SMALL MEDIA

Iranian Internet Infrastructure and Policy Report

July - August 2013
smallmedia.org.uk

This work is licensed under a Creative Commons Attribution-NonCommercial 3.0 Unported License

INTRODUCTION

// On the early evening of September 16, Internet users in Iran began to report that they were able to access Facebook and Twitter without having to resort to anti-filtering tools. Although the censorship regime (colloquially known as the Filternet), had been known to fail for brief periods in the past, this time the opening paralleled the development of a political and social environment in which the relaxation of Internet restrictions has begun to feel inevitable. Perceptions of increasing state leniency have been fuelled by such positive developments as the commuting of web developer Saeed Malekpour's death sentence to life imprisonment.

There have been a number of other signs pointing towards liberalisation. In the previous edition of this series, we noted that the blogging site Tumblr had been unblocked, though we suspected this was unintentional, as several of the domains hosting media content for the platform remained filtered. In the following weeks, however, these addresses were also unblocked, and a semi-official account was created for the Supreme Leader (khamenei-ir.tumblr.com); however, the site was blocked again soon after. The rapid adoption of social networking by the vast majority of ministers in the Rouhani administration (including unprecedented activity by Foreign Minister Mohammad Javad Zarif on Twitter and Facebook) led foreign ambassadors and journalists to excitedly send out their first tweets describing a new *moderate* Iranian filternet. Only the most skeptical commentators repressed their incredulity to see what the morning would bring.

The skeptics were right to hold their tongues; morning brought the disappointment of business-as-usual, and a return to the use of unreliable anti-filtering tools. The sudden liberalization was apparently less due to the enlightenment of the authorities, and more a glimpse into exactly how fragile the apparatus actually is. Although a return to the status quo means continued isolation for Iranian internet users, this breakdown of the normal order at least brought a new understanding of the mysterious filtering regime. In order to address this topical issue, we begin with an attempt to explain what happened using technical evidence, directly disputing the claims made by state media. Despite this setback, we find hope in early government responses to the incident stating that the continued filtering of social networks would be considered by the Supreme Council on Cyberspace.

In this report we also address the emergence of a real shift in the policies and tone of the Iranian government, including the Ministry of Information and Communications Technology, which has laid the groundwork for these heightened expectations. Finally, we add a new feature, tracking the availability and performance of circumvention tools across different Internet Service Providers, in order to lessen confusion about what tools work and how well.

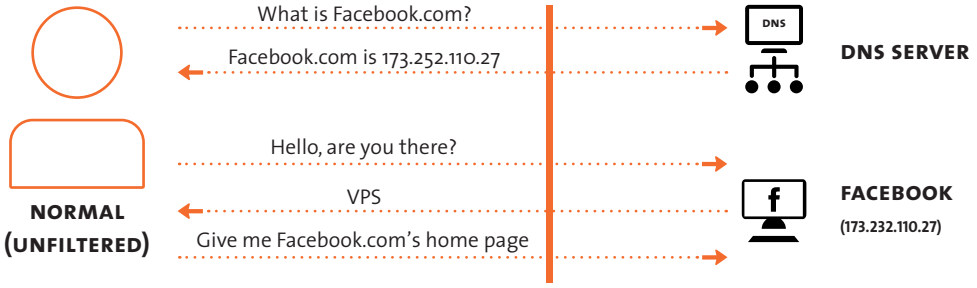
Collin Anderson (Editor) and Small Media

A DAY ON THE OPEN INTERNET: HOW THE FILTERNET FAILED

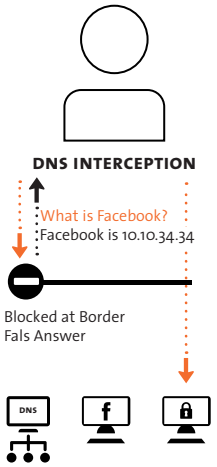
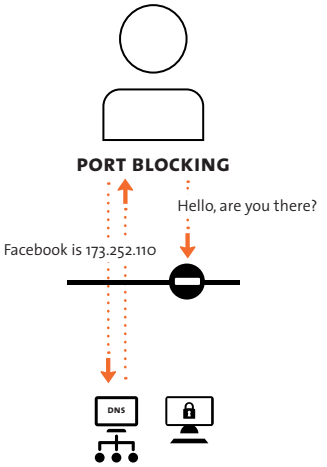
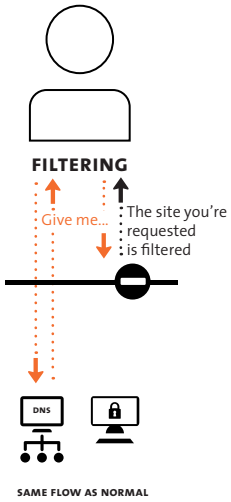
// Iran's censorship apparatus is a product of overlapping legal jurisdictions, physical control over the few pathways for traffic to take out of the country, and the pariah status of Iran's telecommunications sector in the eyes of international equipment vendors. This series has noted a number of occasions in the past where users have reported access to filtered sites, and other publications have documented how simple changes in requests made for blocked content are enough to trick the filter. However, Internet censorship is not necessarily enacted for the purpose of blocking a sophisticated individual from obtaining restricted information; to be effective, it simply has to make access difficult for the majority of the population, whom are often neither technologically-adept nor highly-motivated. As such, the legendary Filternet is ultimately a far simpler collection of standard network equipment than it is often made out to be.

The everyday filtering of web content in Iran is accomplished via one or more of three potential methods, and can be imposed by either the user's local Internet Service Provider (ISP) or the state-affiliated Telecommunications Company of Iran (TCI), which controls the back-end network infrastructure of the country.

HOW NORMAL WEB BROWSING WORKS



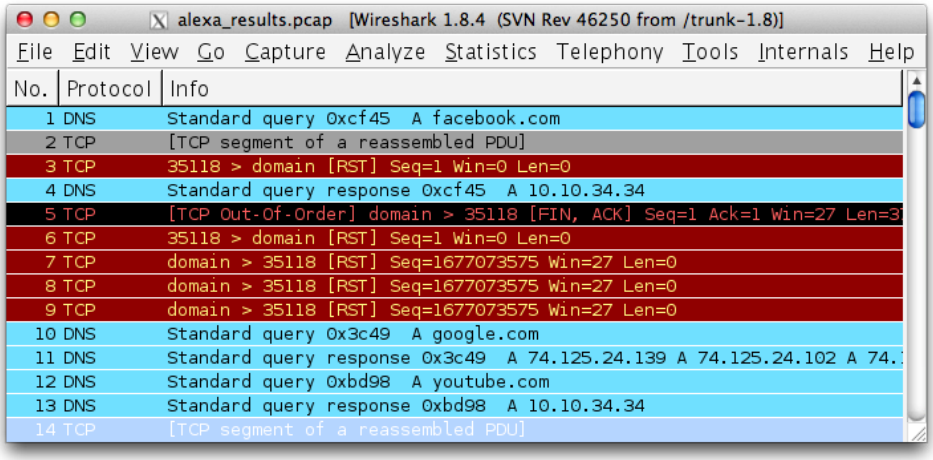
HOW CENSORSHIP OCCURS IN IRAN

DNS INTERCEPTION	ADDRESS OR PORT BLOCKING	WEB CONTENT FILTERING
		
Normally, when a user attempts to connect to a website, a request is made to a *Domain Name System* name server. These are simply directories that translate readable site names like *facebook.com* into Internet routable addresses (IP) like *173.252.110.27*. Under 'DNS Interception' these requests are caught by the Filternet, and false answers are sent back to the user without them knowing. These false answers can be used to send the user to a warning page like *peyvandha.ir* or to redirect them to a fake version of the site they requested.	The user requests the Internet routable address for a domain, and receives the real answer in the process. In *address blocking*, a device along the network between the user and the other end is configured to not deliver *any* traffic it sees destined for a specific address, such as *173.252.110.27* for Facebook. More narrowly, the devices may be configured to only block traffic that is directed for an address and specific *port*, a virtual channel on a computer that is often associated with a specific application - in the case of the web, port number *80*. For example, port blocking would enable the Filternet to allow standard unencrypted traffic, but block encrypted traffic.	The user requests the Internet routable address for a domain, and receives the real answer in the process. The two computers are initially able to connect, preparing both to exchange information, indicating that no address or port blocking is occurring. However, a device between the two ends monitors every request for web content, and checks whether the site or page matches a blacklist of censored content. When the user's web browser sends the request for the filtered domain such as *facebook.com*, the monitoring device finds that domain name is in the list and returns a fake response that contains the blocked site message.

Generally, in most situations, Web Content Filtering is the most simple and common method of restricting access to sensitive material. Interference through rejecting traffic to specific Internet addresses or redirecting visitors to different servers using DNS interception is inflexible, as it leads to the blocking of all access to the end host, whether or not the content is deemed offensive.

Web Content Filtering allows the network operators to create rules as narrow as blocking specific pages, or as broad as prohibiting the entire site. Web content filtering could be seen as equivalent to the monitoring of a phone network by a third party, with calls disconnected whenever banned names or words are mentioned. You might be able to make a call to a banned individual, but as soon as their name is mentioned, the connection would be dropped. Encryption - 'speaking in code' during the phone call - would disturb the monitoring system, making censorship more difficult. The growing expectation of encryption of web traffic (HTTPS) makes monitoring the Internet difficult, particularly when attempting to identify whether requests are for blacklisted sites. For example, if Facebook were to not use encryption, a government could inspect all traffic to see if they are requesting facebook.com or a specific page on Facebook. With HTTPS enabled, a censor only sees the connection as scrambled traffic between computers on the Internet. As a result, censors often chose to block all traffic to the Internet addresses or domain names of hosts of banned content, equivalent to completely disconnecting the phone of a suspect or listing a fake phone number.

Iran has often implemented all three against sites like Facebook and Twitter, with differences occurring between different Internet Service Providers. Small Media conducted tests against multiple ISPs during the incident to test accessibility and differences in networks. It appears that the Web Content Filtering method against Facebook and Twitter had not failed on Monday and normal requests would still trigger the filtered site page. However, many sites, including most major social networks, have moved to using encryption by default, in order to protect user privacy. If a user had previously visited either site through an anti-filtering tool, their browser would had saved the redirect to the HTTPS encrypted version of the site whether they knew it or not, meaning that the monitoring equipment would not be able to block the request. To counteract this, the frequency of DNS Interception in Iran increased, and was discussed as a subject of concern in the first Infrastructure report. For censors, DNS Interception is in some ways preferable to address blocking, as the latter is inflexible -- if a site changes Internet addresses, then the filter rules blocking traffic to that specific address would have to be updated. Sites often change IPs, but rarely change domain names.



During the opening, the filtering apparatus began to return a bizarre set of replies (packet trace above) for previously filtered sites. When a user would make a request for the Internet address of Facebook, it would not only trigger the Filternet's DNS Interception, but it would also send the Web Content Filtering response as well (an HTML message). The latter would not be understood by the user's computer, and potentially be received before fake address lookup. It is likely that this led to the false responses being ignored by the user's computer. With DNS Interception no longer working properly, unless ISPs had specifically blocked traffic to blacklisted website addresses, then no interception would stop a HTTPS connection resulting in these sites' potential availability. The differences between reports of availability could also correspond with some ISPs maintaining back-up content filters and DNS interference themselves, instead of solely relying on the state's censorship. This is unsurprising, as the Computer Crimes Law and other regulatory policies mandate ISPs to run their own filtering system.

Whereas the TCI had not previously maintained address or port blocking for the entire network on blacklisted sites, by the next morning the network had put this in place, blocking all traffic associated with secure web traffic to Facebook, Twitter and Balatarin addresses on all ISPs. During the opening, testing was conducted to determine whether access to Facebook and Twitter could be made across different ISPs, through directing connections to the real address of the sites; in most cases these sites were directly available and in about half of these tests no DNS manipulation affected the end user. Even queries to the TCI's own DNS server continue to return the real addresses for Facebook and Twitter. Now, however, traffic bound for the social media sites' addresses are blocked somewhere on the Telecommunication Company of Iran's network, between devices with the addresses of *78.38.255.100* and *10.10.53.209* (Iran's international gateway on a private network address). These rules cover any request on the secure web port for the entirety of Facebook's *173.252.96.0/19* block of addresses, but only a limited portion of Twitter's network. Addresses associated with Balatarin also appear to be blocked, taking down HTTPS access to Google's PageSpeed network, which is used by many more sites than just Balatarin to protect against denial of service attacks.

TRACEROUTE FOR TWITTER WEB SERVER (HTTPS)	**TRACEROUTE FOR AN ADDRESS IN SAME NETWORK**
Tracing 199.16.156.6 on TCP port 443, 30 hops max **1** [hop-1] 0.761 ms **2** [hop-2] 0.560 ms **3** [hop-3] 4.163 ms **4** 78.154.32.177 3.591 ms **(TCI)** **5** 78.38.255.100 1.972 ms **6** * * * **7** * * * ... **26** * * * **27** * * * **28** * * * **29** * * * **30** * * * Destination not reached	Tracing 199.16.155.4 on TCP port 443 , 30 hops max **1** [hop-1] 0.636 ms **2** [hop-2] 22.000 ms **3** [hop-3] 2.963 ms **4** 78.154.32.177 2.873 ms **5** 78.38.255.100 1.984 ms **6** 10.10.53.209 2.261 ms **7** 213.155.129.33 201.030 ms **(INTERNATIONAL)** ... **17** 38.113.166.18 265.772 ms **18** 76.74.210.109 280.205 ms **19** 199.16.155.4 276.617 ms **(TWITTER)**

Embedded in the filtered page response is information on why the blocking occurred, including whether the trigger was a specific word or the site itself. One of these debugging settings, named 'policy,' is seemingly always set to 'MainPolicy.' Currently, the unusual filtered site response returned has 'policy' set to 'dns-blockty.' Additionally, whereas we had previously estimated that only a few of the most sensitive and difficult to block sites had been subject to DNS manipulation, following the change nearly half of Alexa's 100 most popular sites were intercepted. This parallels previous measurements of web content filtering, suggesting that the same device and blacklist is being used for both methods of blocking. It is possible that the network administration simply duplicated this blacklist setting, and unintentionally applied the web-filtering configuration where it was not appropriate, resulting in the failure. Regardless of intent, this change represents the largest shift in Iran's filtering strategy in the past few years.

Internet traffic maintains a counter indicating the number of routers it has traversed before it reached its destination. That the counters for both the Web Content Filter and DNS Interception traffic match supports the theory that they are in fact the same device. Both of these approaches also suffer from a high degree of failure in detecting attempts to access blocked sites that deviate even slightly from the standard formatting. For example, if a web request to filtered content is preceded with an unnecessary space, it will go through undetected. Similarly, if a DNS request has anything other than the most common flags set (such as 'No Recursion'), it will also skip the filter. Again, the role of censorship equipment is to interfere with the average user, not the most motivated, but these idiosyncrasies show that the apparatus and software at the core of the apparatus is surprisingly unsophisticated and lazily implemented.

CONTENT FILTER RESPONSE FROM DNS QUERY	TCI DNS DNS QUERY (217.218.155.155) FOR FACEBOOK
HTTP/1.1 403 Forbidden Connection:close <html><head><meta http-equiv="Content-Type" content="text/html; charset=windows-1256"><title>M6-5 </title></head><body><iframe src="http://10.10.34.34?type=Invalid Site&policy=**dns-blockty**) " style="width: 100%; height: 100%" scrolling="no" marginwidth="0" marginheight="0" frameborder="0" vspace="0" hspace="0"></iframe></body></html>	;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2 ;; QUESTION SECTION: ;facebook.com. IN A ;; ANSWER SECTION: facebook.com. 724 IN A 173.252.110.27 ;; AUTHORITY SECTION: facebook.com. 28163 IN NS a.ns.facebook.com. facebook.com. 28163 IN NS b.ns.facebook.com. ;; ADDITIONAL SECTION: a.ns.facebook.com. 129483 IN A 69.171.239.12 b.ns.facebook.com. 90143 IN A 69.171.255.12

The state-affiliated Tasnim News Agency and Islamic Republic of Iran Broadcasting have informed the public that the brief period of unblocked access to Facebook was due to a new range of Internet addresses for the site. If this were the case, it would account for why direct requests were not blocked. However, data obtained from the Domain Tools service shows that the address returned for facebook.com at the time, *173.252.110.27*, had been in use since atleast the start of this year. Furthermore, this would not account for the simultaneous availability of Twitter, Balatarin and other SSL-enabled services. Nor would a change of addresses used by Facebook matter if the DNS interception was working correctly. Finally, we note that these openings occurred in the evening, in Iranian time; in the experience of the authors, this is the time at which changes are most frequently made in any network infrastructure, including that of the Iranian Filternet.

English العربية

درباره ما ارتباط با ما

Tasnim News Agency

خبرگزاری تسنیم

صفحه اصلی | عناوین اخبار | سیاسی | بین الملل | پیداری اسلامی | فرهنگی | اقتصادی | ورزشی | اجتماعی | عکس | صوت و فیلم | سایر رسانه ها | استانها

Friday, 20 September 2013

گزیده ای از اخبار : ژاپن ۲ راکتور خود در فوکوشیما را تخریب می‌کند

صفحه اصلی > اقتصادی

سرویس: اقتصادی ، تاریخ: ۲۶/شهریور/۱۳۹۲ - ۱۵:۴۸ ، شناسه خبر: ۱۴۳۸۴۹

تصاویر مرتبط

برگزیده سایت

- فراخوان طرفداران مرسی برای برگزاری تظاهرات فردا در مصر
- دولت از همه فرصت‌های بین‌المللی برای حل مشکلات مردم استفاده کند
- هرگونه دخالت خارجی در سوریه بدون موافقت شورای امنیت "جنایت‌آمیز" است
- برتری گسترش فولاد مقابل ذوب‌آهن
- ولادیمیر پوتین: توسعه روابط با هم‌سایگان اولویت مسکو در قرن ۲۱/ اسلام بخش جدانشدنی هویت ملی روسیه است

برگزیده سرویس

- تداوم رکود خرید و فروش دلار و سکه/ دلار۳۰۷۰، سکه ۹۷۰ هزار تومان
- تسریع ترخیص کالاهای اساسی در نیمه دوم امسال با لغو تحریم‌های کشتیرانی
- سرقت ۲۱ میلیارد دلاری از طریق اینترنت در سال ۲۰۱۲/ هر ۳ ثانیه یک نفر گول خورد
- بهره‌برداری از راه‌آهن قزوین-رشت در سال ۹۳/ ۸۰۰۰ میلیارد ریال برای تکمیل پروژه نیاز است
- شاخص به چند قدمی کانال ۶۱ هزار واحد رسید

تسنیم منتشر کرد

دلیل رفع فیلتر موقت فیس‌بوک مشخص شد

خبرگزاری تسنیم: فیس‌بوک با در دست قرار دادن رنج جدیدی از آی‌پی‌ها توانست شرکت‌های اینترنتی ایران را غافل‌گیر و صفحه خود را برای ایرانی‌ها باز کند هرچند که تمامی این رنج هم‌اکنون مسدود شده است.

نسخه قابل چاپ

به گزارش خبرنگار فناوری اطلاعات و ارتباطات خبرگزاری تسنیم، رفع فیلتر موقت فیس‌بوک و متحیر شدن عده‌ای از کاربران ایرانی از چنین رویدادی منجر به شکل گرفتن موجی رسانه‌ای در ارتباط با این موضوع شد.

بعضا رسانه‌هایی این اقدام را پسندیده اعلام کرده بودند و در مدح و ستایش مسئولان برآمدند و در مقابل عده دیگری بودند که این رویه را چندان شایسته ارزیابی نکردند و در مقابل کسانی هم بودند که با رأیی ممتنع خواستار اعلام رسمی این موضوع شدند.

اما بررسی های خبرنگار تسنیم حاکی از آن است علت اصلی چنین موضوعی که غافل‌گیری شرکت‌های ارائه دهنده خدمات اینترنت را به همراه داشت، ابتکار فیس‌بوک بود.

این شرکت رنج جدیدی از آی‌پی‌ها (IP) را برای خود تعریف کرده که آدرس آن‌ها در بانک‌های آدرس‌های شرکت‌های ارائه دهنده خدمات اینترنت نبوده است و همین موضوع منجر به این شده که برخی شرکت های اینترنتی به صورت کاملا اتفاقی به این آدرس‌ها سرک بکشند و فیس‌بوک را قابل رویت سازند.

به گفته یک مقام مطلع در زیرساخت، این اقدام جدید منجر به این شد که در برابر تقاضای کاربران برای باز کردن صفحه فیس‌بوک، برخی مسیریاب‌ها به سمت مقصدهای جدید (آدرس‌های آی‌پی جدید) رهنمون شوند و فیس‌بوک را همچون سایر سایت‌ها به نمایش بگذارند.

البته دلیل اینکه این سایت برای تمامی کاربران شرکت های اینترنتی در شب گذشته قابل رویت نبود، این بوده که بسیاری از شرکت‌ها همچنان در برابر تقاضای باز کردن صفحه فیس‌بوک به همان رنج سابق آی‌پی‌ها مراجعه کرده‌اند و با فیلتر روبرو شده‌اند.

اما به گفته این منبع مطلع، از صبح بامداد امروز تمامی رنج‌های جدید به شرکت‌ها اطلاع‌رسانی شده و لیست سایت‌های فیلتر شده به روزرسانی شده است تا چنین مشکلی رفع شود.

با این حال کمیته مصادیق محتوای مجرمانه قطعا بعد از بررسی گزارش شرکت ارتباطات زیرساخت حول این موضوع که امروز به این کمیته ارسال شده، نظری جامع و رسمی‌تر درباره این موضوع ارائه خواهد داد.

انتهای پیام/

© Tasnim News Agency. All rights reserved.

FACEBOOK INTERNET ADDRESSES			
2013-01-03	Change	66.220.152.40	69.171.228.24
2013-01-16	Change	69.171.228.24	173.252.110.27
2013-02-06	Change	173.252.110.27	66.220.152.19
2013-02-17	Change	66.220.152.19	173.252.110.27
2013-02-28	Change	173.252.110.27	66.220.152.19
2013-03-22	Change	66.220.152.19	173.252.100.27
2013-04-03	Change	173.252.100.27	69.171.247.29
2013-04-14	Change	69.171.247.29	173.252.100.27
2013-04-26	Change	173.252.100.27	173.252.73.52
2013-05-20	Change	173.252.73.52	66.220.152.19
2013-05-31	Change	66.220.152.19	69.171.247.29
2013-06-12	Change	69.171.247.29	69.171.237.20
2013-06-24	Change	69.171.237.20	173.252.110.27
2013-07-06	Change	173.252.110.27	66.220.152.19
2013-07-19	Change	66.220.152.19	69.171.247.29
2013-07-31	Change	69.171.247.29	173.252.100.27
2013-08-12	Change	173.252.100.27	66.220.152.19
2013-09-06	Change	66.220.152.19	69.171.247.29

CONTENT FILTERING AND BLOCKED SITES

AUGUST 3:
The term "Come to eat (بیا بخورش)" was blocked by Irancell. When a user sends a SMS containing this term, it will not be delivered. 'Come to eat' is an everyday phrase in the Persian language, though it also has sexual connotations when used in a colloquial sense, roughly translating as 'suck it'. (Source)

AUGUST 8:
International Federation of Volleyball (FIVB) was blocked, creating numerous problems for the Iran Federation of Volleyball, as local teams were subsequently unable to register their players on the website. The site was made available after a few hours, authorities reporting that a number of images of women's volleyball on the FIVB website were the reason for the imposition of the block. (Source1, Source2)

AUGUST 15:
A block was imposed upon Blogfa for several hours, then lifted without further explanation. Blogfa founder, Alireza Shirazi, said in an interview with Fars News that the reason for the block was not clear to him, and that the website was unblocked before Blogfa could send its request to the Commission to Determine the Instances of Criminal Content (CDICC). (Source)

AUGUST 17:
A blogger selling illegal movies on his blog was arrested by the Iran Cyber Police (Golestan Province branch). (Source)

AUGUST 18:
A woman who published "pornographic" images on the Internet was arrested by the Iran Cyber Police (South Khorasan Province branch). (Source)

AUGUST 19:
The Mahmoud Ahmadinejad Wikipedia page was blocked a few days after the end of his presidential term. The CDICC claimed that the page contained misinformation and insulting words relating to the former president. (Source)

AUGUST 20:
Va Islamah, a website that focused on discussing and resolving issues facing Sunni Muslims, was blocked. (Source) In addition, Wikipedia Farsi was blocked for several hours and then made available without any explanation. (Source)

AUGUST 28:
Rouhani Meter was blocked by Iranian authorities. Rouhani Meter is a website that has been monitoring the performance of President Rouhani over the first 100 days of his administration. This website was inspired by the Egyptian site, Morsi Meter. (Source) Additionally, Shahrdare Ma (Our Mayor) was blocked without explanation when the website sought to gauge public opinion concerning the performance of Mohammad Bagher Ghalibaf (Mayor of Tehran), and the question of who should be his successor. After the website was filtered, it was completely shut down and the account was suspended. (Source)

AUGUST 28:
The admin of a blog that taught visitors how to create bombs and explosive materials was arrested by Iran's Cyber Police (Ardebil Province branch). (Source)

STATEMENTS FROM MINISTRIES AND POLITICIANS

JULY 30:
Morteza Barari, the Deputy Minister of Information and Communication Technology (ICT), announced that Iran does not have any plans to monitor emails, stating that such measures would be against Islam and sharia. (Source)

AUGUST 2:
Hossein Nami, in his last interview as Minister of ICT claimed that 64% of Internet usage by Iranian users concern scientific subjects, 30% relate to business and other topics, with only 6% using it for illegal and 'unprofessional' purposes. (Source)

AUGUST 6:
Mahmood Vaezi, the Rouhani administration's newly-appointed Minister of ICT, published a plan outlining the future of the Ministry. Vaezi made a series of commitments to: (Source)

- Increase international Internet bandwidth;
- Increase local IP (internal network) bandwidth;
- Regularly update postcodes;
- Increase the number of Internet users;
- Design, build, test, operate, launch and control the satellites that Iran will utilise for purposes of communication;
- Guarantee high-speed access to the National Information Network (SHOMA - commonly known as the 'National Internet') for governmental organisations, businesses and families;
- Increase the number of mobile phone users;
- Ensure Internet access for all villages, in fulfilment of the Universal Service Obligation (USO)

AUGUST 8:

According to a report released by the Minister of ICT, Mahmood Vaezi, the current Internet penetration rate sits at 43%, with 30 million Internet users in total. In addition, the report determines that there are 4.1 million high-speed internet access ports in operation in Iran. This contradicts a June 2013 report by the National Internet Development Management Center (MATMA), which put the Internet penetration rate at 61.06%. A number of other statistics from Vaezi's report are listed below: (Source)

Number of landline users	27.5 million
Landline penetration rate	35%
Number of mobile phone users	60 million
Mobile phone penetration rate	79%
Number of Internet users	30 million
Internet penetration	43%
Number of high speed Internet ports	4.1 million
Local bandwidth	530 Gbps
International bandwidth	71.7 Gbps
Number of postal parcels sent in 1391 (2012/13)	842 million
Postal parcels sent, per capita	11.2
Length of fiber optic system	50,226 km
Fiber optic capacity	362,000 E1
International transit capacity	102 STM1
Number of villages with communications access	52,704
Mobile coverage (include roads, highways, etc.)	Main road: 91% Country lane: 92.8% Railway: 94.12%
Number of rural ICT offices	9,854
Number of saving accounts at the Post Bank of Iran, per 1000 people	95.9

AUGUST 15:

Mahmood Vaezi received a vote of confidence from Iran's Parliament, 218 votes to 45. Vaezi was born on September 13 1952. He has PhD in International Relations and an MSc in Electronic Engineering. He was:

- 1980 - 1987: Director of the Telecommunication Company of Iran (TCI)
- 1987 - 1988: Advisor to the Foreign Minister, Ali Akbar Velayati
- 1988 - 1990: First Deputy Minister of Post and Tele communication
- 1990 - 1998: Deputy Foreign Minister in Europe and American Countries' Affairs
- 1998 - 2000: Economic Deputy of Foreign Minister

He is the Deputy of Foreign Policy at the Center For Strategic Research, where Rouhani had served before his election, a visiting professor at Allameh Tabatabaei University. (Source)

AUGUST 17:

Vaezi announced that the primary objective of the Ministry of ICT shall be to increase Internet speeds and bandwidth (Source). In addition, the Minister published a brief description of SHOMA. The central points from this statement are listed below: (Source)

- SHOMA is a network based on the Internet, making use of switches, routers and data centers. If users request data that is located on a data center inside the country, their traffic will never leave the country, staying inside the network.
- SHOMA is intended to create a private and secure internal network.
- SHOMA is an aggregation of exclusive, local and national networks. It consists of two parts: exclusive and public. The 'exclusive' component will be used for communication and will transfer data between government organisations, state institutions, and the like. Meanwhile, the public component will offer services to standard users.
- SHOMA is not in competition with the Internet. Iran is not cutting Iranian users' access to the 'global' Internet. If the user cannot find the data that they want, then they will be able to access the Internet to search for it, instead.
- The user will be able to make use of high-speed, low-cost connections for data accessed on SHOMA, as well as a number of major foreign websites, such as Google and Yahoo.

AUGUST 31:

Mahmood Vaezi stated that the minister is formulating a new scheme for Internet filtering, also indicating that the cost of Internet access will decrease moderately. (Source)

STATEMENTS FROM CIVIL SOCIETY AND PROFESSIONAL ORGANISATIONS

JULY 31:
Lotfollah Sabohi, Deputy of the Communications Regulatory Authority of Iran (CRA), announced that the CRA will not issue new ISP permits until existing ISPs are properly organised. According to Sabohi, 773 companies have been granted ISP permits, with around 200 of them holding more than one permit, and 142 ISP permits having been granted for Tehran alone. (Source)

AUGUST 2:
Hassan Alizadeh, head of the Information Technology and Digital Media Development Center at the Ministry of Culture, said that 13,147 complaints were lodged concerning SMS advertisements. 11,500 complaints were considered by the Ministry, of which 8,590 were accepted. The main topics of advertising SMS that received complaints were: (Source)

TOPIC	NUMBER OF SMS
Real Estate	700
Holiday Tours	420
Fortune-telling	320
Medical	300
Religious	210

AUGUST 3:
Colonel Koreh Balaghi, the Chief of Iran's Cyber Police (FATA) for West Azerbaijan Province, said the Cyber Police does not have a role in the process of Internet censorship, referring the issue to the Iranian judiciary system. Also in this report, Colonel Balaghi states that he believes social networking sites like Facebook have been launched for the purpose of surveillance, and states that Iranians should not join them. (Source)

AUGUST 5:
The official website of Mehdi Karoubi - a leader of the Green Movement - has been suspended by its host. An email sent to the site's administrator stated that the server cannot host the .ir domain due to ongoing US sanctions against Iran. (Source)

AUGUST 6:
Mehrabad Airport at Tehran has unveiled free wireless Internet access for its passengers. Users must submit their name and mobile number to make use of the service. (Source)

AUGUST 14:
Colonel Masood Zahedian, head of the 'Moral Security Division' of Iran's police force, announced that the police has been monitoring the entirety of satellite television broadcasting into Iran, and has cut 6,200 phone lines in the last three years due to connections with satellite television. He also reiterated the illegality of Iran-based companies engaging in advertising on banned satellite channels. (Source)

AUGUST 18:
A list of provinces hosting the most malware-ridden sites in June/July 2013 was published: (Source)

PROVINCE	NUMBER OF SITES THAT SENT MALWARE
Tehran	32
Lorestan	16
East Azerbaijan	15
Fars	7
Qazvin	6
Kerman	5

AUGUST 19:
The official website of Ayatollah Ali Akbar Hashemi Rafsanjani published a banner reading: "Facebook is a good phenomenon", linking it to a speech of his, in which he stated that: "Today, a Facebook page that has no cost to create can be the subject of television stations and news agencies around the world." As Small Media mentioned in previous reports, it is rumoured that President Hassan Rouhani will remove filtering of social networks such as Facebook. (Source)

AUGUST 23:
Iran's Cyber Police suggested to the Ministry of Youth Affairs and Sports that a Iran-appropriate dating website should be launched. (Source)

AUGUST 24:
Mashregh News, a website closely aligned with the Iranian Revolutionary Guard Corps (IRGC), published an article strongly criticising the online availability of a Persian-language version of the Saudi-backed Asharq Al Awsat newspaper in Iran. Abdolsamad Khoramabadi, the head of CDICC, responded to the article stating that CDICC will block the website shortly. The site was subsequently blocked. (Source)

AUGUST 27:
According to research undertaken by Tahlilgar, just six of the 500 most popular websites in Iran (around 1%) are religious websites. One of these websites is a forum, and the others are websites that have received government backing. (Source)

AUGUST 27:
Raja News, a news site affiliated with Ahmadinejad, was down for an extended period. From accessible records, it appears that the site has been unable to maintain a stable host, switching between iWeb Technologies, a host on the Iranian provider Afranet, and now Hetzner.

AUGUST 31:
Users reported that the Freegate anti-filtering tool began intercepting requests for Facebook and redirecting traffic to site without encryption or notification. (Source)

NETWORK ANALYSIS

	PISHGAMAN	DCI ADSL	SHATEL	MOBINNET	ASIATECH
L2TP(IPSec)	Could Not Connect	Down: 31 kB/s Up: 24 kB/s		Connects, No Traffic	
Psiphon					
Tor	Down: 21 kB/s Up: 8 kB/s	Down: 12 kB/s Up: 6 kB/s	Down: 194 kB/s Up: 29 kB/s	Down: 90 kB/s Up: 7 kB/s	
Hotspot Shield		Connects, Frequently Discon-nects	Down: 198 kB/s Up: 19 kB/s	Down: 102 kB/s Up: 26 kB/s	

TCI DSL SERVICE	DADEH GOSTAR ASR NOVIN (DGA)
We detected the presence of an in-network transparent HTTP cache that caches data which was directly requested by the client. 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. Weakly cacheable 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. Strongly cacheable 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. Your host, NAT, or firewall acts as a DNS server or proxy. Requests sent to this server are eventually processed by X.X.X.X.	Changes to headers or contents sent between the client and our HTTP server show the presence of an otherwise unadvertised HTTP proxy. 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 1452 bytes of payload. The client was able to receive fragmented UDP traffic. The following headers had their capitalization modified by the proxy: Content-Type: text/html Content-Length: 770 Last-Modified: Thu 07 Aug 2013 14:41:02 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 either the headers the client sent or the HTTP response from the server. We have captured the changes for further analysis. The detected HTTP proxy changed images that were sent from our server. 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. A DNS proxy or firewall caused the client's direct DNS request to arrive from another IP address. Instead of your IP address, the request came from X.X.X.X.A DNS proxy or firewall generated a new request rather than passing the client's request unmodified.

MOBINNET	PISHGAMAN
You are listed on the following Spamhaus blacklists: XBL PBL 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. A DNS proxy or firewall caused the client's direct DNS request to arrive from another IP address. Instead of your IP address, the request came from X.X.X.X. A DNS proxy or firewall generated a new request rather than passing the client's request unmodified. Direct UDP access to remote SIP servers (port 5060) is blocked	

IRANCELL	
Direct TCP access to remote SMTP servers (port 25) is prohibited. This means you cannot send email via SMTP to arbitrary mail servers. Such blocking is a common countermeasure against malware abusing infected machines for generating spam. Your ISP likely provides a specific mail server that is permitted. Also, webmail services remain unaffected Direct TCP access to remote SIP servers (port 5060) is blocked. Direct TCP access to remote PPTP Control servers (port 1723) is blocked. Direct TCP access to remote DNS servers (port 53) is blocked. The network you are using appears to enforce the use of a local DNS resolver.	