SMALL MEDIA

IRANIAN INTERNET INFRASTRUCTURE AND POLICY REPORT

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

INTRODUCTION 1

// The extent of content access restrictions and general connectivity of the Internet in Iran has historically been strongly tied to domestic political and economic stability. Although filtering and throttling of international connection speeds are a daily experience for the average user, in times of crisis the Iranian government demonstrates the full extent of its capabilities for disruption and surveillance. Our reporting begins in October, in the days immediately following the return of Mehdi Hashemi Rafsanjani from self-imposed exile, the rapid depreciation of the exchange rate of the Iranian Rial, Ahmadinejad's U.N. General Assembly speech, global controversy over the film "Innocence of Muslims," and demonstrations over the economic health of the country. These moments of contention were met with substantial episodes of more aggressive and more sophisticated Internet censorship, in parallel to consistent satellite jamming and takedowns of locally-hosted websites. As the political order of the country returned to the status quo, there appears to have been less technical changes in content-filtering system and the apparatus reverted to its prior state. Outside of access restrictions, in recent months users had difficulties accessing normal websites, spawning rumors about changes to the domestic network infrastructure and difficulties paying for international transit and equipment.

POLICY DEVELOPMENTS 2

// During the reporting period, a pattern of the filtering and takedown of foreign currency trading sites emerged as a response to the rapid speculative devaluation of the Iranian Rial. As a result of either being blocked, if hosted internationally, or disabled by their local host, a number either began to self-censor or moved to other platforms, such as foreign social media, in order to continue operations. These enforcement activities mirror statements by government officials and events describing the role of domestic content platforms in the "National Internet," particularly with regard to the reach of judicial or national security takedown processes.

CONTENT FILTERING AND BLOCKED SITES

- 3 October 2012: Several websites that show the foreign exchange rates of the Iranian Rial and precious metals, such as Mazene, Sarafi Tehran, Mesghal and Online Currency, are blocked in Iran. Some of these websites change the displayed price of currency to zero, in order to protect themselves against the filtering. Mesghal's Iranian webhosting account was later suspended and the site moved its reporting to a Facebook page. As of January 2013, restrictions on exchange websites have not been lifted. (Source)

- 5 October 2012: Foreign-hosted multimedia content, such as MP3, MP4, AVI and SWF files, are filtered without any explanation a week after unblocking of Gmail. These restrictions are removed within the week. [Mechanisms Further Described in "Technical Developments" Section] (Source)

· 22 October 2012: Dr. Behbood Gorjizadeh's official website is blocked. Gorjizadeh attempted to run in the 2012 Parliamentary election for the Gachsaran county but had his eligibility rejected by authorities. Although the site remains blocked, it reports about 1,500 visitors a month and continues to publish content, such arguments for structural changes to the administration of natural resources. (Source)

· 29 October 2012: Zahedan Press, an ultra conservative news website that covers the Sistan and Baluchestan province, is blocked after a lawsuit by the Governor of Sistan and Baluchestan, potentially due its accusations of terrorist affiliations at a time of hostilities with the province's significant Baluch population. (Source) On December 9, after protests from religious groups and a court appeal, it is unblocked by the order of judicial authorities. (Source)

· 17 November 2012: LinkedIn, previously the last remaining unfiltered, popular social network, is blocked without any explanation. At the time of publication, LinkedIn was available on at least one ISP, suggesting the episode was limited or lifted. (Source)

· 12 December 2012: Shiraze and Ghariv, two conservative news websites are blocked despite having registered on the Ministry of Islamic Guidance and Culture's Samandehi website. Shiraze has been particularly prominent in the Fars province since it launched in 2010. By January 2013, this restriction appears to have been removed. (Source)

· 24 December 2012: Green Press, a famous environmental advocacy site, is blocked due to a lawsuit by Iran's Environmental Protection Agency. The site's domain name, greenpress.ir, appears to have been revoked by Iran's central registrar, IRNIC, since the court decision and the organization moved publication to a Facebook page and another site. (Source)

· 25 December 2012: Several websites that carry news about gold and jewelries price, such as Iran's National Union of Gold and Jewelry and Tehran Gold and Jewelry Union, are blocked. The reasons for the filtering are unclear although the growth of gold price in Iran and unstable economic situation is assumed to be one of the main reasons. The latter is available at publication, while the former remains blocked. (Source)

POLICY

· 3 October 2012: Mehdi Akhavan Behabadi, the secretary of the Supreme Council of Cyberspace announced the council will take over filtering regulations and policies. Other ministries, committees, communications companies and government agencies will act based on these decisions. Behabadi said Iran has not any plans to cut off the Internet and replace it

by the National Internet. In addition, a National Center of Cyberspace will begin operations, with three committees on: (Source)

a. Cyberspace Regulation and Policies
b. Security in the Cyberspace
c. Increasing the Content in the Cyberspace.

· 23 December 2012: Behabadi, in another interview with ISNA, stated that he does not believed in an official, "National" email, search engine, or Internet. In this interview, he rejected any plans to launch a "National Internet" and argued that the phrasing is incorrect. Regard to Behabadi, Iran has a plan to reduce the amount of filtering, although it does not mean the system will completely disappear. He also reiterated that the blocking of Gmail in late September was an accident that resulted out of attempting to add further restrictions to YouTube. (Source)

CIVIL SOCIETY, PROFESSIONAL ORGANIZATION STATEMENTS

· Mehdi Botourabi, the director of the popular blogging platform Persianblog stated on October 10th, that the filtering of blogs has increased exponentially, and the rate this year (2012-2013) is six times more than last year. (Source)

· Naeimeh Eshraghi, granddaughter of Ayatollah Khomeini, in an interview with Asr Iran criticised the censorship of the Internet in Iran, particularly of Facebook. In the article, she argues that Facebook is a way for better understanding the Iranian people internationally and stronger public dialogue domestically. (Source)

· The Iranian Artists Forum, on 27 December 2012, strongly criticised Internet censorship and satellite jamming in Iran. Amongst a wide array of public figures and media, a former Minister of Culture and Islamic Guidance and a former Deputy of Cinema were participants in this meeting. (Source)

· Alireza Shirazi, the founder of another famous Persian-language blogging site, Blogfa, expressed concerns on Twitter about the future of the domestic blogosphere due to filtering: "Horrible events are occurring. I receive orders to block around or more than 100 blogs per day. In the future, [we won't] have any blogs." (Source) Shirazi has previously noted weeks where Blogfa received up to 600 takedown orders, elaborating that they are often for offending terms related to hacking and music. (Source)

TECHNICAL DEVELOPMENTS 3

BLOCKING MULTIMEDIA CONTENT BY TYPE

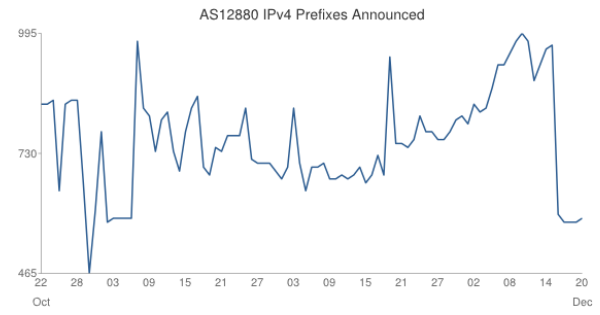
Beginning around October 6 2012, timed with demonstrations over economic conditions, the Telecommunications Company of Iran, blocked foreign-hosted media files. According to initial reports, this blocking targeted audio (.MP3), video (.MP4, .AVI) and Adobe Flash/Shockwave content. Attempts to access these files would result in a "request timeout," effectively no answer to the attempt to fetch content, which differs from normal blocking that generates a 'Forbidden' code and blocked webpage response.

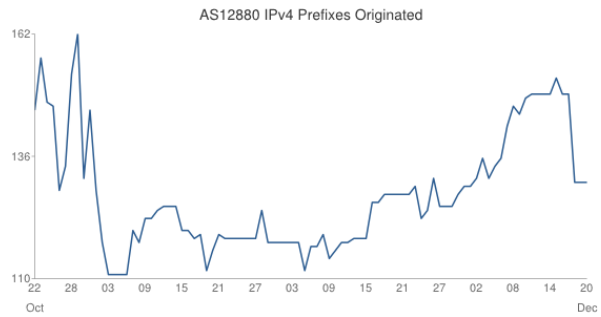
Upon investigation, it appears that the trigger was based on header information returned from the server, rather than the file extension or deep packet inspection specifying multimedia content. A constructed response, returning only a 'Content-Type' header set to 'audio/mpeg,' would trigger the described behavior. This episode is additionally unique from normal filtering because it is based on data returned from the server, rather than requests sent from the client. The nature of the blocking made research into the origin of these filtering rules difficult, and the interference had ended within the week. (Source)

POOR NETWORK PERFORMANCE AND SUSPICIOUS DISRUPTIONS

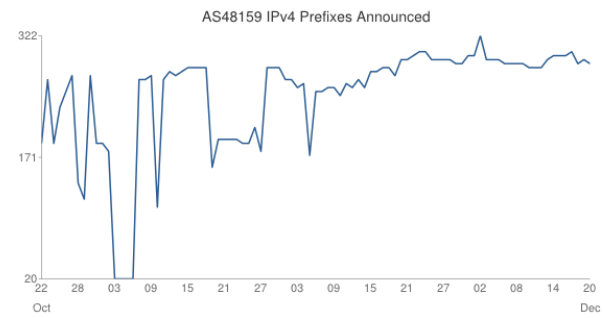
The reporting period has been marked by both anecdotal and measurable indications of network instability. Overall, it would appear that a number of consumer ISPs have suffered from 10-20% packetlost. This and reliable will fluctuate throughout the day with huge performance decrement in connectivity during traditional office hours. Furthermore, suspicious BGP activity and also, triggering a rumor about BGP attack against the traffic exchange points of the Telecommunication Infrastructure Company of Iran. According to the public data offered by the Internet backbone provider Hurricane Electric, substantial drops in BGP advertisements occur in late October and in early December for the two international gateways. Renesys, a network monitoring service, offers reports that show substantial and frequent disruptions to the connectivity of specific ISPs. (Source) These disruptions may in part be linked to the explosion of natural gas pipeline that also carried telecommunications links. (Source) However, regardless of reason, Iran's international connectivity remains one of the most unstable in the world. (Source)

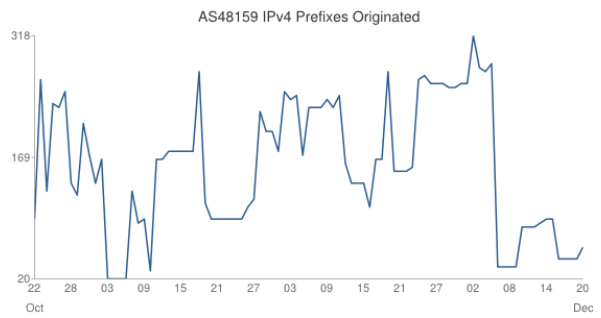
BGP Activity for AS12880, Information Technology Company (Source)	





BGP Activity for AS48159, Telecommunication Infrastructure Company of Iran (Source)	





INGRESS FILTERING

Although the use of filtering to block external websites is well known, there is little documentation of restrictions on the accessibility of domestic Iranian content to an outside audience. During one investigation on the national use of private network addresses, it was noted that content hosted in this space would naturally be unreachable from outside, however, this differs from a content filter actively inspecting incoming connections in order to terminate offending requests. (Source) Between October 2012 and January 2013, the domestically-hosted website of the Association of Iranian Exchanges (kanoonsarafan.com), an independent, apolitical and nonprofit organization of currency traders licensed by the Central Bank of Iran, was blocked to connections originating from outside of the country, including to domestic users on a VPN. Connections from outside to any server in Iran requesting the domain in the Hostname or the the full URL (such as "http://peyvandha.ir/www.kanoonsarafan.com") would return a "403 Forbidden" response, with the blocking reason as "Invalid Site" or empty, respectively. While the site remained reachable within the country, it appears that the blocking occurred at the international gateway.

As of January 2013, a cursory examination of search engine results for sites that match the Iranian filtering response returned a small set of blogs that appear to be blocked for non-Iranian

visitors, including two photoblogs and a hip hop music site -- dastpokht.mihanblog.com (now deleted), 2fblog.mihanblog.com, rap3da58.com.

ANTI-FILTER TOOL LOCKING

As of December, users on Mobinnet, Pishgaman and TCI ADSL Service have been unable to use the Spotflux anti-filtering service. Early March the company had claimed that, when the government blocked access to secure web services, "more than one thousand Spotflux users in Iran were able to continue accessing the web, while remaining safe from the sort of deep packet inspection that might tip off the repressive regime." (Source) Spotflux appears to be a customized frontend for the popular, open-source OpenVPN tunneling software. The mechanism for this blocking is unclear, other OpenVPN-based service have previously been disrupted through deep packet inspection, but blocking of Spotflux may have been more easily accomplished through blacklisting the service's IP addresses.

Additionally, unconfirmed reports have suggested that Pars Online and other ISPs may be interfering with access to Tor, although the anonymity network still maintains a large user base in Iran that has not substantially declined around the time of such reports. (Source) Upon inquiry, other providers have reported that their user base has remained stable during the reporting period.

DNS HIJACKING

Around October 2, DNS requests throughout the country for 'youtube.com' began to return the address of 10.10.34.34, otherwise known as the domestic filtered site page. Watching data in transit, it would appear that the false answers originated out of the private network that acts as Iran's international gateway, around network of 10.10.53.34 and mostly likely operated by the Data Communication Affairs department within the TCI. Additionally, TCP requests, rather than the normal UDP, returned the legitimate results. While it appears all international DNS requests are potential subject to inspection, only UDP traffic triggers false answers. While the nationwide tampering has ended, it is unclear if other domains are subject to interception and to what extent such activities occur at the ISP level. Publically-searchable, Persian-language blogposts have documented previous cases of such attacks against social networks and popular opposition sites. (Source)

This interception technique should be disconcerting regardless of the availability of anti-filtering tools and VPN services. It was noted in the incident report on the breach of the Dutch company DigiNotar, which led to the forging of security credentials that were later used to spy on Internet users in Iran, that of the logged requests to authenticate the false certificates, "95% of these IP addresses originated from the Islamic Republic of Iran" and that a "sample of the remaining 5% of the affected IP addresses was inspected, which mainly showed exit nodes

for The Onion Router (Tor), proxies and Virtual Private Network (VPN) servers." The report adds,

> *"The most likely modus operandi used during the [man-in-the-middle] attack, based on the accumulated OCSP data, is that of Domain Name System (DNS) cache poisoning... This modus operandi would explain why traffic that went through proxies, Tor exit nodes and VPNs was also affected by the MITM attack ... "*

(Source, PDF)

Unless the anti-filtering tool properly tunnels DNS traffic securely out of the country and authenticates itself to the user, an intermediary may be able to control the user's online activities and even completely hijack their connection for surveillance or filtering, even though they may think they are safely protected by the irnormal provider.

INFRASTRUCTURE DEVELOPMENTS

· 10 November 2012: Reza Taghipour, Minister of Information and Communications Technology, repeated previously heard statements about the national network mandated in the Fifth Five Year Development Plan including 20 Mbps connectivity. According to Taghipour and statements by others, the Telecommunications Company of Iran and private companies plan to provide a fiber Internet connections for 10 million homes, based on FTTH or FTTx technology, within the next eight years. (Source: Aftab, Comments to ITU by the Communication Regulatory Authority of Iran)

· 18 December 2012: Broadband Regulatory Commission approved an increase of broadband Internet tariffs increased by about 50 percent, according to TIC the cost of service for end users will rise by about 10 to 15 percent. According to the Commission, the price change is due to changes in the foreign exchange rates causing increases in the cost of international transit. (Source: ISNA, Tabnak)

· RighTel, the third mobile service provider of Iran, is increasing its coverage for 3G and now has 17 cities under partial 3G mobile coverage.

· TCI has started to advertise consumer ADSL service in large provinces, which indicates that they have installed more telecommunications equipment recently, such as DSLAMs.

· Mobinnet, the biggest WiMax provider in Iran, reports 135 cities under coverage.

RUMORS 4

// Considering the role of secrecy in a censorship and surveillance regime, it remains difficult to fully account for the various assertions and claims that spread through personal networks, blogs and social media. While rumors always warrant skeptical evaluation, they have on a number of occasions turned out at least partially correct in the history of Iran's Internet, and thus are significant to the process of modeling potential security threats, as well as the identification of areas for future research. We present such statements as claimed and attempt to cite related evidence were possible.

In the course of the reporting period, a significant number of claims have been made that regarding disruptions to connectivity. In addition to the rumors of attacks against the network, other accounts have alleged that TCI has lost some of it's gateway connectivity due to infrastructure or payment issues, transitions of the network to Huawei-based products, and failures of the filtering system. Additionally, we do note, based on cursory evidence, that some networks have increased their capacity for DNS hijacking and Voice-over-IP blocking.

COORDINATION OF NETWORK TIME AND RECORDING OF RAW TRAFFIC

In order to more precisely coordinate the logging of Internet traffic ISPs, mandated by the Cyber Crime Law, government telecommunications agencies have required that providers use TCI's central time server (NTP). Additionally, they have deployed servers, running tcpdump, for the collection of the raw traffic streams of users inside of ISP data networks.

ONE BASE CONTENT FILTERING SYSTEM LEAD TO PERFORMANCE FAILURE

One of the most frequently offered causes for network disruptions and throttling is the centralization of Internet connectivity, for the purpose of censorship. This creates a situation where the whole of the country's traffic is reliant on one base and one node routing. Now after years of unstablenInternet connection, the government is attempting to decentralize filtering on a province level. Esfahan is the trial zone and new equipment is being installed in TCI's main building in the city. The main reason for the shift in infrastructure is to reduce the load on Tehran's equipment and reduce the network latency created by routing traffic out of a direct path. Additionally, the new centers can act as a failover solution for Tehran.

HUAWEI OR CISCO?

After increasing sanctions on Iran, TCI has had a more difficult time buying Cisco products for their network. They have started to deploy Huawei for some of their core routers and are providing Internet for some ISPs based on their new Huawei BGP Infrastructure. This rumor mirrors public press reports on sales of Huawei equipment to Iran (Source) and research on the equipment within the TCI. (Source)

FUTURE OF FACEBOOK BLOCKING?

Social Networks such as Facebook and Twitter will be unblocked. Naeimeh Eshraghi, an active Facebook user with a large following, commented to Anarpress that she had heard the social networking site will soon be unblocked by the regime, adding that Facebook is simply a tool and that authorities have "only now understood that these platforms cannot be harmful themselves." These rumors have followed calls from a wide range of Iran's blogger community to unblock Facebook, which arose after an official fan page for Ayatollah Ali Khamenei was created. (Source) However, in late December, Mehdi Akhavan Behabadi, in an interview with the Donya-e-Eqtesad newspaper rejected all reports about unblocking Facebook and other social networks. According to this interview, he adds that the Supreme Council of Cyberspace has a plan to manage social networks in the future. (Source)

NETWORK ANALYSIS 5

TCI DSL Service	Pishgaman Toseh Ertebat	Mobinnet
ICSI Netalyzr		
The applet was unable to receive fragmented UDP traffic. The maximum packet successfully received was 1452 bytes of payload. 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 195.22.211.217 and *. The path between our system and your network does not appear to report properly when the sender needs to fragment traffic.	Direct TCP connections to remote DNS servers (port 53) succeed, but do not receive the expected content. A DNS proxy or firewall generated a new request rather than passing the applet's request unmodified. A DNS proxy or firewall caused the applet's direct DNS request to arrive from another IP address. Instead of your IP address, the request came from [IP Removed].	UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The applet was unable to transmit an arbitrary request 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. A DNS proxy or firewall caused the applet's direct DNS request to arrive from another IP address. Instead of your IP address, the request came from [IP Removed]. A DNS proxy or firewall generated a new request rather than passing the applet's request unmodified. An in-path DNS proxy modifies NXDOMAIN errors. Instead of forwarding the error, the device replaces it with a response redirecting you to IP address [IP Removed].

6	* * *	
7	10.21.22.97	29.888 ms
8	10.21.21.65	27.558 ms
9	* * *	
10	89.221.34.190	113.948 ms
11	195.22.211.103	213.982 ms

8	78.38.240.90	79.509 ms
9	217.218.154.250	96.908 ms
10	10.10.53.30	91.776 ms
	10.10.53.6	141.744 ms
	10.10.53.30	84.443 ms
11	92.50.194.141	308.572 ms

7	10.10.53.142	309.082 ms
8	63.218.109.249	841.145 ms
	10.10.53.246	417.923 ms
9	87.226.139.57	836.385 ms
	63.218.44.190	469.799 ms
10	213.242.110.37	399.487 ms
	80.91.247.90	402.818 ms
	213.242.110.37	681.469 ms

Traceroute 8.8.8.8

7	* * *	
8	10.21.22.97	258.246 ms
	10.21.28.97	303.156 ms
9	10.21.21.65	304.729 ms
10	* * *	
11	89.221.34.190	280.281 ms
12	89.221.34.75	379.451 ms

8	78.38.240.90	78.527 ms
9	217.218.154.250	80.725 ms
10	10.10.53.30	80.819 ms
	10.10.53.26	79.504 ms
11	213.248.92.137	312.698 ms

7	10.10.53.134	86.050 ms
8	92.50.194.237	409.048 ms
	213.248.92.133	407.883 ms
	10.10.53.246	408.640 ms
9	63.216.0.38	616.271 ms
	80.91.248.90	423.712 ms

Visual Traceroutes

Facebook	Twitter