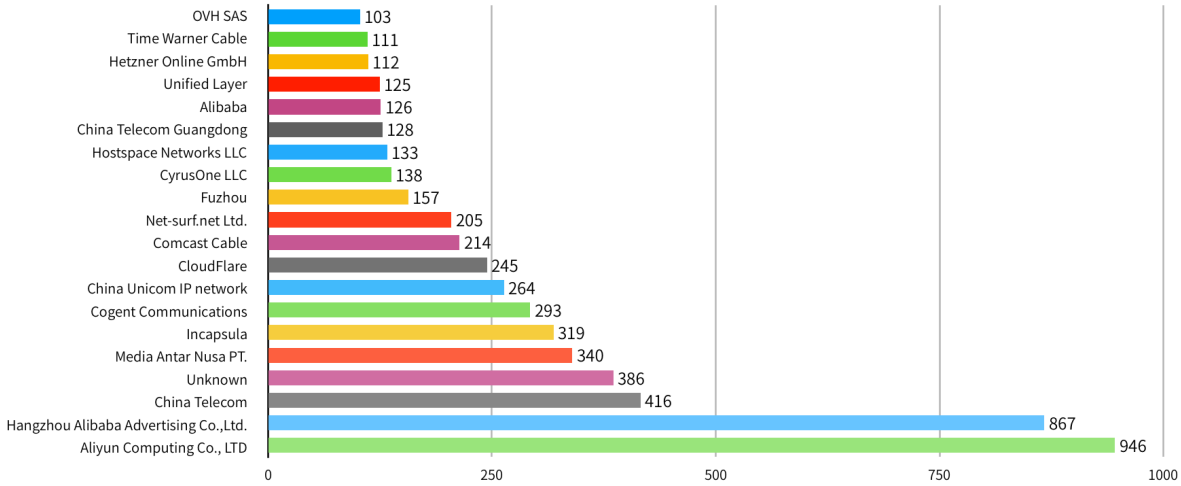


这些受攻击 IP 网络提供商以及所属组织如下：

ISP:

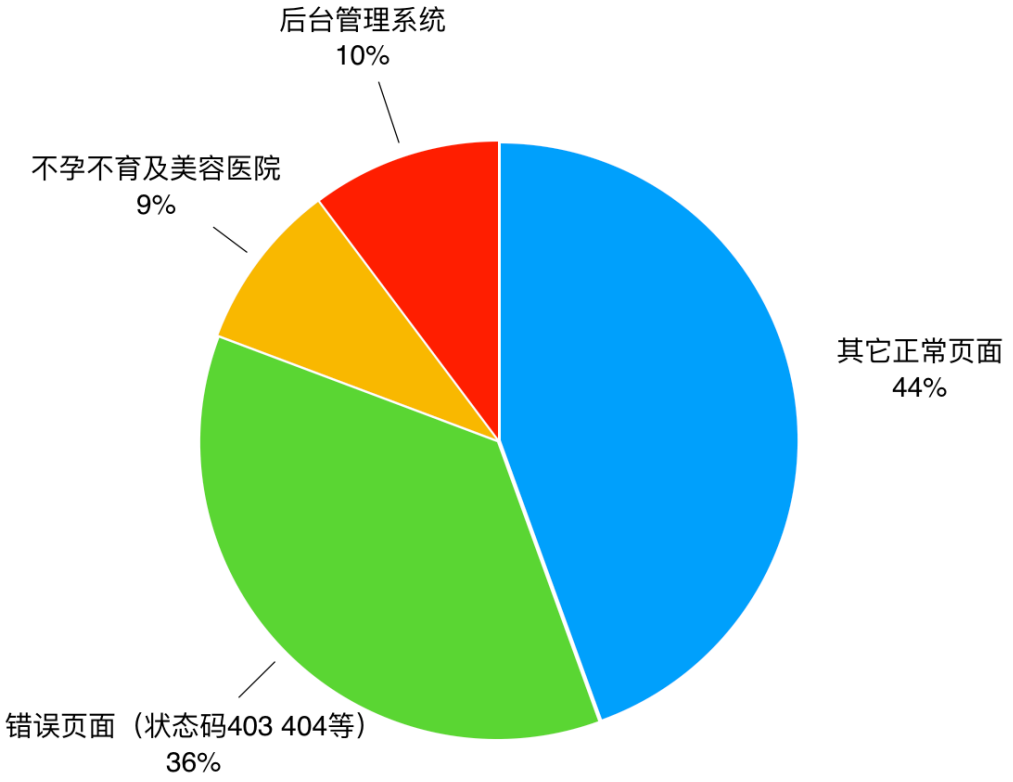


Orginization:



可以看到阿里云一直是被攻击的首要目标，这也从侧面解释了为什么国内受攻击 IP 浙江位居第二。

根据 ZoomEye 网络空间探测引擎的历史数据，我们提取出上述 3705 个 IP 中始终存活的 IP 以及 IP 段的 Web 端口信息，对其进行分析，得出如下结论：



1. 数据中大量页面返回 403、404 等状态码或返回服务器默认页面。该部分网站可能采取了一定的防御措施。

2. 各类后台管理系统和莆田系医院、整容医院在被攻击后依旧会持续存活（注：关于图中所涉及的不孕不育及美容医院，部分出现在网上公开的莆田系医院名单上，部分未出现在名单上，但仍存在莆田系医院的可能）。

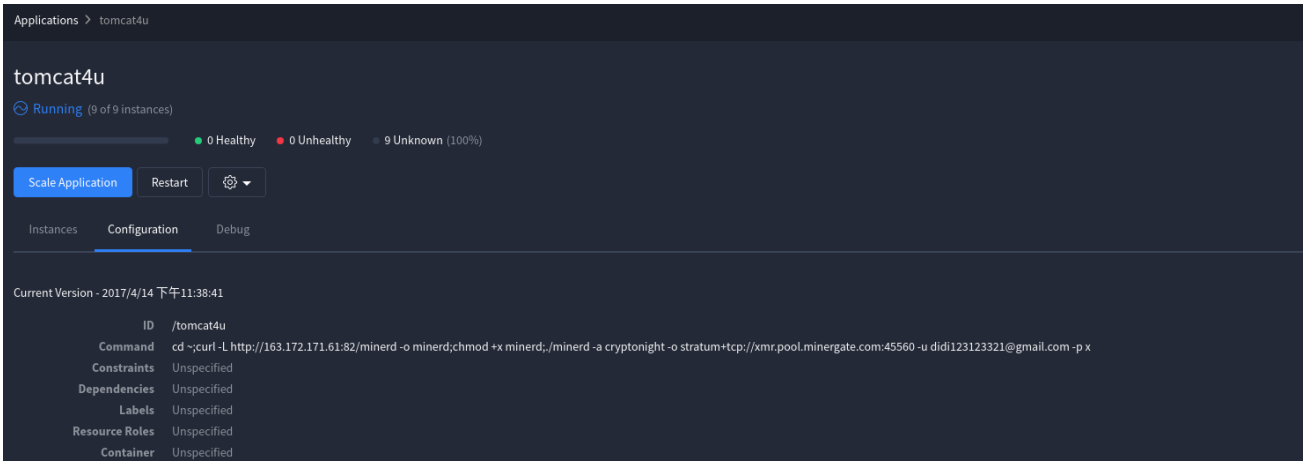
五．挖矿产业

5.1 职业选手和临时工

5.1.1 利用大数据框架挖矿的职业选手

Mesos 是 Apache 下的开源分布式管理框架，Mesos 运行在集群的每一台主机上并提供相关应用(Hadoop、Spark 等)的 API 供使用，而 Marathon 则是运行在 Mesos 之上的应用管理平台，通过 Marathon UI 或者 REST API ，我们可以很容易地创建和管理各节点。可以说，如果 Marathon 出现了安全问题，那么其后的整个集群都将收到影响。

2017 年 4 月，404 实验室在对其进行研究的过程中，无意中发现某个 Marathon UI 界面出现了一个叫做 tomcat4u 的应用。



经后期分析，该程序为开源的挖矿程序。在虚拟货币热潮还未到来之际，容器管理平台已经成为了黑产的目标之一。

5.1.2 利用 DNN 远程命令执行漏洞挖矿的临时工

2017 年 11 月，404 内部蜜罐项目“炼妖壶”捕获到利用 DotNetNuke 任意代码执行漏洞（CVE-2017-9822）进行挖矿活动的攻击流量。该挖矿活动可以大致分为三个步骤：

1. 通过 DotNetnuke 任意代码执行漏洞（CVE-2017-9822）在 Windows 主机上执行 PowerShell。
2. 下载“scv.ps1”脚本用于感染 Windows 主机并运行挖矿程序。
3. 下载 raven.exe、probe.py、zealot.zip 等文件，通过永恒之蓝漏洞继续感染内网主机。

由于脚本中一个小错误， powershell 被写成了 powershll，导致只会在感染当天进行挖矿行为。再结合感染过程中包含了东拼西凑的各式脚本，我们认为攻击者表现得较为业余。

5.1.3 利用 WebLogic 漏洞进行挖矿的职业选手

2017 年 12 月，大量使用 WebLogic 服务器的企业受到黑客攻击，该攻击利用的是未打补丁的 WebLogic 服务器存在的高危漏洞。攻击者攻击目标、目的明确，通过感染未打补丁的主机实现挖取门罗币的目的。

5.1.4 只打 1099 端口的佛系临时工

2017 年 12 月，根据 404 内部蜜罐项目“炼妖壶”，我们观察到一个利用 Java 反序列化漏洞以及部分 PHP CMS 远程命令执行漏洞交叉进行挖矿的黑产团伙。但由于种种原因，该黑产团伙仅在 1099 端口上尝试 Java 反序列化漏洞，写入的 Webshell 部分未被正常利用。这也使其最终因效果不明显而放弃相关尝试。以下漏洞被其利用：

1. Weblogic 远程命令执行漏洞(CVE-2015-4852 和 CVE-2017-10271)
   攻击结果：只对 1099 端口上存在漏洞的主机有影响
2. Jboss 远程命令执行漏洞(CVE-2017-7504 和 CVE-2017-12149)
   攻击结果：只对 1099 端口上存在漏洞的主机有影响
3. Typecho 前台任意代码执行漏洞
   攻击结果：部分成功，会在 web 目录下成功写入名为 cools.php 的一句话木马，但未成功利用该一句话木马。
4. Weathermap 编辑器远程代码执行漏洞
   攻击结果：利用成功

由于最终没有造成大范围的危害，故在此仅提醒大家，涉及的组件：Weblogic，Jboss 等请及时更新，打上最新的补丁。

注：在该报告发布前夕，404 实验室时隔两个多月再次捕获到相关的攻击流量，相关 JAVA 反序列化漏洞的利用端口从 1099 更新至 80。

5.2 观点与总结

在对 2017 年挖矿相关的事件进行梳理的过程中，我们提出以下观点：

1. 用物联网设备组成僵尸网络进行挖矿效果并不明显。随着挖矿行业的兴起，部分由物联网设备组成的僵尸网络也尝试投身挖矿事业。但是由于物联网设备计算能力偏弱，即使拥有庞大的数量，也无法弥补算力上巨大的差距。

2. 挖矿行业的首要目标是性能强的主机，所以高性能家用电脑会是感染的目标之一。这直接催生了浏览器挖矿行业的发展。这也让部分漏洞，例如未授权修改路由器 DNS 等漏洞重新焕发生机。

3. 矿机因其强大的计算能力，可能会成为被攻击的目标之一，矿机被入侵的事件可能会发生。

4. CDN，运营商，广告提供商可能是潜在的被攻击对象。通过 CDN 污染，运营商劫持，广告中加入挖矿代码极有可能对大范围人群造成影响。

由于虚拟货币的价值会极大地影响行业的发展，所以随着虚拟货币热潮的散去，相关攻击活动也会减少。但由于虚拟货币特殊的价值性，在挖矿产业蓬勃发展的这段时间，相关攻击方法仍将会被长久利用，甚至会被黑产其他行业所学习。网络空间的防御将呈现多元化的特征。

六．结语

综上所述，物联网设备的更新机制很关键，2017 年的多数僵尸网络都受到了 Mirai 的相关影响，需要得到控制，挖矿是跟随利益而来，在新的一年热潮可能会回落，但由于虚拟货币的特性，仍然将会长期存在，新出现的各种攻击形式都会被延用。

每年的形式都会有不同的变化。我们也仅仅使根据 2017 年的网络空间现象说出了我们的观点和看法。其中未必正确，欢迎交流讨论与指正。

最后感谢 404 实验室每一位小伙伴的努力，谢谢！

七．参考链接

[1] ZoomEye 网络空间搜索引擎
https://www.zoomeye.org/
[2] Seebug 漏洞平台
https://www.seebug.org/
[3] 《抓住“新代码”的影子 —— 基于 GoAhead 系列网络摄像头多个漏洞分析》
https://paper.seebug.org/252/
[4] 《NSA 泄密事件之 SMB 系列远程命令执行漏洞及 Doublepulsar 后门全球数据分析》
https://paper.seebug.org/299/
[5] 《被忽视的攻击面：Python package 钓鱼》
https://paper.seebug.org/326/

[6] 2017 年比特币价格走势截图来源
https://coinmarketcap.com