ZoomEye 网络空间测绘

——委内瑞拉停电事件对其网络关键基础设施和重要信息系统影响

知道创宇 404 实验室

版本	时间	描述
第一版	2019 年 3 月 21 日	完成《ZoomEye 网络空间测绘（委内瑞拉）》第一版

目录

一. 前言

委内瑞拉，是一个位于南美洲北部的热带国家，也是南美洲最重要的产油国。根据《2012 年度世界能源统计数据报告》，委内瑞拉已探明石油储量为 2965 亿桶，占全球 18%，石油出口也成为了该国主要的经济支柱。

由于该国政策、国际形势等多方面因素的影响，近些年该国石油产量逐年下滑，国内局势动荡。2019 年 3 月 7 日晚，委内瑞拉发生了大面积停电事件，全国大范围陷入黑暗。

本文将从网络空间测绘的视角对该国的网络建设情况和停电事件进行一定的分析判断。

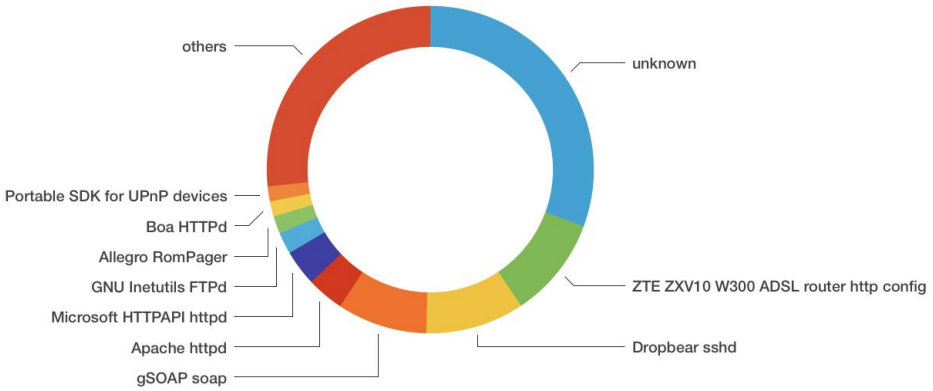
二. 委内瑞拉网络建设情况

截止 2019 年 3 月 15 日，ZoomEye 一共收录了委内瑞拉 1637553 个 IP 的 3067202 条 banner 信息。

2.1 设备类型统计

已识别的设备组件约占该国总设备组件的三分之二，其中 ZTE ZXV10 W300 路由器的 web 管理界面约占总设备组件数的十分之一。

设备类型	收录数量
unknown	939493
ZTE ZXV10 W300 ADSL router http config	306794
Dropbear sshd	299320
gSOAP soap	273037
Apache httpd	112538
Microsoft HTTPAPI httpd	108508
GNU Inetutils FTPd	65765
Allegro RomPager	53103
Boa HTTPd	45948
Portable SDK for UPnP devices	45694
others	817002



值得一提的是，一共识别出 306444 台 ZTE ZXV10 W300 路由器，299250 个 Dropbear sshd 服务，即是 ZTE ZXV10 W300 路由器又存在 Dropbear sshd 服务的 IP 数量高达 244111 个。依次可以做出判断：该路由器可能被广泛用作家庭路由器。这也就意味着，一旦该路由器存在漏洞被攻击，可能会导致委内瑞拉大范围的家庭网络瘫痪。

2.2 开放端口统计

端口分布情况如下：

端口	数量
80	606380
443	526397
22	361730
7547	347805
8080	176303
21	118545
1900	86736
53	86576
5357	64599
others	692131

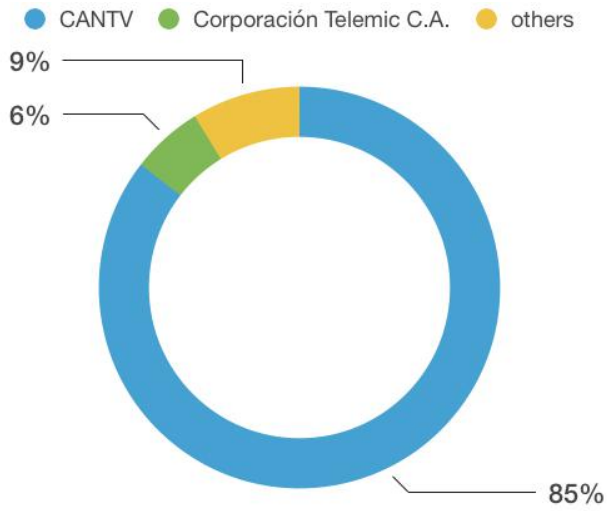
根据 1.1 已知的结论，该国已经识别出的 banner 主要是 ZTE ZXV10 W300 路由器。80、443、22、7547 端口占比较高也和该路由器占比较高有关。

值得注意的是，5357 端口出现在第十位，其中有 62139 个 banner 被识别为 Microsoft-HTTPAPI/2.0。经过判断，这些 IP 都属于 Movilnet 公司。根据其官网介绍， Movilnet 是委内瑞拉移动通信的领先公司,属于委内瑞拉的国营电话和互联网服务提供商 CANTV 的子公司。

2.3 ISP 归属统计

根据 IP 所属 ISP（互联网服务供应商）统计结果如下：

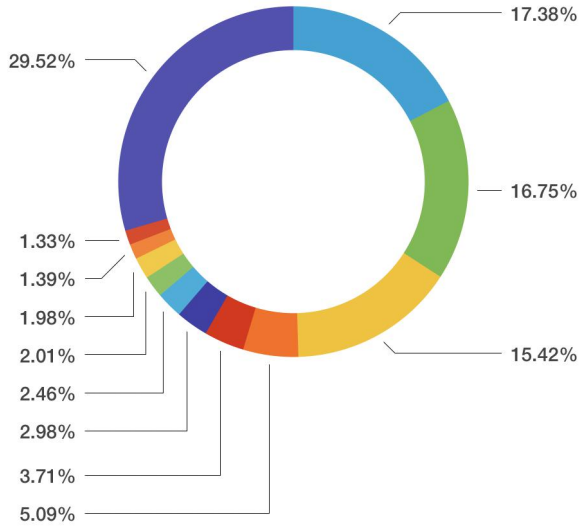
CANTV	2613192
Corporación Telemic C.A.	176781
others	267229



委内瑞拉的国营电话和互联网服务提供商 CANTV 占据了绝对的优势，百分之 85 的 IP 都属于该公司。

注： CANTV 是委内瑞拉的国营电话和互联网服务提供商，是委内瑞拉最大的电信提供商。1991 年私有化后，2007 年重新国有化。细观该 ISP 下的路由器，也大多是 ZTE ZXV10 W300。 还有少量其它品牌的路由器，例如： D-Link、 TP-Link 等。部分路由器可能存在漏洞（例如 D-Link DIR 系列，该系列路由器历史上存在大量安全漏洞。而在该 ISP 下，存在三个 D-Link DIR 系列路由器 ）

ZTE ZXV10 W300 ADSL router http config	303814
Dropbear sshd	292852
gSOAP soap	269543
Microsoft HTTPAPI httpd	88948
GNU Inetutils FTPd	64935
Allegro RomPager	52070
Boa HTTPd	42930
Apache httpd	35065
Portable SDK for UPnP devices	34537
Microsoft Terminal Service	24305
Microsoft IIS httpd	23220
others	516113



ISP 为 CANTV 下识别的组件分布

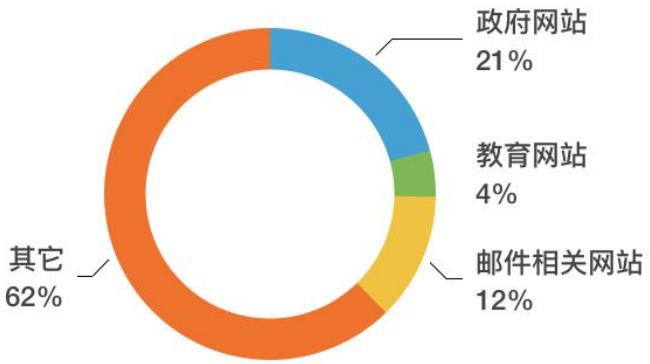
排名第二的 Corporación Telemic C.A. 为委内瑞拉电视广播公司和电信提供商。相比于 CANTV 中存在的组件而言，该 ISP 下并未存在大量民用路由器，取而代之的是存在 11219 台被识别为 Microsoft HTTPAPI httpd 的组件。经过验证，这部分 IP 背后对应着真实的 Windows 系统。

2.4 HTTPS 证书统计

ZoomEye 网络空间搜索引擎一共识别出 252144 个 HTTPS 证书信息，去除路由器的证书、自签名证书 等证书信息后，一共提取出 645 个域名信息，其中域名类型如下：

表格 4

网站类型	数量
政府网站	134
教育网站	29
邮件相关网站	80
其它	402

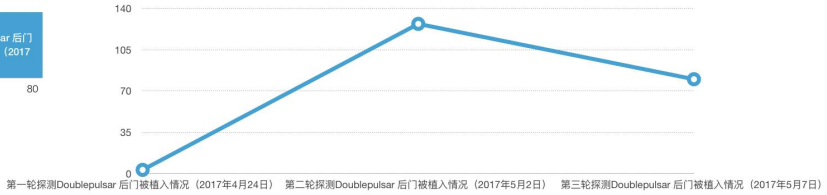


政府和教育类网站占据了总网站数量的四分之一，邮件类网站占比为 12%，其它类型网站仅占比 62%。从 HTTPS 证书的角度来看，该国互联网发展较为落后，政府/教育类网站仍然是该国互联网发展的主要力量。

2.5 安全响应能力

2017 年永恒之蓝漏洞泄露后，能否快速修复相关漏洞也从侧面反映出安全响应能力。

	第一轮探测 Doublepulsar 后门被植入情况（2017年4月24日）	第二轮探测 Doublepulsar 后门被植入情况（2017年5月2日）	第三轮探测 Doublepulsar 后门被植入情况（2017年5月7日）
影响委内瑞拉主机数量	3	127	80



	第一轮漏洞存在情况（2017年4月24日）	第二轮漏洞存在情况（2017年5月2日）	第三轮漏洞存在情况（2017年5月7日）
影响主机数量	179	142	132

可以看到，委内瑞拉在 2017 年 4 月 24 日，漏洞刚爆发时，仅仅只有 3 个主机被植入 Doublepulsar 后门。这也从侧面反映出该国并非网络战争的首要目标。但是在漏洞已经爆发了三个星期后，该国存在漏洞的主机数量仍然有 132 台，仅仅比最开始的 179 台减少了 47 台，这也从侧面反映出该国安全应急响应能力十分欠缺。

2.6 石油销售渠道

在对该国背景的了解中，可以知道：该国主要依赖于石油出口。但在对已有的 banner 进行搜索之后，我们仅仅发现了一家石油生产相关的公司（http://200.*.*.*）和一个出口各类物品（包括石油）的公司（http://201.*.*.*）。

从侧面也反映出该国石油出口有固定的经销渠道，印证了石油开采被国有企业把控的事实。

2.7 工控端口分布情况

根据 ZoomEye 网络空间搜索引擎的数据，委内瑞拉少量工控设备暴露在公网。已知的工控设备或工控协议有（近一年内活跃过的）：

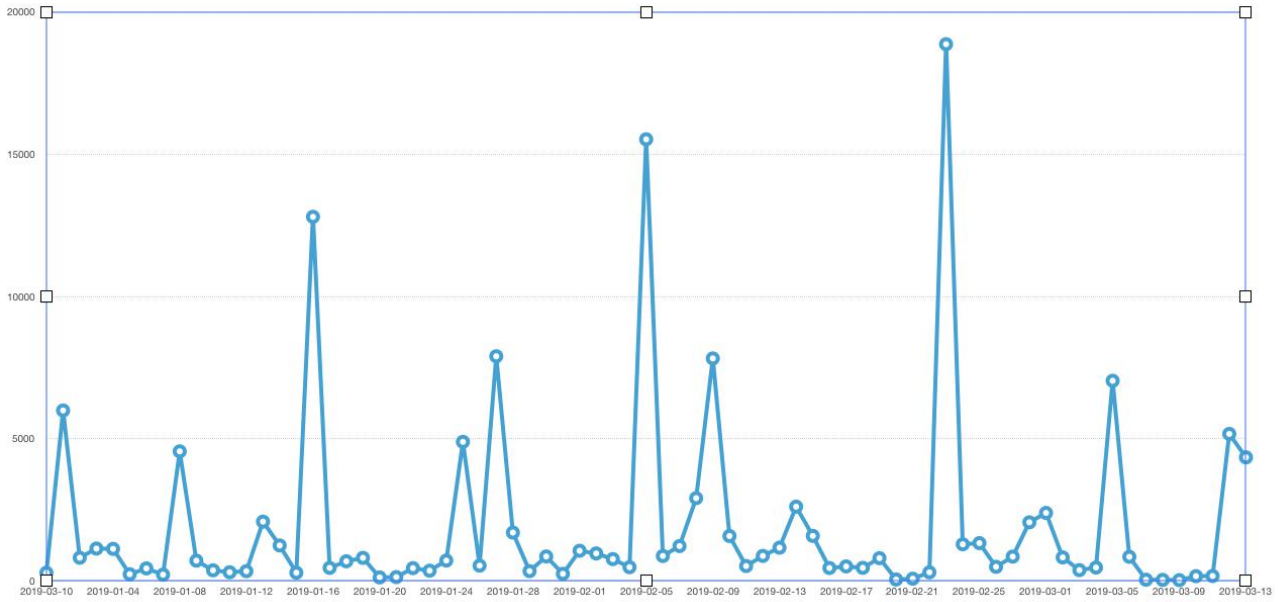
工控设备/协议	数量
Siemens S7 PLC Device	1
Modbus	6
BACnet	1

Crimson V3	1
OMRON FINS	1

三. 停电事件所造成的影响

ZoomEye 网络空间搜索引擎对外探测是具有一定周期性和规律性的。

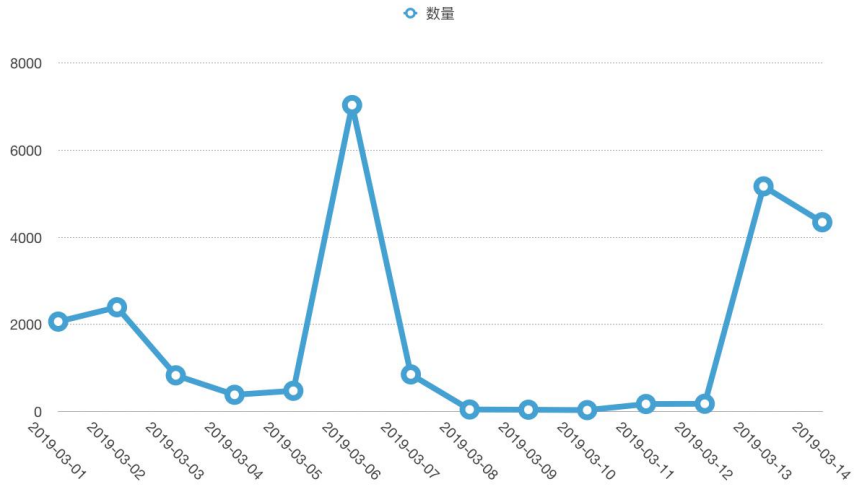
根据前文我们已知委内瑞拉公网上的设备有很大比例的家用路由器。



上图是 ZoomEye 每日录入位于委内瑞拉的 banner 数量，在 3 月初，有明显的数据变化。我们认为这和委内瑞拉的停电事件有较强的关联。

三月具体的数据如下：

时间	数量
2019-03-01	2062
2019-03-02	2392
2019-03-03	828
2019-03-04	381
2019-03-05	473
2019-03-06	7037
2019-03-07	849
2019-03-08	43
2019-03-09	38
2019-03-10	29
2019-03-11	169
2019-03-12	175
2019-03-13	5169
2019-03-14	4345



可以看到，3 月 8 日开始，ZoomEye 录入 banner 数量骤减，在 3 月 11 日录入数量有所回升。3 月 13 日录入数量恢复到正常水平。这和已知的委内瑞拉停电事件信息基本吻合

（3 月 7 日傍晚开始停电）。这也从另一个层面说明从 2019 年 3 月 13 日开始，委内瑞拉的供电已经正常。

统计 3 月 9 日至 3 月 12 日 ZoomEye 网络空间搜索引擎收录的 banner 数据，委内瑞拉全国大范围停电期间，这些地区仍然存在部分能够联网的设备：

地区	停电期间收录数量
Capital（委内瑞拉首都加拉加斯）	250
Carabobo（委内瑞拉卡拉沃沃州）	66
Mérida（委内瑞拉梅里达）	52
未知地区	16
Anzoátegui	14
Miranda	13
Aragua	9
Zulia	8
Táchira	6
Lara	6
Vargas	5
Portuguesa	2
Guárico	2
Falcón	2
Bolívar	1
Barinas	1
Amazonas	1

可以看到，在全国大范围停电期间，委内瑞拉首都加拉加斯、首都附近的卡拉沃沃州（该州有自己的发电厂）以及西边的梅里达仍然能有电力供应。

注： ZoomEye 网络空间搜索引擎使用 GeoIP 提供的 IP 数据库获取 IP 地址对应的地理信息。理论上，IP 地址可以精确到市级。

统计断电期间识别出的组件，主要包括路由器、摄像头、Windows 系统等。在前文中已知的民众常用的路由器类型 ZTE ZXV10 W300 则没有出现。可见在全国大范围停电期间，有限的电力仅仅被用于国家机器的正常运转。

四. 结语

有关此次停电事件，在没有实际有力的证据曝光之前，并不能从网络空间测绘的角度证明停电是由于网络攻击所造成的。

本文从 ZoomEye 网络空间搜索引擎的角度去探讨委内瑞拉的互联网发展情况和停电事件的恢复情况。主要的结论如下：

1. 该国互联网建设较为落后。

2. 该国停电事件在 2019 年 3 月 13 日 （停电后第六天）基本恢复。

3. 如果说停电事件背后存在网络攻击，该国暴露在公网上的众多 ZTE 路由器、Movilnet 公司的相关主机都可能会成为下一步的被攻击目标。

网络安全建设并非一蹴而就，委内瑞拉在这方面要走的路还很长。