知道创宇 暗网雷达

2018 上半年

暗网研究报告

知道创宇404实验室

文档说明

本文的内容是北京知道创宇公司 404 实验室 2018 上半年暗网研究报告。文中的资料、说明等相关内容归北京知道创宇信息技术有限公司 （以下简称“知道创宇”）所有。本文中的任何部分未经知道创宇许可，不得转印、影印或复印。

“暗网雷达”是知道创宇自主研发的针对暗网空间的搜索引擎，正如钟馗之眼 ZoomEye 一样强大，暗网雷达收录了暗网中的设备、网站内容及其使用的服务或组件等信息。通过强大的暗网节点接入能力及独创的暗网爬虫引擎技术，实现全暗网的信息采集及监测，覆盖 Tor， I2P 等常见暗网类型。

北京市朝阳区阜安西路望京 SOHO 中心 T3-A 座-15 层

客服热线（Customer Hotline）：400-060-9587；010-57076191

传真（Fax）：010-57076117

邮编（Post Code）：100102

Site：https://www.knownsec.com

Email：sec@knownsec.com

目 录

1 基本概念

1.1 Deep web / Dark web / Darknet

讲述暗网之前，需要先了解“深网”(Deep web)、“暗网”(Dark web) 和“黑暗网络”(Darknet) 这三个词。虽然媒体可能经常交替使用它们，但实际上它们代表着截然不同而又相关的互联网区段。

“深网”(Deep web) 是指服务器上可通过标准的网络浏览器和连接方法访问的页面和服务，但主流搜索引擎不会收录这些页面和服务。搜索引擎之所以不会收录深网，通常是因为网站或服务的配置错误、拒绝爬虫爬取信息、需要付费查看、需要注册查看或其他内容访问限制。

“暗网”(Dark web) 是深网中相对较小的一部分，与被故意隐藏的 Web 服务和页面有关。仅使用标准浏览器无法直接访问这些服务和页面，必须依靠使用覆盖网络 (Overlay Network)；而这种网络需要特定访问权限、代理配置、专用软件或特殊网络协议。

“黑暗网络”(Darknet) 是在网络层访问受限的框架，例如 Tor 或 I2P。私有 VPN 和网状网络 (Mesh Network) 也属于这个类别。通过这些框架的网络流量会被屏蔽。当进行数据传输时，系统只会显示您连接的黑暗网络以及您传输了多少数据，而不一定会显示您访问的网站或所涉及数据的内容。与之相反的是，直接与明网（Clean Net）或与未加密的表网服务和深网服务交互。在这种情况下，您与所请求资源之间的互联网服务提供商 (ISP) 和网络运营商可以看到您传输的流量内容。

1.2 暗网（Dark Web）的组成

暗网只能通过 Tor （The Onion Routing）和 I2P（Invisible Internet Project）等网络访问。

Tor 又名洋葱网络，是用于匿名通信的软件，该名称源自原始软件项目名称“The Onion Router”的首字母缩写词，Tor 网络由超过七千个中继节点组成，每个中继节点都是由全球志愿者免费提供，经过层层中继节点的中转，从而达到隐藏用户真实地址、避免网络监控及流量分析的目的。

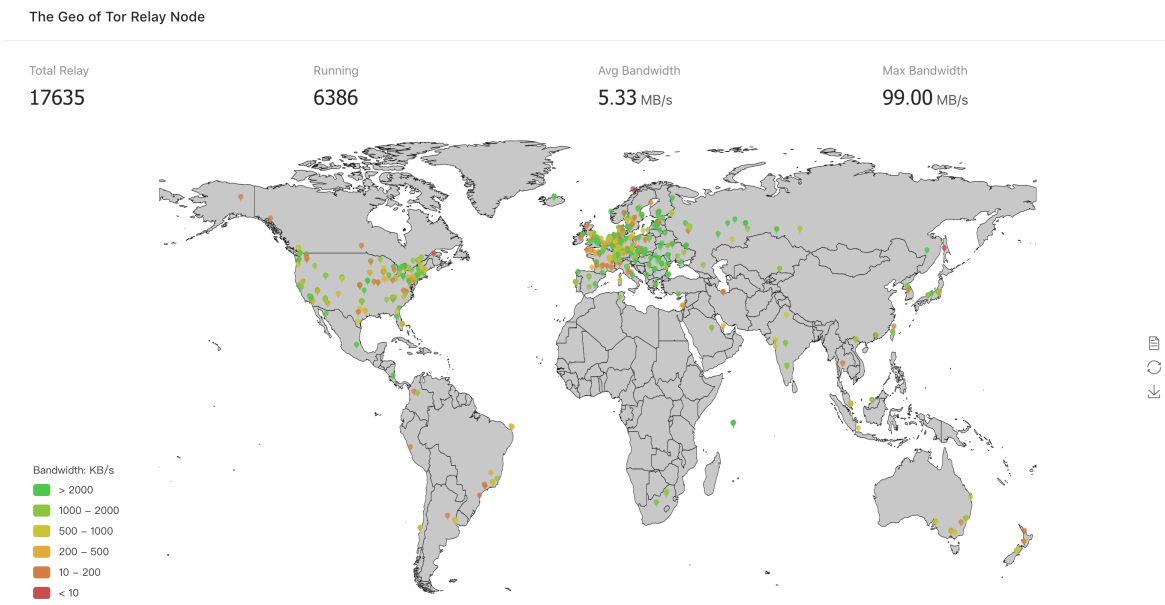
I2P 网络是由 I2P 路由器以洋葱路由方式组成的表层网络，创建于其上的应用程序可以安全匿名的相互通信。它可以同时使用 UDP 及 TCP 协议，支持 UPnP 映射。其应用包括匿名上网、聊天、网站搭建和文件传输。

通过知道创宇“暗网雷达”的实时监测数据表明，Tor 网络大约拥有 12 万个独立域名(onion address)，而 I2P 网络公开地址薄大约只有 8 千个地址，体量相对 Tor 网络要小得多。

2 暗网的现状

2.1 Tor 全球中继节点分布

截至 2018 年 7 月 31 日，我们统计了全球中继节点的分布状况，全球总计有 17635 个中继节点，其中正在运行的有 6386 个，它们的平均带宽为 5.33MB/s，最大带宽为 99MB/s；相比其他区域而言，北美和欧洲的带宽更大；大部分中继节点分布在北美和欧洲，中国香港只有 6 个。



因此可以得出结论，相比表网而言，暗网的规模要小的很多，Tor 网络节点带宽不足以支撑超大的网络流量，网络媒体关于暗网与表网的“冰山比喻”有些夸张了。

2.2 Tor 网络数据统计

根据 Tor 官方项目的统计数据显示，2018 年上半年 Tor 暗网地址（onion addresses (version 2 only)）数量峰值为 121078 个。

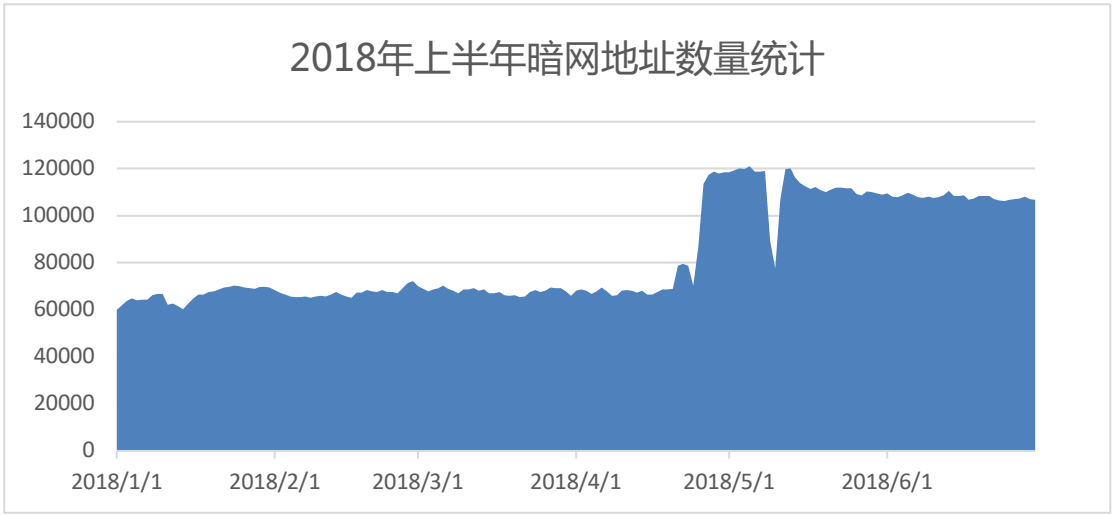


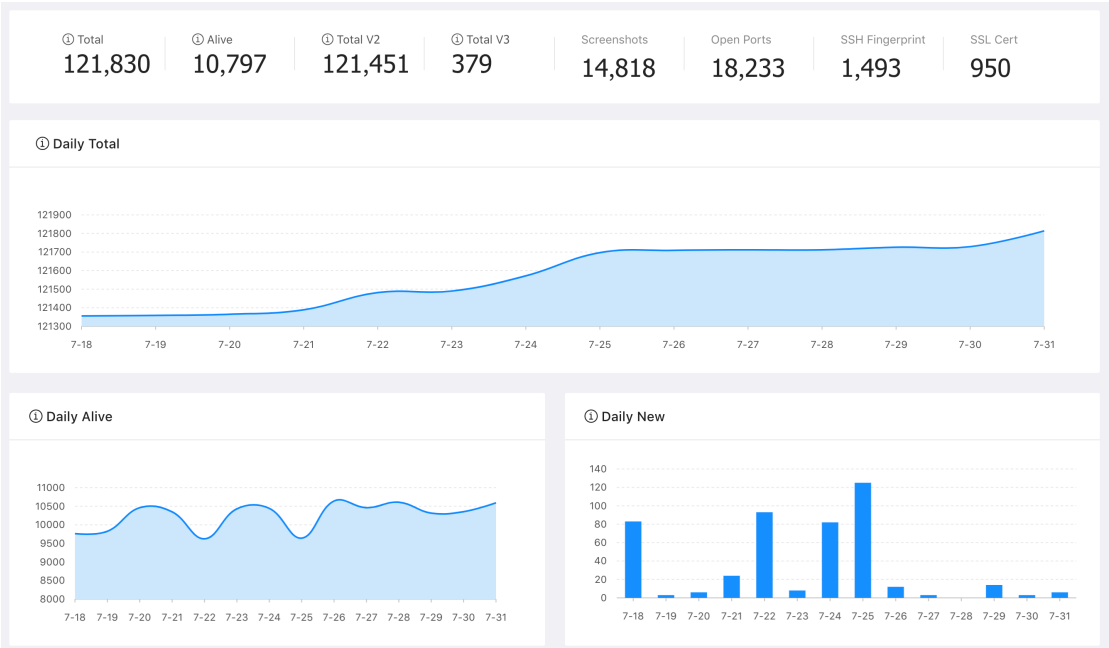
图 2.2 暗网地址数量

Tor 网络来自中国用户数量平均每天 1159 人 ,高峰期为 2018 年 5 月 9 日，达到 3951 人，绝大多数暗网中文用户使用 Meet 类型的流量访问 Tor 暗网。

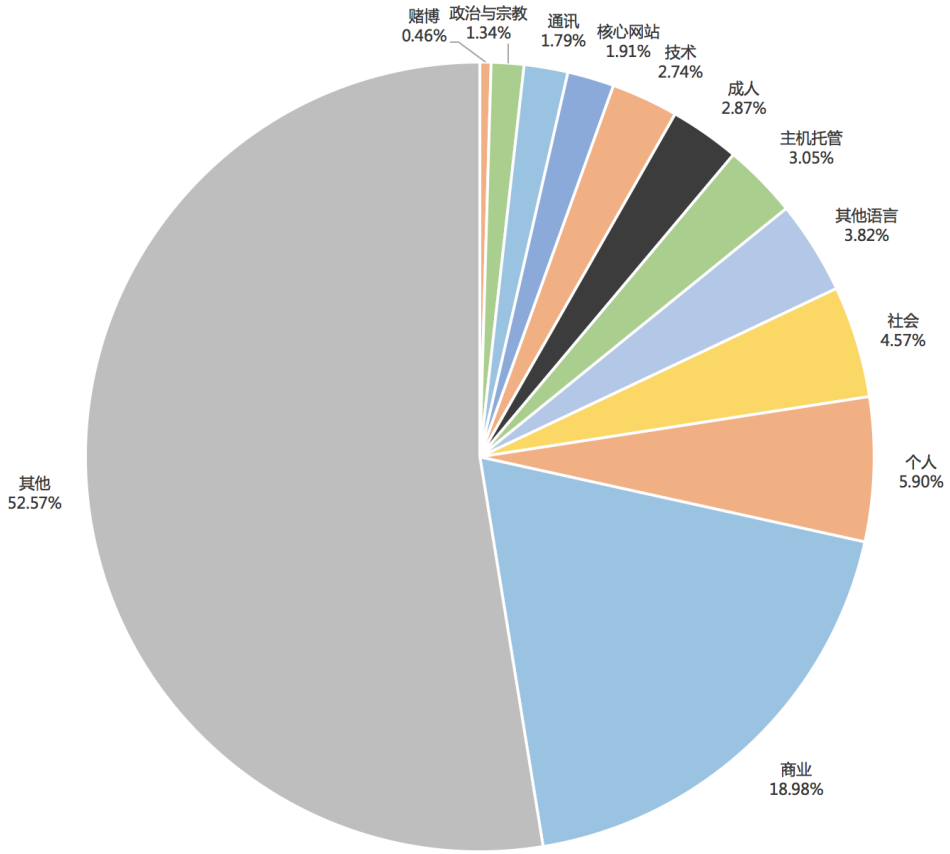
图 2.2. 暗网中国用户数量统计

针对约 12 万左右的暗网域名，我们深入进行了研究，得出结论：

- Onion 域名每日存活量约 1.2 万左右，只占总数的 10%；
- Onion v2 类型的域名有 121451 个，v3 类型的域名只有 379 个；
- 每日平均暗网新增数量为 30 个；



2.3 Tor 暗网的主要类别

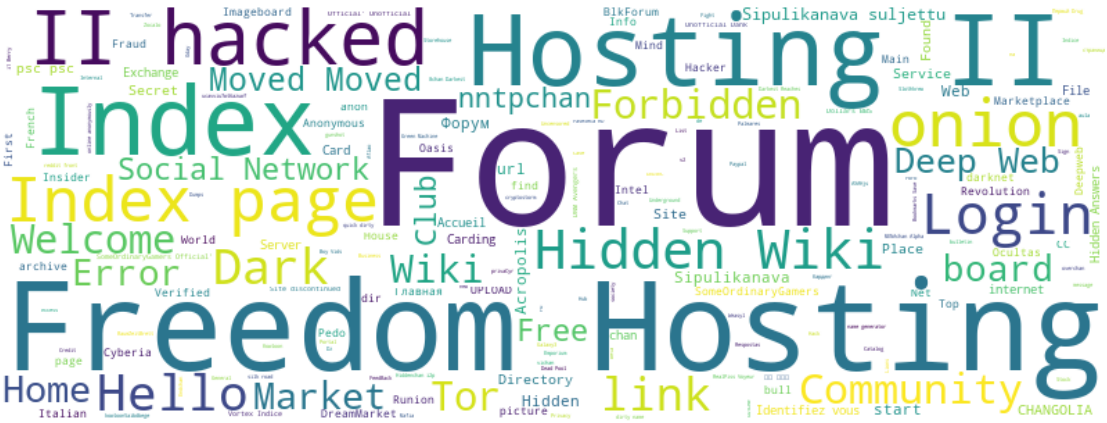


通过知道创宇“暗网雷达”的监测，我们将暗网归为 12 大类，各类占比如上图所示；通过对各类中独立域名的标题进行整合分析，提取网站标题中关键字出现的频率，生成词云：

- 商业类占 18.98%；其中包括交易市场，自营商店，第三方托管平台（网站担保）；交易品种大多是信用卡、枪支、毒品、护照、电子产品、伪钞、欧元票据、亚马逊礼品卡、解密服务、杀手服务、比特币洗钱服务等；大多数网站使用比特币进行交易。

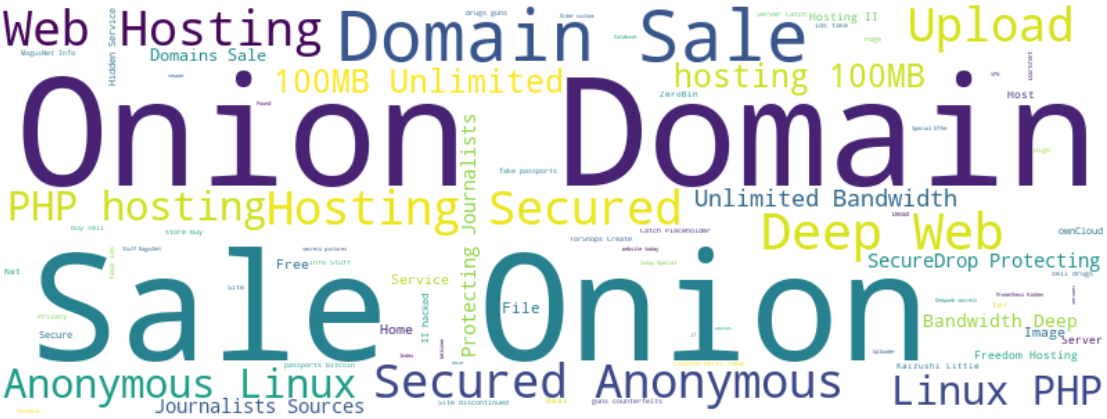
- 个人类占 5.90%；包括个人博客，页面，书籍等。

- 社会类占 4.57%；包括论坛，暗网维基等。



- 其他语言（非英语）占 3.82%；

- 主机托管类占 3.05%；主要为暗网服务托管商的宣传站，介绍其机器性能与架构。

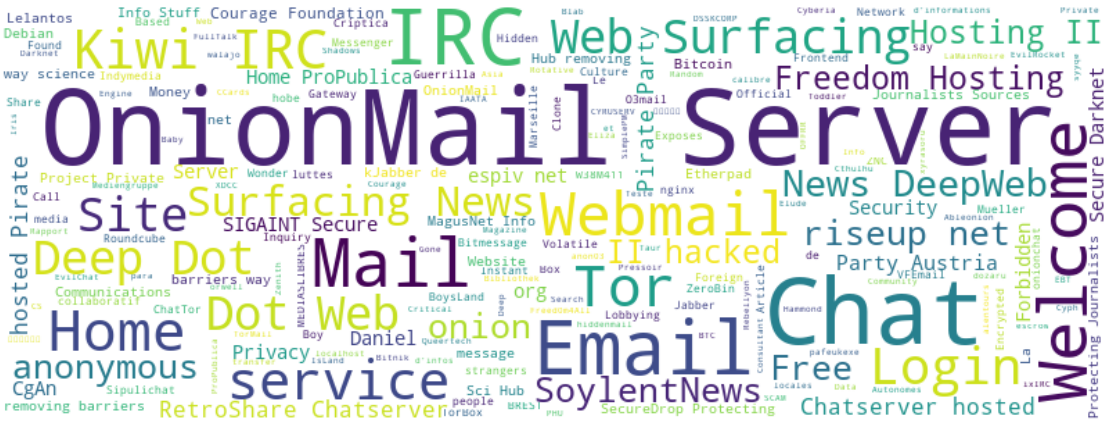


- 成人类占 2.87%；

- 技术类占 2.74%；分享技术 / 出售黑客技术 / 售卖 0day / 漏洞利用

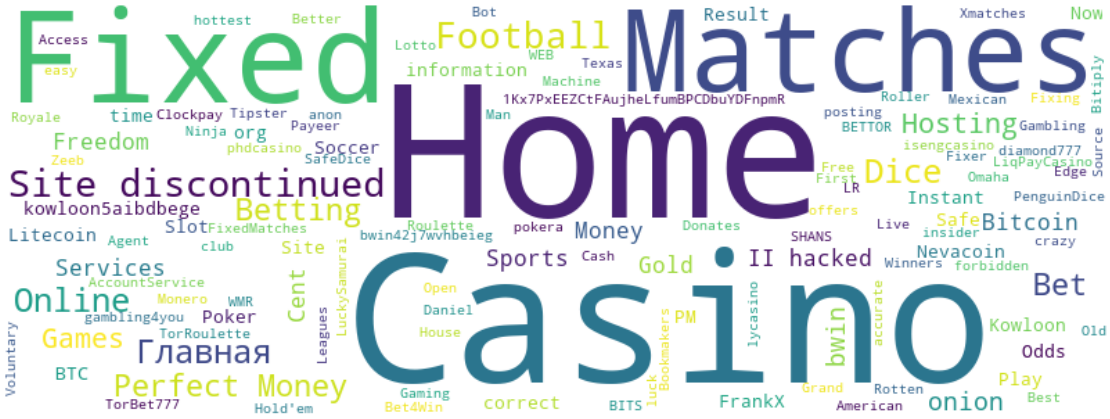
- 核心网站占 1.91%；包括暗网搜索引擎，暗网链接目录等

- 通讯类占 1.79%；包括聊天室，邮件服务，暗网邮箱



- 政治与宗教类占 1.34%；包括暗网的新闻媒体机构，全球维基解密，政党丑闻，激进主义言论，传教等。

- 赌博类占 0.46%；网络赌场等。

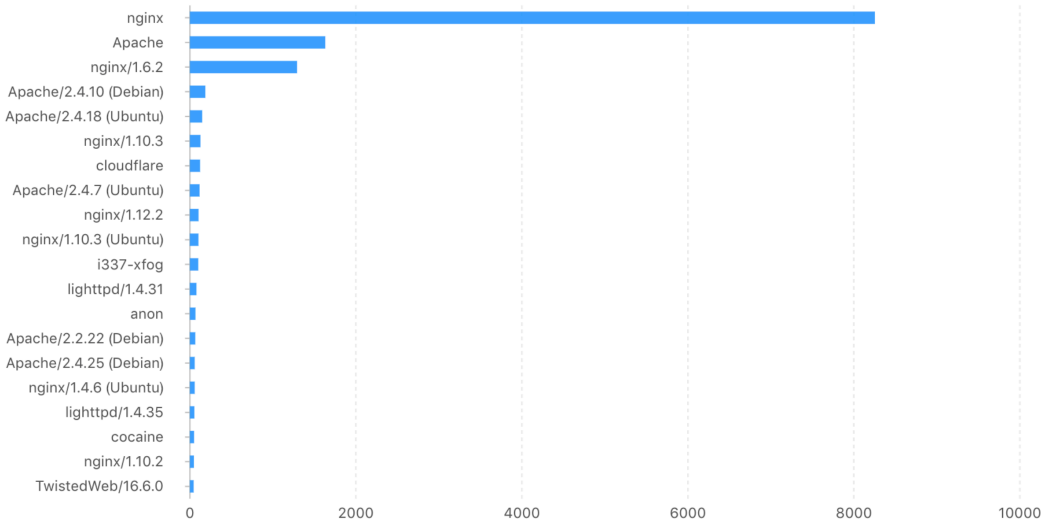


- 其他类(艺术 ,音乐 ,需登陆的 ,无内容 ,被查封的 ,视频等)占 52.57%；

可以看到”Freedom Hosting Ⅱ - hacked”这几个词在各大类中都占据很高的比例。原因是匿名者组织（Anonymous）攻击了当时最大的 Tor 暗网托管服务提供商 Freedom Hosting Ⅱ，因为它向大量共享儿童色情图片的网站提供主机托管服务。直接导致约 20%的 Tor 网站关闭。

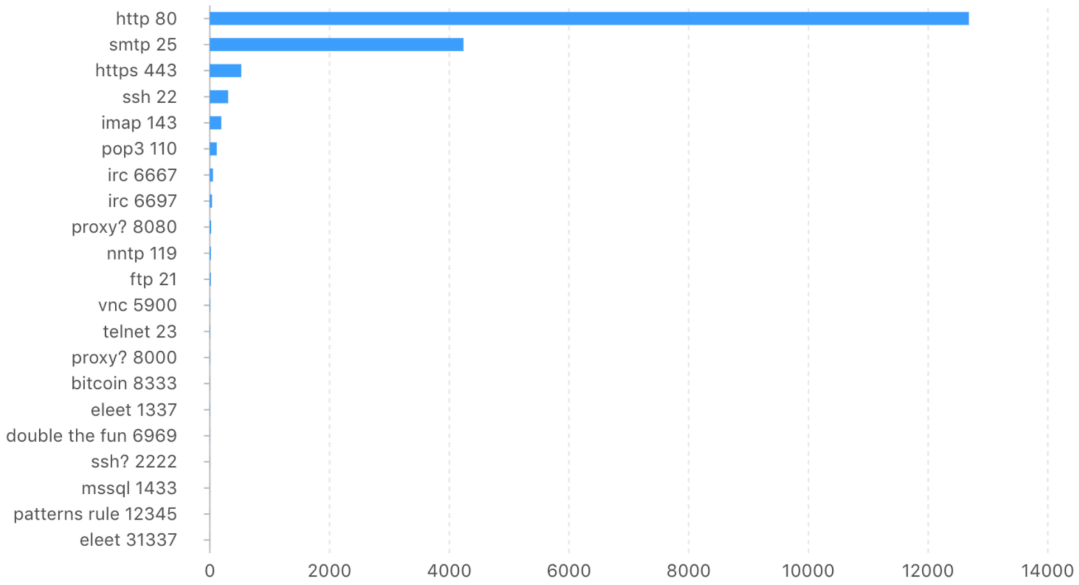
2.4 Tor 暗网 Web 服务分布

我们统计了排名前 20 的 Web 服务器， 绝大多数暗网网站使用 Nginx 和 Apache 作为 Web 服务器，约 1%的暗网使用了 Cloudflare 作为其 DDoS 防护措施。



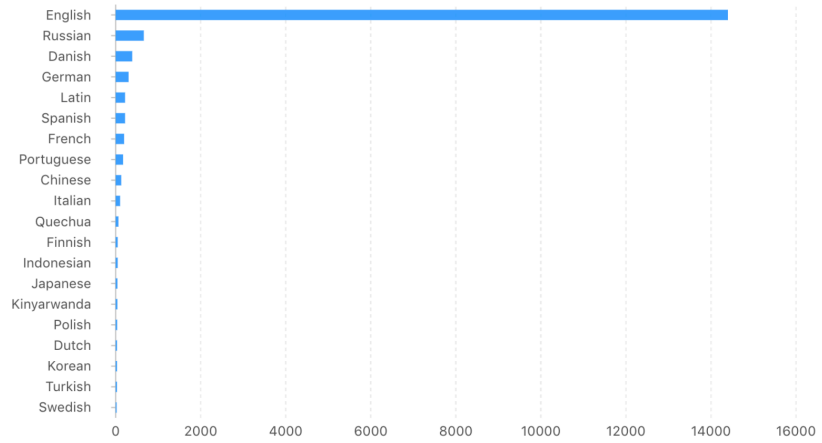
2.5 Tor 暗网开放端口分布

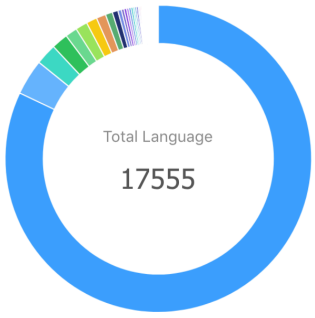
http 80 端口占 69.55%；smtp 25 端口占比 23.24%；https 443 端口占 2.88%；ssh 22 端口占 1.68%。



2.6 Tor 暗网语种分布

通过机器学习分析网站的标题和内容，我们将暗网进行了语种归类，Tor 暗网语种总数有 80 种，英语依旧是暗网中最流行的语言，占比高达 82.02%；接着依次是俄语 3.77%、丹麦语 2.22%、德语 1.73%、拉丁语 1.26%、西班牙语 1.26%、法语 1.13%、葡萄牙语 1.00%、汉语 0.75%、意大利语 0.60%。





3 暗网的威胁

由于暗网的匿名特性，暗网中充斥着大量欺诈，非法的交易，没有限制的信息泄露，甚至是危害国家安全的犯罪等， 这些风险一直在威胁着社会，企业和国家的安全。2018 年上半年，中国互联网就有大量的疑似数据泄露事件的信息在暗网传播，例如：《某视频网站内网权限及千万条用户数据库暗网售卖事件》

2018 年 3 月 8 日，黑客在暗网论坛发布某视频网站 1500 万一手用户数据

2018 年 6 月 9 日，黑客在暗网论坛发布某视频网站 SHLL+内网权限并公布了 300 条用户数据

2018 年 6 月 13 日凌晨，某视频网站官方发布公告称网站遭遇黑客攻击，近千万条用户数据外泄，提醒用户修改密码

另外还有诸如

- 某省 1000 万学籍信息在暗网出售
- 某快递公司 10 亿条快递物流数据暗网出售

等一系列的隐私信息泄露的事件在中国互联网引起广泛传播和关注。

暗网也成为各种威胁情报信息的重要来源之一。

从我们监测的数据来看，暗网还在呈现缓慢增长的态势，随着暗网用户的增多，黑市及加密数字货币的发展，更多的黑客在利益的的驱动下开展各种活动，把之前通过表网（互联网）传播的非法交易更多的转移至暗网，通过各种技术手段躲避追踪。对监管和调查造成了一定的困难。

面对日益增长的暗网威胁， 知道创宇 404 安全研究团队会持续通过技术手段来测绘暗网，提供威胁情报，追踪和对抗来自暗网的威胁，为了更好更安全的互联网。