lavits
******
2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias

ISSN 2175-9596

NETWORK INTERFERENCE IN LATIN AMERICA: EVALUATING NETWORK MEASUREMENTS TO DETECT INFORMATION CONTROLS AND INTERNET CENSORSHIP

Interferencia de red en América Latina: evaluando mediciones de red para detectar controles de información y censura de Internet

Interferência de rede na América Latina: avaliando medições de rede para detectar controles de informação e censura na Internet

Vasilis Ververis[a]
Olga Khrustaleva[b]
Eliana Quiroz[c]

[a] Humboldt University, Berlin, Germany. Universidade Estadual do Piauí, Teresina, Brazil.
[b] American University.
[c] CIDES, Universidad Mayor de San Andrés, Bolivia. Potsdam University, Potsdam, Germany.

Abstract

This research analyzes open network measurement data and reports collected during a certain period of time from three countries (Colombia, Chile, Venezuela and Brazil) in Latin America by using methodologies to detect possible signs of network interference that may result to information control, Internet censorship or surveillance. The collected data will be cross compared and examined for potential similarities or common characteristics that limit the freedom of expression in the region.

Keywords: Internet censorship; Brazil; Colombia; Venezuela; Chile; Information controls.

Resumen

Esta investigación analiza datos abiertos de medición de red y reportes recolectados durante un periodo de tiempo en tres países (Colombia, Chile Venezuela y Brasil) en América Latina usando metodologías para detectar posibles señales de interferencia de red que podrían resultar en controles de información, censura de Internet o vigilancia. Los datos recolectados son *comparados y examinados en busca de potenciales semejanzas o características comunes que limitan la libertad de expresión en la región.*

Palabras clave: *Surveillance; Law; Smartphones; Privacy; Security.*

Resumo

Essa pesquisa analisa dados abertos da medição de rede e relatórios coletados durante um periodo de tempo de três países na América Latina (Colômbia, Chile, Venezuela e Brasil), usando metodologias para detectar possíveis sinais de interferência na rede que talvez resulte no controle de informação, censura da Internet ou vigilância. Os dados coletados serão comparados e examinados para encontrar semelhanças potenciais ou características comuns que limitem a liberdade de expressão na região.

Palavras-chave: *Censura da Internet; Colômbia; Venezuela; Chile; Brasil; Controle de informações.*

INTRODUCTION

This paper presents our analysis of networks measurements on a number of countries in South America and highlights cases of network interferences and Internet censorship. The corpus of our results are based on OONI (Open Observatory of Network Interference) network measurements data collected from a number of volunteers throughout the years. For the sake of historical analysis we included data from June 2016 to November 2017.

The selected countries have not only a higher density of network measurements through time, but also present a greater network diversity and hence provide data originating from multiple vantage points within countries. The paper has three sections, beginning with a brief literature review on the state of Internet blocking and censorship in Latin America (LATAM). Following the results section describes our conducted research methodology and presents the results of the network measurements data analysis in Colombia, Venezuela, Chile and Brazil. Finally, the last section concludes with a summary of the findings and our final remarks.

PREVIOUS RESEARCH

In 2016, the declaration of the independence of cyberspace celebrated its twentieth anniversary. Back in time, its creators and the first Internet enthusiasts like John Gilmore believed that Internet was created as a global space that can’t be restricted physically and is prone to censorship. “Net interprets censorship as damage and routes around it”, Gilmore famously said (Elmer-Dewitt, 1993). However, the situation has changed dramatically in the past two decades and digital censorship, surveillance and other information control means are now an unfortunate reality that limits freedom of expression around the globe.

The freedom of thought and expression is the matter of article 19 of the Universal Declaration of Human Rights and article 13 of the American Convention on Human Rights. And these documents condemn censorship as a way to limit these fundamental rights. The Organization of American States (OAS) distinguishes in its reports between three types of censorship – prior censorship, direct and indirect censorship. OAS points out that "abuse of governmental or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information" is indirect censorship and classifies Internet blocking and filtering as prior censorship (Lanza, 2017).

The annual report of the special rapporteur for freedom of expression of the inter-American commission on human rights details worrisome cases from across Americas, in which freedom of expression is threatened. Among cases condemned by the rapporteur are intermediary liability law projects, surveillance, blocking and content takedowns as well as violence and intimidation against journalists (Lanza, 2017a). The 2015 report mentions a Brazilian case, where a judge ordered Whatsapp instant messaging (IM) and Voice over IP (VoIP) service to be blocked in the territory of that country, after the company refused to comply with a court request to provide data of a specific user. The higher court then reversed the decision, arguing that blocking affected thousands of people because of a local investigation, but upheld the request to provide the data to Civil Police (Lanza, 2015). Regardless of the past court case and the public uproar, Brazil has again censored Whatsapp services in May 2016 throughout the country, disrupting thereby the voice and text communication of its citizens completely, since Whatsapp IM and VoIP services are used daily by the majority of the people in Brazil (Ververis, V., Xynou, M., & Scott, W., 2016).

Direct Internet censorship such as shutdowns, blocking and filtering are among the better traceable censorship techniques and therefore, much more data is available. Internet censorship can be divided into three core processes: the prescription, when censors decide on what content they are going to block (i.e. gambling sites, pornography); the identification, when censors classify which traffic has to be blocked and the interference itself, where the censor actually "intercede in communication and prevents access to censored materials by blocking access or impairing the connection" (Hall, Aaron, Jones, & Feamster, 2016). Blocking and filtering can be performed at different points of control such as the Internet backbone, Internet Service Providers (ISPs), institutions, personal devices or application services. According to the author there are three types of blocking and filtering: those that imply keyword filtering, domain name blocking or IP address blocking (Hall, J. L., Aaron, M. D., Jones, B., & Feamster, N., 2016).

One of the issues with Internet censorship in LATAM are “preventive restrictions”, where companies might block certain content, even before there was any court decision about the legality of the content in question (Nunziato, 2012, p. 31). Another aspect that Nunziato criticizes in his article is the lack of transparency, since users are rarely well informed about their internet activities being censored. When trying to access blocked websites, they often get an error (such as “404 not found”) and, less often, an explanation that the site was blocked for legal reasons, together with the link of the corresponding law.

Bambauer (2012) argues that all filtering must be recognized as censorship, although in some cases, such as child pornography, censorship is justifiable. Hence, there has to be an ideally transparent discourse, about what exactly can be rightfully blocked. He also points out that in order to achieve transparency, any outsourcing of censorship to entities less accountable than governments should be avoided. Furthermore, according to Bambauer, it is important to recognize that digital censorship is not just practiced by authoritarian governments, but can be present in democratic countries as well.

RESULTS

In this paper we have compiled a list of OONI data analyzed from countries with a significant amount of network measurements from an adequate number of vantage points inside the country, different ISPs and various Autonomous Systems (ASes). The OONI data comprise of network measurements have been collected through OONI tests from 2012 and are licensed under a creative commons attribution sharealike version 4.0 international license (OONI, 2017). The most relevant test through which we derived our findings, is the web connectivity test, that probes for the reachability of a website and enumerates the possible reasons for failing to access it, by recording all the possible errors and identifying the reason of a possible blocking or network interference (OONI, 2016).

The selected data cover Colombia, Venezuela Chile and Brazil in numerous distinct ASes, from June 2016 to November 2017. It's important to note that all network measurements are far from complete as the majority of the data analyzed, have been submitted in specific instances of time, in various frequencies, often not repeated network measurements and not in all possible network vantage points within a country.

Volunteer based network measurements present a significant ratio of false positives and often false negatives on blocked or censored resources. We characterize confirmed cases of censorship based on network measurements that found to contain evidence of block pages or other known evidence of network filtering or blockages. Network interferences may have occurred due to the probed network being inaccessible, which might be due to network outage or the resource not being reachable at the time the measurement took place. Given that, many ISPs or networks do not explicitly provide block pages or relevant information that could be extracted from the networks and used as an evidence of censorship or blocking, we may fail to verify some cases of blocking and network interferences, that took place for a limited amount of time, as well as blocked access to specific content or resources.

Diverse vantage points and the scarcity of longitudinal network measurements in the region is a limitation of our research, as compared to other countries, in many of the countries in question relatively few OONI data have been collected (submitted network measurements). The list of URLs used to conduct the network measurements in OONI data were derived from the Citizen lab test lists (Citizen Lab, 2017) a community driven collection of relevant URLs, conducted by individual contributors for local country specific websites that are different for each probed country, as well as a global URL list that is constant to all countries. The data analyzed consist of network measurements reports from OONI web connectivity and HTTP requests tests. Both tests have the ability to detect which of the tested websites are being blocked, if they are reachable and the reason for them not being reachable. Specific software versions and implementations of ooniprobe, the main software used to perform network measurements, have a functionality that allows users to test, specify and provide test lists on URLs outside Citizen lab's test list.

Following, we are presenting our findings from the analysis of OONI network measurements collected from Colombia, Venezuela Chile and Brazil.

COLOMBIA

In our analysis we have detected a number of ISPs that were blocking websites, by various methods and using block pages to inform users about the filtering regulations. However, most of the blocked pages detected, are misclassifying the websites, by providing an invalid blocking landing page, that does not actually justify the reason of blocking these websites as the cited law related to child pornography, appearing to be something like a "default justification" for blocking. (Secretaría Jurídica Distrital de la Alcaldía Mayor, 2001). Tigo Une ISP (EPM Telecomunicaciones S.A. E.S.P.) is among the ISPs that blocks websites unrelated to the law cited on their block page. We have found two URLs blocked on this ISP, "http://filestube.com", a meta-search engine established in 2007 specialized in searching files from various file sharing and uploading services (Filestube, 2007), and "http://www.youngerbabes.com", a pornographic website. Similarly, we detected that all ISPs in our research redirect users that try to access these websites to a block landing page (Tigo Une, 2017a), (OONI data, 2016c), (OONI data, 2017c) unrelated to the law cited on their landing block page (Etb ISP, 2017a), (Claro ISP, 2017) by using an HTTP proxy or a Deep Packet Inspection (DPI) filtering infrastructure to block these resources.

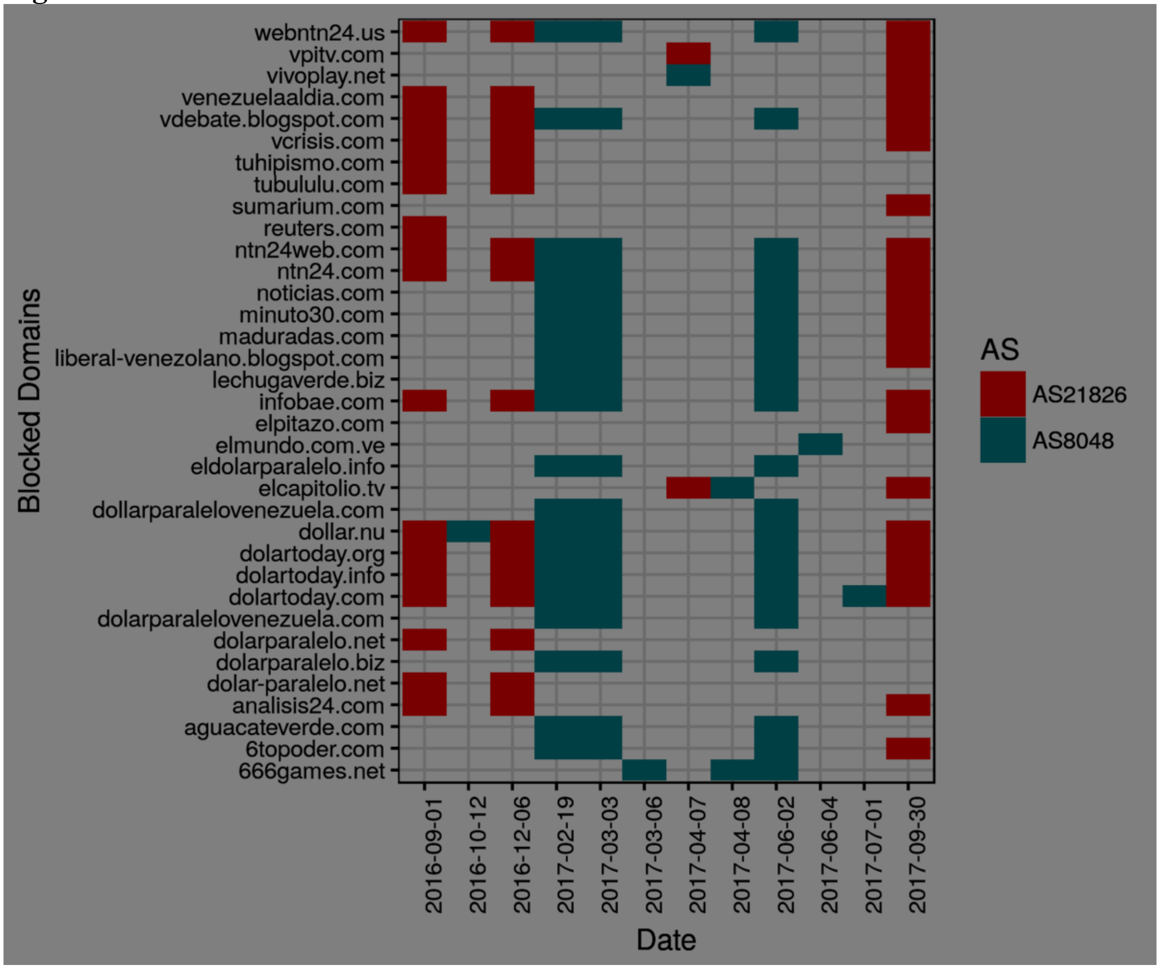
The country recently started regulating the online gambling websites, issuing public blocklists and forcing the ISPs to block the entries of the published blocklist. Internet regulations and blocking of resources via blocklists often end up blocking much more resources than the ones intended, due to human and technical failures, transparency, nonexistent post removal policies and ease of blocking. Building upon a censorship infrastructure, Colombia's gambling blocking regulations are related to the gambling of other European countries (Ververis, 2015, 2017). To the authors' knowledge, Colombia is the first country in LATAM to publish a blocklist of URLs (Aldana, 2017). The list, in its current form, has 325 entries of which a considerable number of entries are malformed, containing syntactical errors, incorrect URLs as inputs (such as the entry number 318: "Bookiesport*"*), email addresses (entry number 284: "c-crisari@hotmail.com") or malformed text (entry number 303: "/(S(eb1sttfzoriyp4qf5r0xs2lf))/Default.aspx?ReturnUrl=%2f}"). Another crucial detail about the blocklist is that it includes a Facebook profile page (entry number 280: https://m.facebook.com/profile.php?id=100013654141621&refid=46&tsid&fref=search), thereby implying that the ISPs in Colombia should block the Facebook website.

We have identified three different gambling landing block pages from Tigo Une ISP (Tigo Une ISP, 2017b), Telefónica ISP (Telefonica ISP, 2017) and Etb ISP (Etb ISP, 2017b), (OONI data, 2017d, 2017e, 2017f).Given the organization of the blocklist and the misclassification of websites on the numerous block pages, we may safely assume that the ISPs in Colombia might block and censor further resources and websites besides the ones we identified.

VENEZUELA

Venezuela has been known for increasingly censoring media and individuals who oppose the politics of Nicolas Maduro's government. Activists reported being spied on and the analysis of OONI data showed blocking and filtering of various news media via Domain Name System (DNS) hijacking. A number of possibly politically motivated blocking incidents have been detected. NT24 and Infobae are two international news website that have been blocked within the country. The reason of NT24 blockage is not clear. In the case of Infobae, according to the Venezuelan government, the censorship was related to the published images of the murdered chavista representative Robert Serra. In 2016, an NGO Espacio Publico brought a report before the Inter-American Commission on Human Rights, where it accused CANTV (Compañía Anónima Nacional Teléfonos de Venezuela) of repeatedly refusing to release public information. The information in question was about websites blocked in certain regions of the country during protests of 2014, which in many places turned violent. In the report Espacio Publico claimed that CANTV's refusal to release information violates Article 13 of the American Convention on Human Rights (Association Civíl Espacio Publico, 2016). Figure 1 illustrates the domain names found blocked in Venezuela, along with the date of the network measurements, derived from OONI data during 2016 to 2017. The total number of domain names found censored within 2 ISPs, CANTV Servicios (AS8048) and Corporación Telemic C.A. (AS21826) is 35.

Figure 1



OONI: Venezuela’s censored websites during 2016-2017 based. 2017.

CHILE

During May 2017 a number of users in Chile were unable to access Riseup's website and services, such as private wikis and the group collaboration platform (“we.riseup.net”), chat and online communication, real-time collaboration with documents (“pad.riseup.net”), file upload (“share.riseup.net”), as well as access to their email accounts and all other services hosted at Riseup's main domain such as the VPN services (“black.riseup.net”, “vpn.riseup.net”), Riseup account management (“accounts.riseup.net”) and user support (“support.riseup.net”). Additionally, external domains that use Riseup's DNS name servers were also found to be inaccessible by the same ISP in Chile. Among these were domains hosting websites and services such as “0xacab.org” a source code hosting repository and development collaboration platform. Riseup is a collective, dedicated to providing private and secure email and hosting services for individuals and organizations committed to political and social justice. Many human rights activists from around the world rely on Riseup services in order to perform their daily communications and operations.

OONI data reveal that the websites ”riseup.net” (OONI data, 2017a) and “mail.riseup.net” (OONI data, 2017b) were not accessible and failed to resolve the IP address of the domain (“riseup.net”) by users of the ISP VTR BANDA ANCHA (AS22047).

The first known measurement report evident of the inaccessibility of the riseup domain (websites “riseup.net” and “mail.riseup.net”) was performed on 17th of May 2017. Since then and up to August 2017, the domain name `riseup.net` and its subdomains as well as external domains using Riseup's DNS nameservers are inaccessible from this ISP. The measurements analyzed from the OONI data show that after the 17th of May 2017 the DNS queries towards the domain “riseup.net” did not return any responses back.

COMMUNICATION WITH THE VTR ISP

The VTR ISP agreed on setting up a meeting and provide further explanations on the case of Riseup. Throughout the meeting ISP confirmed having been blocking the Riseup domain since the 12th of May 2017 after a ransomware attack incident by the Wannacry ransomware cryptoworm (*Millar, Sheila, Marshall, Tracy, Cardon, & Nathan, 2017)*. VTR is part of the Liberty Global public limited company, an international TV and broadband company with operations in more than 30 countries cross Europe, LATAM and the Caribbean (Liberty Global, 2016). The day of the ransomware incident all ISPs that were part of the Liberty Global company have received threat alerts related to the incident and according to VTR one of riseup's IPs was referenced to the attack, without specifying the exact involvement. Consequently and based on the Liberty's Global threat alert, the technical department of VTR decided to block the IP addresses, mentioned in the announcement, and any related domain names. More specifically, on 12th of May 2017 the VTR ISP has blocked a list of IP addresses that were mentioned in the threat alert in order to block all network traffic that was related to the ransomware attack.

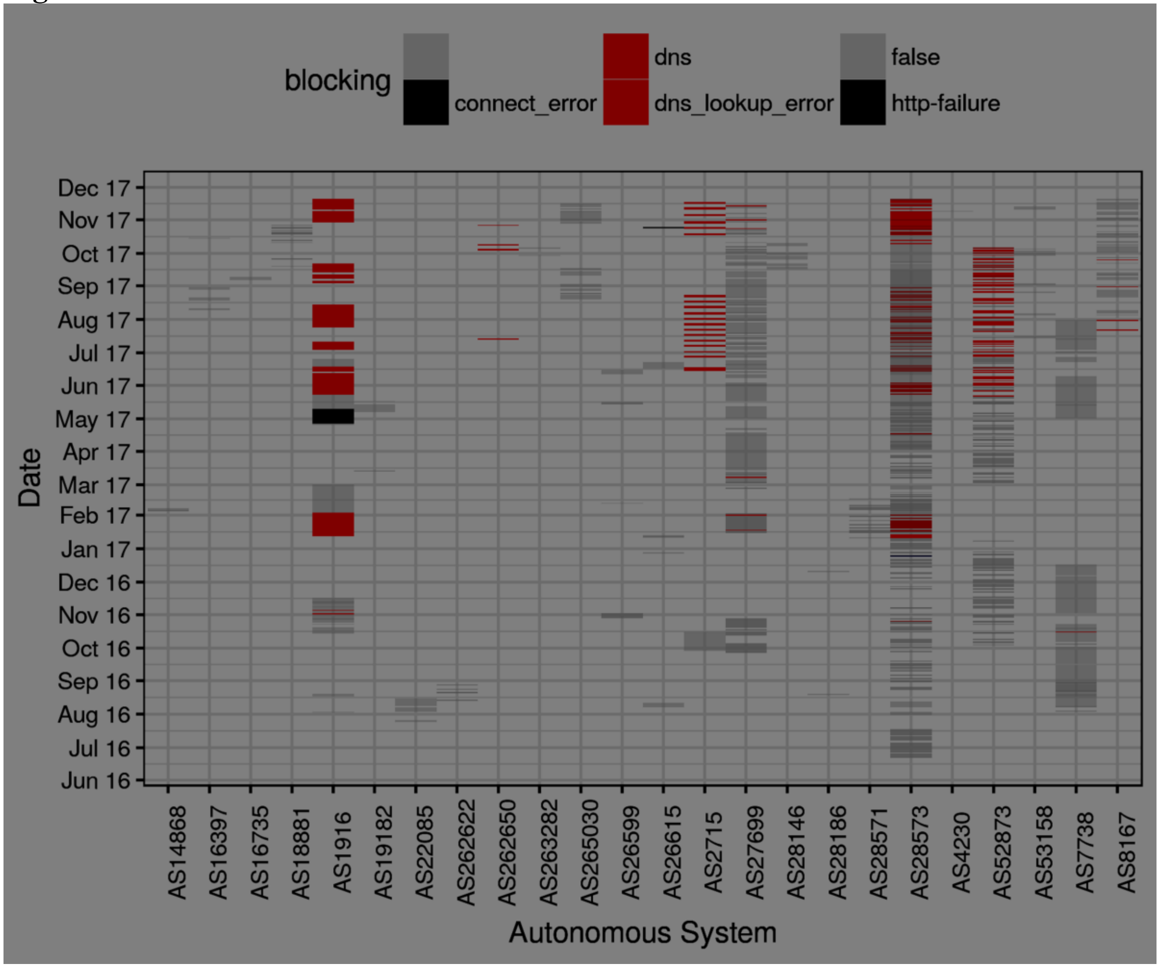
One of the IP addresses mentioned on the threat alert (IP address “199.254.238.52”) was a directory authority (Tor project, 2017) of the Tor network. Among other operations, directory authorities help Tor clients to learn the list of available Tor relays that comprise the Tor network, thus blocking directory authorities may disrupt network connectivity and degrade network performance to Tor users and the Tor network. VTR ISP has also blocked the domain name of Riseup (“riseup.net”) that was extracted from the DNS pointer record (PTR) responses of the IP address in question (“longclaw.riseup.net”). According to the VTR ISP, they had used internal procedures to block IPs and domains upon alerts, and theoretically also for lifting such blockings when the alert threats expire. Only that in this case, they neglect to raise the blocking upon the threat alert expiration, without stating any further clarifications or details on their internal procedures related to the blocking of resources.

BRAZIL

Another finding inferred from the OONI data is the case of a website (hosted in Brazil) that is not accessible from many ISPs, and numerous networks in Brazil and worldwide. The website in question is “pernambuco.com” a regional news portal part of the “Pernambuco Daily” newspaper publishing group, being nothing less, but the oldest circulating newspaper in LATAM (Gaspar L., 2009). Volunteers in Brazil have been submitting a vast amount of network measurements from a distinct number of network vantage points, which will be used as a supporting evidence to determine how often and in which networks the website was not accessible. The most likely explanation of the failure to access the website are potential network misconfigurations or other network failures that render its domain name unresolvable (the answers to the DNS queries performed are not returning any responses) in many networks.

OONI network measurements conducted for the website “pernambuco.com” have been submitted from 24 ASes that cover most broadband and cellular ISPs in Brazil. Figure 2 illustrates the networks measurements, analyzed from the HTTP requests and web connectivity OONI tests, during June 2016 to November 2107. The gray colored lines (“false” test key) illustrate that the website was accessible at the time of measurement on the given ASes. The dark blue color (“connect_error” and “http-failure” test keys) indicate connectivity failures due to transient network errors or server failures and the red colored lines (“dns”, “dns_lookup_error” test keys) that indicate DNS failures and consequently the inaccessibility of the website. A DNS lookup error is a failure to resolve the IP address of a given domain name, while the rest of the DNS errors found indicate inconsistent responses to DNS queries performed to the given domain (“pernambuco.com”). The website in question was found to be inaccessible in 8 ASes (out of 24 ASes) and appears to be randomly accessible within different date ranges and on different ASes. On the rest of the 16 ASes the website is invariably accessible and indicates no DNS failures or other network failures.

Figure 2



OONI: Brazil’s Accessibility of Pernambuco.com website during June 2016 - November 2017. 2017.

A further analysis of the DNS errors brings further evidence that the failure may occur due to a network configuration issue and specifically the DNS server configuration. The underlying DNS provider uses a DNS server configuration that is considered a bad practice and can lead to configuration conflicts that may render “pernambuco.com” inaccessible. The findings of the analysis enumerate further affected domains hosted on the same DNS provider and provide evidence regarding the worldwide inaccessibility of the “pernambuco.com” website on a specific date (15th of November 2017) from 284 networks outside Brazil (Evdokimov & Ververis, 2017).

However the analysis of the DNS errors does not justify the accessibility and unobstructedly access to the website within two thirds of the networks tested, 14 out of 24 ASes. Furthermore, it is unclear how all network measurements indicate that the website was occasionally reachable at times with no recorded DNS or other failures in all ASes. Our attempts to further investigate on the case of network misconfiguration by trying to contact the administrators of “pernambuco.com”, notifying them about the failure to reach the website and requesting further information that could potentially help to identify the root cause of the problem, unfortunately, remained unresponded

CONCLUSIONS

Our analysis of OONI data in the LATAM region revealed that Colombia is blocking a number of websites and redirects users to block pages that not only provide irrelevant information about the blocking, but also do not justify the real reason for the blocking. Columbia is the first country in LATAM to regulate online gambling services and publishes a gambling blocklist with poor guidelines and frightful errors, denoting that the blocklist has not been reviewed properly. Some of the entries in the Colombian blocklist include an email address and a Facebook profile page and --according to the law imposes to ISPs to block these resources. The network measurements, analyzed regarding Venezuela, provide evidence that the country has been censoring news and media websites recently due to political reasons. We have identified 35 domain names that host news, media, blogs, exchange currency information, and video games websites.

Following in Chile the VTR ISP has blocked the private wikis, group collaboration platforms, chat and online communication, real-time collaboration with documents, file upload as well as access to email services and all other services and websites hosted by Riseup an autonomous technical collective that offers its services to activists and groups or people working on liberatory social change all over the world. The ISP claimed (on a private meeting) that the blocking of Riseup was part of a security response to a malware incident. Upon the expiration of the malware incident the VTR ISP neglected to raise the blocking, resulting to the blocking of Riseup services and websites for more than 3 months.

During this period all users of this ISP were unable to access any of Riseup's services and websites. Subsequently the ISP has blocked at least one Tor directory authority (the one provided by Riseup) and that could cause network connectivity disruptions and performance degradations of the Tor network.

Concluding with the case of Brazil, where we have identified that supposed network interferences and inaccessibility to web content might as well be caused by potential network failures due to misconfigurations or bad practices. The result of this potential misconfiguration is nothing less but an old regional news portal “pernambuco.com” being inaccessible from one third of the measured networks (8 out of 24 ASes) as well as more than 280 networks worldwide for a duration of at least a year (since November 2016). And even more crucially, the website as of the time of this publication is still inaccessible within many networks.

Regarding further research, the following remarks can be made. Network measurements are not an exhaustive method for studying censorship, since information controls are not limited to technical means. Many cases documented by researchers, activists and the special rapporteur for freedom of expression demonstrate that there are a huge number of means to censor speech, online and offline, including surveillance, intimidation and legal action as well as propaganda using fake news and botnets in social media platforms. Accordingly, a combination of network measurements with other quantitative and qualitative methods such as social media analysis, surveys and interviews can result in a profound and multi-dimensional study of information controls.

Regarding the moment of data collection, it has been proved, that information controls often toughen and expand before and during major political events, such as elections, referendums and demonstrations. Therefore, conducting network measurements in a timely manner a priori to these events can prove a useful way for analyzing data on Internet censorship.

REFERENCES

Aldana, A. (2017). *Paginas web ilegales*. Retrieved from https://web.archive.org/web/20171120020053/http://static.iris.net.co/semana/upload/documents/paginas-web-ilegales.pdf.

Bambauer, D. E. (2012). Censorship V3.1. *Arizona Legal Studies*, 12-28.

Citizen Lab (2017). URL testing lists intended for discovering website censorship. Retrieved from https://github.com/citizenlab/test-lists.

Claro ISP (2017). *Landing block page*. Retrieved from https://web.archive.org/web/20171122003844/http://furl.telmexla.net.co/dignidad.php?CAT.

Elmer-Dewitt, P. (1993, December 06). First Nation in Cyberspace. *Time Magazine* [online version]. Retrieved from http://content.time.com/time/magazine/article/0,9171,979768,00.html.

Etb ISP (2017b). *Gambling landing blocking page*. Retrieved from https://web.archive.org/web/20171122013124/http://guardian.etb.net.co/public/stop.htmopt?CAT.

Filestube (2007). *FilesTube search engine*. Retrieved from https://web.archive.org/web/20070618025003/http://www.filestube.com:80/about.html.

Gaspar, L. (2009). Pesquisa escolar online. Fundação Joaquim Nabuco. *Diario de Pernambuco.* Retrieved from http://web.archive.org/web/20160819132856/http://basilio.fundaj.gov.br/pesquisaescolar/index.php?option=com_content&view=article&id=237&Itemid=183.

Hall, J. L., Aaron, M. D., Jones, B., & Feamster, N. (2016). A Survey of Worldwide Censorship Techniques [online document]. Retrieved from https://datatracker.ietf.org/meeting/96/materials/slides-96-saag-4.

Lanza, E. (2015). *Annual Report of the Inter-American Commission on Human Rights 2015*. Retrieved from http://www.oas.org/en/iachr/expression/docs/reports/annual/AnnualReport2015RELE.pdf.

Lanza, E. (2017a). Informe Anual de la Comisión Interamericana de Derechos Humanos 2016. *OAS*. Retrieved http://www.oas.org/en/iachr/expression/docs/reports/annual/AnnualReport2016RELE.pdf.

Lanza, E. (2017b). Standards for a Free, Open and Inclusive Internet. *Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights*.

ETB ISP (2017). *Landing block page*. Retrieved from https://web.archive.org/web/20171122001123/http://www.etb.com.co/pages/ley69de2001.aspx

Evdokimov L., & Ververis V. (2017). *Identifying cases of DNS misconfiguration: Not quite censorship*. [online document]. Retrieved from https://web.archive.org/web/20171126230644/https://ooni.torproject.org/post/not-quite-network-censorship.

Liberty Global (2016). *LiLac Group Chile*. Retrieved from https://www.libertyglobal.com/oo-chile.html.

Millar, S., Marshall, A., Tracy, P., Cardon, P., & Nathan A. (2017). WannaCry: Are Your Security Tools Up to Date? *The National Law Review*. Washington: Keller and Heckman LLP. Retrieved from https://www.natlawreview.com/article/wannacry-are-your-security-tools-to-date.

Nunziato, D. C. (2012). Preservar la libertad en Internet en las Américas. In E. Bertoni (Ed.). *Hacia una Internet libre de censura*. Palermo: Facultad de Derecho Centro de Estudios en Libertad de Expresión y Acceso a la Información, Universidad de Palermo.

OONI data. (2016b). Retrieved from https://web.archive.org/web/20171122001953/https://api.ooni.io/api/v1/measurement/temp-id-16865057.

OONI data. (2017c). Retrieved from https://web.archive.org/web/20171122003329/https://api.ooni.io/api/v1/measurement/temp-id-35388992.

OONI data. (2017d). Retrieved from https://web.archive.org/web/20171122023656/https://api.ooni.io/api/v1/measurement/temp-id-93684079.

OONI data. (2017e). Retrieved from https://web.archive.org/web/20171122024003/https://api.ooni.io/api/v1/measurement/temp-id-79070065.

OONI data. (2017f). Retrieved from https://web.archive.org/web/20171122023249/https://api.ooni.io/api/v1/measurement/temp-id-93858456.

OONI (2016a). *OONI test specifications* [Web connectivity test specification]. Retrieved from https://github.com/TheTorProject/ooni-spec/blob/master/test-specs/ts-017-web-connectivity.md.

OONI (2017a). *OONI Explorer report of Riseup website URL*. Retrieved from https://explorer.ooni.torproject.org/measurement/20170522T011558Z_AS22047_m9OSyUAyfTh8Dlqt2FVbpj0V3gnzDyRYfcjytDMjK5cptY5wVL?input=https:%2F%2Friseup.net.

Secretaría Jurídica Distrital de la Alcaldía Mayor (2001). *Ley 679 de 2001*. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=18309.

Telefonica ISP (2017). *Gambling landing block page*. Retrieved from https://web.archive.org/web/20171122011901/http://www.telefonica.co/JuegosPorInternet.

Tigo Une ISP (2017a). *Landing block page*. Retrieved from https://web.archive.org/web/20171121230229/http://controldecontenido.une.net.co.

Tigo Une ISP (2017b). *Gambling landing block page*. Retrieved from https://web.archive.org/web/20171122011303/http://www.controldecontenido.une.net.co/ControlJuegosAzar.htm.

Tor project (2017). *Tor FAQ*. Retrieved from https://www.torproject.org/docs/faq#KeyManagement.

Ververis, V., Isaakidis, M., Loizidou, C., & Fabian, B. (2017). Internet censorship capabilities in Cyprus: An investigation of online gambling blocklisting. *E-Democracy*. Berlin: Springer [CCIS 792, in press].

Ververis, V., Kargiotakis, G., Filastò, A. Fabian, B., & Afentoulis, A. (2015). Understanding Internet Censorship Policy: The Case of Greece. *Free and Open Communications on the Internet, USENIX*, 2017, Vancouver, BC, Canada.

Ververis, V., Xynou, M., & Scott, W. (2016). *OONI Data Reveals How WhatsApp Was Blocked (Again) in Brazil*. Retrieved from https://web.archive.org/web/20160906002832/https://ooni.torproject.org/post/brazil-whatsapp-block.