SMALL MEDIA

IRANIAN INTERNET INFRASTRUCTURE AND POLICY REPORT

// January - February 2013
// www.smallmedia.org.uk

INTRODUCTION 1

// As the June election approaches and the internal politics of the government becomes more continuous, Iran's Internet connectivity, and the accessibility of uncensored information, continues to deteriorate, reflecting offline crackdowns on the press. Prominent Persian-language websites and other online services have been filtered one by one, and communications with external platforms is becoming progressively more difficult. From a technical perspective, few things have been changed in recent months, and in this report we focus on the evolution of the infrastructure policies of the Telecommunication Company of Iran and Ministry of Information and Communications Technology, as well as the ramping up of the censorship of pro-government media.

POLICY DEVELOPMENTS 2

CONTENT FILTERING AND BLOCKED SITES

- **JANUARY - FEBRUARY**: Persian-language music blogs, dating sites, digital securit information and movie download hubs are subject to increased filtering and content takedown orders. Sites hosted through Iranian-owned service providers, including those on foreign-based servers leased by companies such as Mihan Web Host, began to display notices that offending domain had been blocked by the Committee for Determining Examples of Criminal Web Content, advising the owner on how to appeal the takedown. Examples can be found on fullmusic4.ir, marshalsat.pro, num1vpn1.org, and myplus.ir. Contrary to initial reports, these domain names were not seized by the domain registrar or the country-level Internet registry, instead content was removed by the host company and a filtered page was posted in its place.


این دامین به دستور دبیرخانه کارگروه مصادیق مجرمانه اینترنتی مسدود شده است

چنانچه مالک این تارنما به مسدود سازی و پالایش تارنمای خود اعتراض و شکایت دارد می تواند جهت پیگیری از طریق نشانی rafefilter.internet.ir شکایت خود را به دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه ارسال نماید.

با سپاس | واحد ارائه دهندگان خدمات میزبانی / دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه | تلفن/نمابر: 02133927413

- **1 JANUARY 2013**: Travian, a popular Persian-language online roleplaying game, was blocked despite having a license from the Ministry of Culture and Islamic Guidance. According to Fars News Agency, Travian was blocked in order to support 'the development of domestic online game companies,' 'to protect personal information' and 'protect against the transfer of money out of the country.' Travian was unblocked on January 10, 2013,

(Source: 1, 2, 3) but the company notified users that the website will be completely shut down on March, 21, 2013. Travian has had 150,000 users in Iran, of them 100,000 are active. (Source: 1, 2) The founder of the first domestically produced game, 'Asmandez,' reacted to he incident, saying that filtering is not a solution to support national game production. He continued that, while filtering is a momentary shock for users, after a few days, the users can find the new way to bypass it. (Source)

- **17 JANUARY 2013**: The anonymous question and answer site, Ask.fm, was blocked without any explanation. This service was popular amongst Iranian Twitter users and the filtering is occurring at the international gateway. (Source)

- **19 JANUARY 2013:** Google is reported blocked for several hours. Although it is unclea why, on what ISPs or for how long, Google's Transparency Report does show a decrease in incoming traffic from Iran during this time. (Source)

- **20 JANUARY 2013:** The Ghariv website was unblocked after being filtered on 12 De cember 2012, due to a complaint filed by the Director of the Iranian Blood Transfusion Organization (Fars branch) (Source). The news site Shiraze was blocked in December for similar reasons, and it now appears to be available as well. (Source)

- **27 JANUARY 2013:** The pro-government news sites Tabnak and Baztab Emrooz are blocked for several days due to the content of user comments, allegedly under the order of the Prosecutor General of Tehran. (Source) Both sites have been linked to former Presidential candidate Mohsen Rezaee, and Baztab was previously filtered in 2005 and shut down in 2007 for comments regarding government figures and for reasons of 'national secu rity.' (Source) Two years later, the Baztab team relaunched the current site, Baztab Em rooz, on a server based outside of the country. Whereas Baztab Emrooz was directly filtered at this time, Tabnak is hosted by the domestic provider 'Iran Samaneh.' Rather than direct government filtering, it appears that the Tabnak's services were firewalled from the rest of the domestic and global Internet by the hosting company. From probes of the Tabnak site, it was evident that the server was still on during this time and had been restarted recently, perhaps in response to its sudden unavailability. Baztab Emrooz also reported being the target of a denial of service attack during this time, which we independently correlated with high network latency. It has since began using the service Cloudflare to protect their site.

TABNAK.IR	
FILTERED (JANUARY)	**NOT FILTERED (FEBRUARY)**
25/tcp open smtp Postfix smtpd 80/tcp closed http 443/tcp closed https Uptime 1.806 days (since Fri Jan 25 22:24:44 2013)	25/tcp open smtp 80/tcp open http 443/tcp open https
7 195.146.33.30 1.677ms 8 78.38.240.41 1.949ms 9 78.38.255.58 1.634ms 10 85-15-0-73.rasana.net 2.271ms 11 85-15-0-6.rasana.net 2.535ms 12 85-15-0-30.rasana.net 4.677ms 13 94-182-146-21.rasana.net 1023.905ms	10 195.146.33.30 140.261ms 11 78.38.240.41 199.263ms 12 78.38.255.58 203.065ms 13 85-15-0-177.rasana.net 189.394ms 14 85-15-0-6.rasana.net 202.349ms 15 85-15-0-165.rasana.net 186.427ms 16 85-15-0-174.rasana.net 189.281ms 17 85-15-0-30.rasana.net 188.068ms 18 94-182-144-138.rasana.net 192.185ms 19 94-182-146-21.rasana.net 126.706ms

- **28 JANUARY 2013:** Tarikhe Irani (The Iranian History) is blocked without any explanation. The website has stopped its services since, and stated that they will not publish any more content due to the restrictions. This websites was managed by Sadegh Kharazi, a former Deputy Foreign Minister. (Source)

STATEMENTS FROM MINISTRIES

- **DECEMBER - FEBRUARY**: Reza Taghipour, head of the Ministry of Information and Communications Technology since 2008, was dismissed 11 December 2012 and named an adviser to the President on ICT issues. (Source) Upon the dismissal, President Ahmad inejad attempted to appoint the head of the Ministry of Roads and Transportation to lead the agency, as well as to combine it with the Ministry of Urban Development. After being blocked in both attempts by the Majlis, Armed Forces General Mohammad Hassan Nami was named interim administrator, and in February confirmed as its head. (Source) The appointment of Nami made widespread headlines for his having pursued graduate studies in North Korea's Kim Il Sung University, reported connections with the design of the national Internet and involvement with a domestic Google Earth competitor.

- **26 JANUARY 2013:** Mehdi Akhavan Behabadi, Secretary of the Supreme Council of Cyberspace, announced several significant policy changes in an interview with Khabar Online (Source), including:
  - *VPN Registration:* Internet users will soon be able to buy state-approved VPN connections, and that all VPNs in the market at this time are illegal. Behabadi stated that the purpose of the registration is to the benefit of security of the users in their on-line banking and corporate transactions. Accordingly, the use of VPNs has to be deemed "legitimate" by the Ministry to be legal and the provider must register on www.vpn.ir. This site is only reachable to Iran users, as it is located on the private national network.

;; ANSWER SECTION:

vpn.ir.	**3342**	**IN**	**A**	**10.201.22.74**

  - *Filtering is Going Intelligent*: In the next three months, Internet filtering will begin to occur more frequently based on content, and not against whole domains or websites. However, certain sites, such as social networks, will remain entirely blocked.
  - *More Access for Domestic Hosting*: The government will begin sponsoring domestic hosting services for websites, including through decreasing costs at national data centers, and providing other incentives to encourage administrators to move their hosting to a domestic location. This push will begin with news sites and move toothers progressively.

- **NATIONAL NETWORK:** Iran's national network has officially entered its second phase and the Ministry of Information and Communications Technology believes that they can test the network in the next Persian year, which begins in March. (Source) Additionally, the Ministry has changed the name of the network from "National Information Network" to "Internal Virtual Network". (Source)

- **INTERNET SPEED:** In an interview with ISNA, Ali Tavasoli, a member of the Supreme Council of Cyberspace, stated that the poor Internet performance is not due to an international gateway outage. Instead, the problems are being caused by the infrastruc ture require ments of "cyber attacks" on Iran's network. (Source) This follows recent reports of slow speeds and the disruption of specific services, such as Google TalCivil

CIVIL SOCIETY, PROFESSIONAL ORGANIZATION STATEMENTS

- **MEHDI AKHAVAN BEHABADI**, in another interview with ISNA, stated that joining social networks is not illegal according to the Cyber Crimes Law, however, the use of circumven tion tools is prohibited and users may be subject to prosecution. Behabadi went on to state that the current implementation of content filtering is not efficient and requires revision, however, there remains a national need for the filtering of illegal content (Source)

- **ESMAEIL AHMADI-MOGHADDAM**, chief of the National Police stated that his organiztion does not have any direct involvement in the filtering of the Internet. (Source) However, on 4 January 2013, Ahmadi-Moghaddam announced plans to develop software and strat egies to control social network sites. (Source)

- **AYATOLLAH MAKAREM SHIRAZI**, in response to an online theological question about using Rightel's video call service, stated that such technologies brings corruption to the Islamic society. (Source) Soon afterward, a website was started to promote negative news and stories about Rightel. (Source)

TECHNICAL DEVELOPMENTS

// As anniversaries and political events that have historical triggered increased technical and non-technical interference with access to information and independent media approach, the policy trends and statements of government officials enable us to reexamine the nature of Iran's Internet and predict where to look for future changes. When the national email providers were introduced last year, we saw the disruption of Gmail and governmental policies promoting the use of domestic mail for reasons of 'privacy and information security.' Where the Supreme Council of Cyberspace promotes new policies on the registration of VPNs, we can expect that unregistered VPN connection will be blocked and throttled. As VPNs have been one of the most popular anti-filtering mechanisms, this rhetoric also highlights the necessity of educating users on the new and differing types of anti-filtering technologies freely available. Similarly, Ahmadi-Moghaddam's comments on more sophisticated filtering hint at the possibility of a change in the software and hardware that drives the censorship apparatus. In this iteration of the policy report, we begin discussion of three nascent trends that we believe hint at the future of Iran's Internet, with the intent to revisit them in more detail in subsequent occasions.

VIBER AND WHATSAPP BLOCKED

Beginning in early February, users on social networks and social media began to complain that the popular text and voice communications service Viber had stopped sending messages. Shortly thereafter, another chat service, Whatsapp, became unusable. Upon investigation, it appears that this block is in place at least on Mobinnet, Parsonline, SabaNet and Shatel for both Android and iOS versions of the applications. (Alternative Reference)

THROTTLED AND BLOCKED ANTI-FILTER TOOLS

Tor, the famous anonymization and anti-filter tool, appears to be the subject of sophisticated disruption and blocking. Users on Parsonline, Mobinnet and Shatel have reported difficulties connecting to the Tor network and Tor's metrics have shown rapid fluctuations in use. (Source: 1, 2)

Iranian Internet users report still being able to use other tools such as SOCKS Proxifire, Freegate and Hotspot Shield. (Source)

INBOUND SSH FILTERING

As a component of encouraging the adoption of domestic platforms for hosting online content, the Fifth Development Plan mandated the establishment of regional data centers, which offer leased servers and collocation. From public documentation and connectivity tests, it would appear that SSH on its normal port, 22, is blocked to international connections for the service providers Tebyan, Soroush Rasanheh and Afranet. These blocks appear to be based on firewall rules, instead of protocol detection through deep packet inspection, as connectivity is possible on an alternative port.

NETWORK ANALYSIS

UPDATES

REMOVED SMTP PROXYING

In our last report, we found that some ISPs were performing transparent proxying of the SMTP mail delivery protocol. However, before we were able to confirm and trace where in the network the interception was occurring, it appears to have ended. We will continue to monitor for surveillance of services and collect data where possible, particularly for those critical channels such as mail and web.

SIP BLOCKING

It appears that streaming communications services are being interfered with, specifically those based on the RTP protocol and on the networks of Mobinnet and Shatel. Since the previous report, these ISPs have unblocked SIP voice service on port 5060 (UDP), however, voice over IP calls will likely drop due to RTP packet lost.

TCI DSL SERVICE	PISHGAMAN TOSEH ERTEBAT	MOBINNET
ICSI NETALYZR		
Direct TCP access to remote SIP servers (port 5060) is blocked. Basic UDP access is available. The client was unable to send fragmented UDP traffic. The most likely cause is an error in your network's firewall configuration or NAT. The maximum packet successfully sent was 1442 bytes of payload. The client was unable to receive fragmented UDP traffic. The most likely cause is an error in your network's firewall configuration or NAT. The maximum packet successfully received was 1452 bytes of payload. UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The client was unable to transmit a non-DNS traffic on this UDP port, but was able to transmit a legitimate DNS request, suggesting that a proxy, NAT, or firewall intercepted and blocked the deliberately invalid request. Changes to headers or contents sent between the client and our HTTP server show the presence of an otherwise unadvertised HTTP proxy. The following headers had their capitalization modified by the proxy: Content-Type: text/html Content-Length: 770 Last-Modified: Tue 26 Feb 2013 07:51:28 GMT Set-Cookie: netAlizEd=BaR; path=/; domain=netalyzr.icsi.berkeley.edu Connection: keep-alive The following headers were added by the proxy to HTTP responses: Proxy-Connection: keep-alive The detected HTTP proxy changed images that were sent from our server. The detected HTTP proxy changed either the headers the client sent or the HTTP response from the server. We have captured the changes for further analysis. We detected the presence of an in-network transparent HTTP cache that caches data which was directly requested by the client. EDNS-enabled requests for small responses remain unanswered. This suggests that a proxy or firewall is unable to handle extended DNS requests.	UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The client was unable to transmit a non-DNS traffic on this UDP port, but was able to transmit a legitimate DNS request, suggesting that a proxy, NAT, or firewall intercepted and blocked the deliberately invalid request. The path between your network and our system supports an MTU of at least 1500 bytes, and the path between our system and your network has an MTU of 1480 bytes. The path MTU bottleneck that fails to properly report the ICMP "too big" is between * and *. The path between our system and your network does not appear to report properly when the sender needs to fragment traffic. EDNS-enabled requests for large responses remain unanswered. This suggests that a proxy or firewall is unable to handle large extended DNS requests or fragmented UDP traffic.	UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The client was unable to transmit a non-DNS traffic on this UDP port, but was able to transmit a legitimate DNS request, suggesting that a proxy, NAT, or firewall intercepted and blocked the deliberately invalid request. EDNS-enabled requests for large responses remain unanswered. This suggests that a proxy or firewall is unable to handle large extended DNS requests or fragmented UDP traffic.

EDNS-enabled requests for medium-sized responses remain unanswered. This suggests that a proxy or firewall is unable to handle extended DNS requests or DNS requests larger than 512 bytes. EDNS-enabled requests for large responses remain unanswered. This suggests that a proxy or firewall is unable to handle large extended DNS requests or fragmented UDP traffic. A detected in-network HTTP cache incorrectly caches information Weakly uncacheable data was cached between you and our server, even when the data was requested directly and explicitly. This suggests that there is an HTTP cache in the network which examines and caches web traffic. Since this content was not supposed to be cached, the HTTP cache is probably operating incorrectly.		
TRACEROUTE 4.2.2.2		
7 * * * 8 10.21.22.97 132.493 ms 10.21.28.97 117.942 ms 9 10.21.21.65 104.776 ms 10* * * 11* * * 12 * * * 13 * * *	6 *** 7 10.152.32.249 78.021ms 8 78.38.240.90 66.183ms 9 217.218.154.250 99.562ms 1010.10.53.26 90.637ms 10.10.53.6 75.746ms 10.10.53.26 94.378ms 1179.133.75.161 160.180ms 12 (..)rostelecom.ru 169.605ms 13 ***	3 *** 4 10.47.33.2 85.031ms 5 78.38.250.1 78.695ms 6 10.10.53.142 69.374ms 7 92.50.194.237 454.566ms (..)pccwbtn.net 486.660ms 10.10.53.246 73.188ms 8 (..)telia.net 511.590ms (..)rostelecom.ru 362.436ms (..)pccwbtn.net 331.174ms
TRACEROUTE 8.8.8.8		
7 * * * 8 10.21.22.97 132.493 ms 10.21.28.97 117.942 ms 9 10.21.21. 65 104.776 ms 10* * * 11* * * 12 * * * 13 * * *	6 *** 7 10.152.32.249 48.616 ms 8 78.38.240.90 99.733 ms 9 217.218.154.250 78.249 ms 10 10.10.53.26 96.858 ms 10.10.53.6 70.005 ms 10.10.53.26 85.908 ms 11ldn-b1-link.telia.net 203.431 ms	3 *** 4 10.47.33.2 84.891ms 5 78.38.250.1 73.677ms 6 10.10.53.142 68.994ms 7 (..)pccwbtn.net 454.942ms 92.50.194.237 414.496ms (..)telia.net 486.229ms 8 10.10.53.109 72.148ms (..)pccwbtn.net 410.098ms 95.167.93.97 408.325ms 9 (..)telia.net 506.006ms 74.125.49.77 421.422ms (..)telia.net 495.223ms

Visual Traceroutes

Red: Domestic,

Brown: International Routes,

Blue: End Destinations