SMALL MEDIA

IRANIAN INTERNET INFRASTRUCTURE AND POLICY REPORT

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

INTRODUCTION

// When we began work on the Internet Infrastructure and Policy Report series late last year, our ambition was to document the rich technical and political complexities of Iran's communications environment, which are often missed due to language, nuance and diffusion of sources. Although public reports often focus on the battles between the censors and Facebook, or the Cyber Army and reformist sites, these narratives often pass over the meaningful role of administrative entities, conservative factions and private individuals in the complex polity and security of the domestic network. We believed then that we can better predict the future when the motivations of these actors are better understood. There is no better affirmation of this than the timing of the February edition of this series, were we noted,

> "When Supreme Council of Cyberspace promotes new policies on the registration of VPNs, we can expect that unregistered VPN connection will be blocked and throttled."

Released on March 8, within hours Iranian Internet users began to report that outbound VPN connections and other anti-filter tools were no longer working. After several years of discouraging public use of circumvention tools and direct threats of blocking, including brief periods of actual disruption, it appears that to the agencies administering Iran's censorship policies the balance between control and development no longer favors the free flow of information over the Internet. Whereas services such as Skype, which provided at least the appearance of privacy, made surveillance of communications more difficult, it was saved by its essential use by businesses and the substantial demographic of Iranians with family members outside of the country. Whether from a confidence in the ability of the state to control networks, reflected in the recurrent promises of "smart filtering," or the urgency of coming elections, those pathways not immediately subject to control or surveillance have been increasingly subject to disruption or outright blocking.

This narrative, while startling in itself, is incomplete. Filtering has limits and costs that do not favor states with populations as technologically-savvy as that of Iran, provoking other forms of surveillance or interference. This month brought the quiet return of phishing and malware against individuals inside and outside of the country. Masquerading as satire or tools, these attacks bring light to a private hacking community that has matured in recent years, and whose motivations are unclear. As users seek alternative ways to bypass filtering and communicate online, they are more in need of dedicated and appropriate resources that will help them make more sophisticated decisions about their security and privacy against such threats.

POLICY DEVELOPMENTS

CONTENT FILTERING AND BLOCKED SITES

- **FEBRUARY 3:** Tabnak is unblocked, a week after the site was taken down under the authority of the Prosecutor General of Tehran on January 27. (Source)

- **FEBRUARY 3:** Viber is blocked without any explanation, this restriction appears to have been lifted with a few days of implementation.

- **FEBRUARY 13:** Voice of Russia Persian (persian.ruvr.ru) is blocked. The website reacted to the blocking, claiming that such an action might affect the relationship between Russia and Iran. The site is unblocked two weeks later without any explanation for the filtering. (Source)

- **FEBRUARY 19**: Two pro-Ahmadinejad blogs, Hamsazi and Khatkhaty, are blocked due to publishing a critical post about the Supreme Leader. (Source)

- **FEBRUARY 21:** Baztab Emrooz is blocked for the third time in the year. Its director announced on his Facebook profile that the court ordered the blocking, while disputing the evidence for the decision. (Source)

- **FEBRUARY 24:** WhatsApp and Viber are blocked.

- **MARCH 4:** VPN.ir is filtered for around 30 minutes. (Source)

- **MARCH 6:** All VPNs are blocked without any explanation from the Iranian authorities. (Source)

- **MARCH 17:** 1900 websites were blocked by the Iran's Police of Alborz province. These web sites were active in scamming, illegal drugs, satellite instruments, etc. 10 Internet cafés were closed as well. (Source)

- **MARCH:** Secure access to Wikipedia (HTTPS/SSL) appears to have been blocked. At least one thousand Persian-language Wikipedia pages are blocked at the central gateway, not including articles in other languages or ISP-level rules. By browsing Wikipedia over SSL, users could previously bypass this filtering, since the encryption prevents intermediaries from monitoring the connection.

STATEMENTS FROM MINISTRIES

- **FEBRUARY:** The FETA Cyberpolice of Fars announced that it was the most active regional agency, pursuring 314 cases of cybercrimes, including: 208 instances of the theft of bank account information, 7 of harassment and 6 selling contraband items. (Source)

- **FEBRUARY 3:** Mehdi Akhavan Behabadi, Secretary of the Supreme Council of Cyberspace (SCC), while promoting the forthcoming intelligent filtering system stated that less than 10% of online population have used circumvention tools, and that the majority of the use of such tools is to access pornography. Behabadi also stated that the long term answer to public demand for foreign-based social networks is to improve domestic platforms. (Source)

- **FEBRUARY 5:** In another interview, with Khabar Online, Behabadi announced:
  - Facebook will remain blocked in the short-term.
  - The filtering mechanism will change from URL filtering to content filtering, blocking specific users and text online, rather than whole pages or sites, which the SCC believes will mitigate the public frustration over the extent and execution of filtering. The first phase of content-based blocking will be deployed within the next three months (May/June).
  - The Commission to Determine the Instances of Criminal Content (CDICC) does not have any role in the actual implementation of Internet censorship. The CDICC can only identify the types of online content that violate the law, with the Ministry of Information and Communications Technology having the ultimate responsibility for implementation.
  - The SCC has suggested that the judicial system create a Special Filtering Court for remediating issues related to censorship.
  - The SCC wants to block all illegal VPNs, in part to force websites move their servers inside Iran. Behabadi claimed that the loading speed of websites inside Iran will be "10 times faster" than the websites hosted outside. (Source)

- **FEBRUARY 6:** Abdolsamad Khoramabadi, head of CDICC, announced a list of cyber crimes pertaining to the June Presidential election. Included in the list are:
  - Encouraging the public to boycott the elections,
  - Publishing fake results of surveys and polling,
  - Publishing content that mocks the elections or candidates (Source)

- **FEBRUARY 6:** Registered entities can request approval as a legal VPN by registering on VPN.ir. According to the 'Terms & Condition' on the site, the registration of foreign VPNs is for the secure data transmission of network traffic over the public Internet network platform as part of the business of large organizations. The SCC has limited registration to businesses, companies and universities. A legal VPN is not a tool to

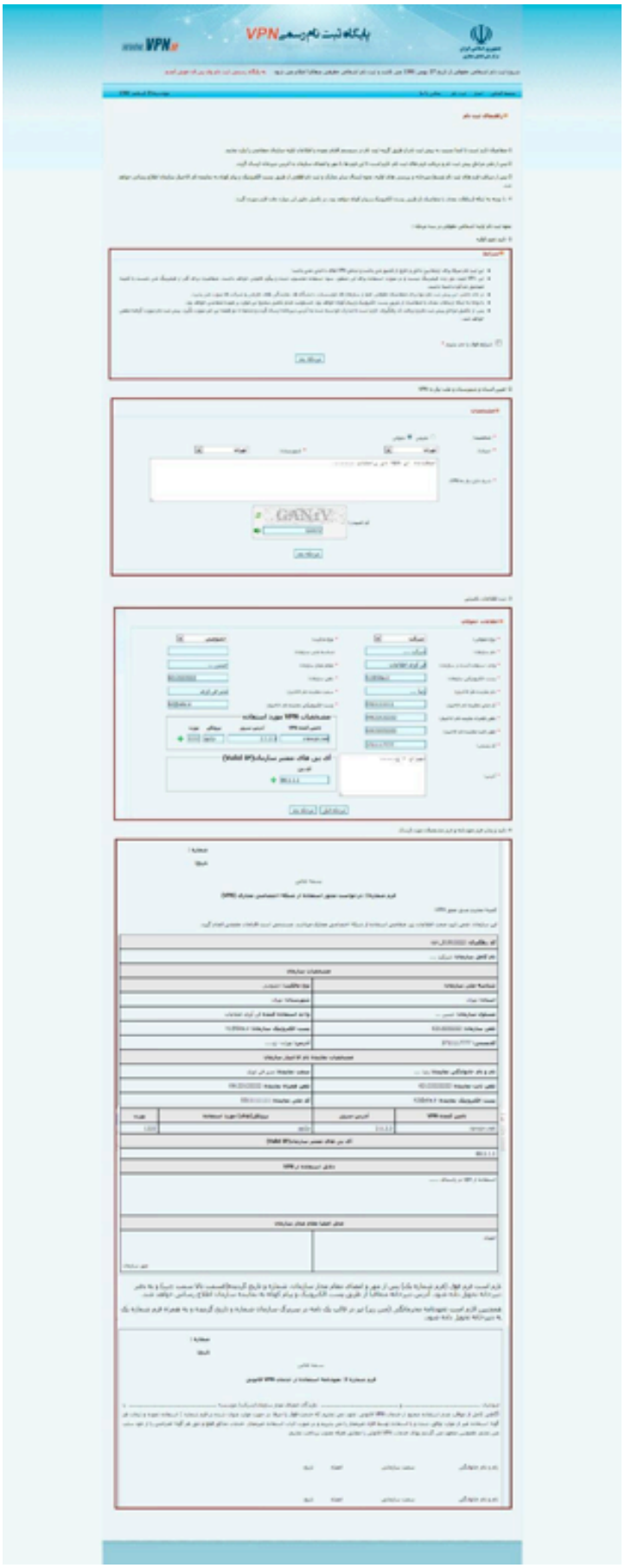
bypass the filtering system, and if the user wants to use it as a circumvention tool, they must contact the CCDIC. VPN.ir, as noted previously, is only accessible within Iran, due to it being located on the country's internal network. (Source: 1, 2)

- **FEBRUARY 27:** In an interview with the Donyaye Eghtesad newspaper, Reza Bagheri Asl, Director of the New Technologies Department at Majlis Research Center, claimed that one of the purposes of legal VPNs is to enable Iranians to bypass the geolocation restrictions of certain services imposed due to international sanctions. In his example, the users of official VPNs may access international banks and transfer money outside of the country securely. According to the interview, Bagheri Asl stated that the government has the technical ability to block all illegal VPNs without any problems, and that legal VPNs cannot be used to circumvent filtering. (Source)

- **MARCH 13:** Mohammad Hossein Nami, head of the Ministry of Information and Communications Technology, stated that President Mahmoud Ahmadinejad gave a special order to the ministry to investigate the VPN situation in Iran. (Source)

- **MARCH 17:** In an interview with IRNA, a prominent, conservative member of the parliament, Ali Motahari, noted, in reference to the recent filtering of high profile sites, that the filtering committee (CDICC) can only order the blocking of weblogs, not websites or news agencies, which are overseen by the Press Supervisory Board. (Source)

- **MARCH 20:** Behabadi states that "national Internet" is not the right name for the government's network infrastructure projects, asserting that 'localised Internet' is more appropriate, as Iran will produce something inside the country and use it. He also added that there are no plans to lift the administrative restrictions limiting connection speeds to 128kbps for home users. (Source)


پایگاه ثبت نام رسمی VPN

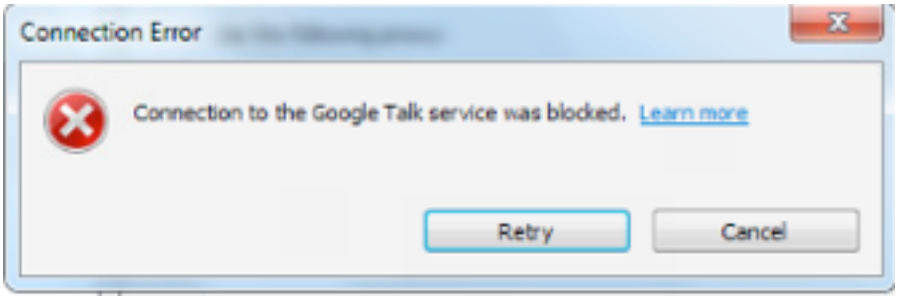
CIVIL SOCIETY, PROFESSIONAL ORGANIZATION STATEMENTS

- **FEBRUARY 6:** According to Weblognews, a prominent conservative blog on Persian cyberspace, the filtering method for domestically hosted sites has changed, and in some cases the CDICC has directly ordered companies to remove content from sites without any notification to the owner. The report notes that one of its own posts that criticised Internet censorship was deleted by the host company under the CDICC order. (Source)

TECHNICAL DEVELOPMENTS

VOICE OVER IP SERVICES BLOCKED

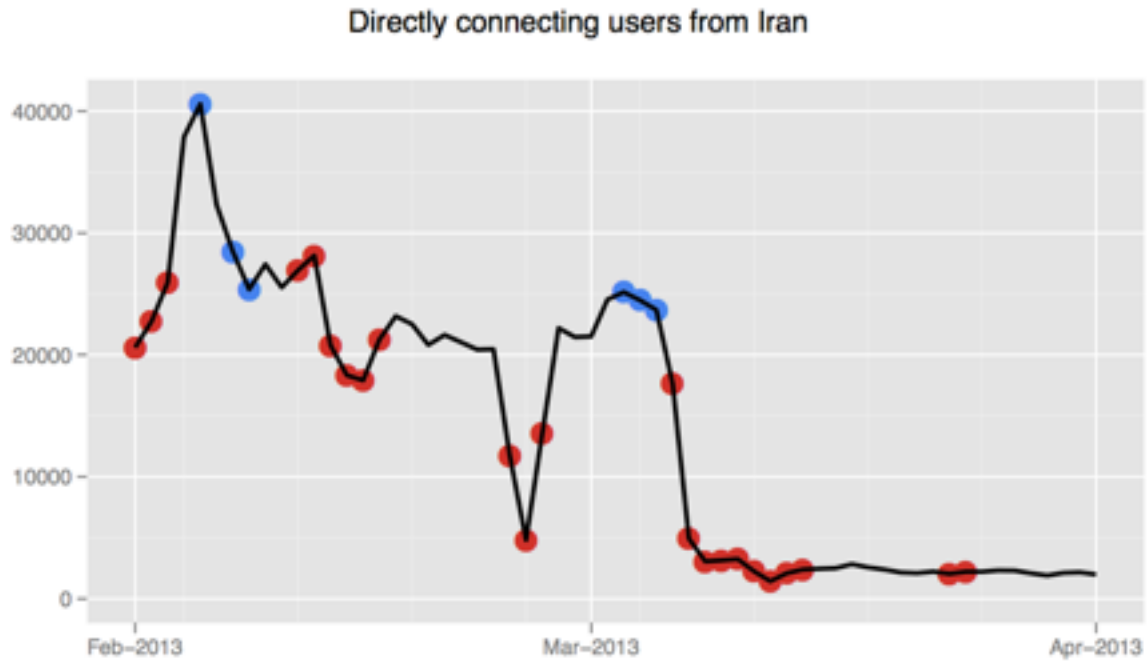
Following February's restrictions on mobile chat applications, in March, users on several ISPs, including Datak, Parsonline, Mobinnet and Shatel, began to report that Skype and the desktop version of Google Talk were no longer able to connect. One user was able to confirm the blocking of Skype with Datak's technical support and a search of social media on the issue returns multiple complaints of disruption, beginning in early March and as recent as early April. (Source)



VPN AND ANTI-FILTERING TOOLS BLOCKED

Beginning March 6, Iranian Internet users began to report difficulties connecting to the VPN networks that constitute a significant share of anti-filtering services. On a preliminary evaluation of the data of a significant VPN provider, it appears that a component of this blocking was implemented by individual Internet services due to the differences of timing and scale of the decline traffic from different networks. Additionally, some networks appear to have not fully blocked the range of available protocols or implementations of VPNs, creating confusion about the extent of the change. It appears generally that the most common two protocols, PPTP and L2TP have been targeted. This is made easier to implement due to their generally relying on a fixed port, however, in tests it appeared that attempts to connect to a widely known VPN service was being terminated based on the authentication handshake, rather than simple port blocking. This utilization of deep packet inspection on traffic behavior in order to block connections mirrors the method currently used to disrupt connections to the Tor anonymity network. (Source)

These incongruencies also shed further evidence to Iran imposing a two level censorship regime, with some measure of filtering occurring on the ISP level, while the TCI implements its own set of controls.



The shift to different tools appears to largely followed word of mouth advice through email and social networks, with FreeGate, Socksifier and Psiphon gaining popularity. However, due to throttling of specific protocols, and potentially all traffic, most anti-filtering tools appear to be slow and unreliable. Additionally, as we describe in the next section, these methods of education on tools suffer from an issue of trust. Legitimate anti-filtering software has previously been tainted with malware and redistributed on filesharing sites. (Source)

راهنمایی	DropBox	Share 4	Mega	Google Drive	Version	File
اینجا	دریافت	دریافت	دریافت	دریافت	2.88	Hot Spot Shield
اینجا	دریافت	دریافت	دریافت	دریافت		Spot Flux
اینجا	دریافت	دریافت	دریافت	دریافت	3	Psiphon
اینجا	دریافت	دریافت	دریافت	دریافت		Security Kiss
اینجا	دریافت	دریافت	دریافت	دریافت	232	Expat Shield
اینجا	دریافت	دریافت	دریافت	دریافت		Cyber Ghost
اینجا	دریافت	دریافت	دریافت	دریافت	1.0.38	Tunnel Bear
اینجا	دریافت	دریافت	دریافت	دریافت	1210	Ultrasurf
اینجا	دریافت	دریافت	دریافت	دریافت		VPNium
اینجا	دریافت	دریافت	دریافت	دریافت	20130315	YourFreedom
اینجا	دریافت	دریافت	دریافت	دریافت	2.3.25-5	Tor
اینجا	دریافت	دریافت	دریافت	دریافت	0.2.3.25	Vidalia - Tor
اینجا	دریافت	دریافت	دریافت	دریافت	a 2.4.11	OBFS Proxy - Tor
اینجا	دریافت	دریافت	دریافت	دریافت	4.1.9	Gpass

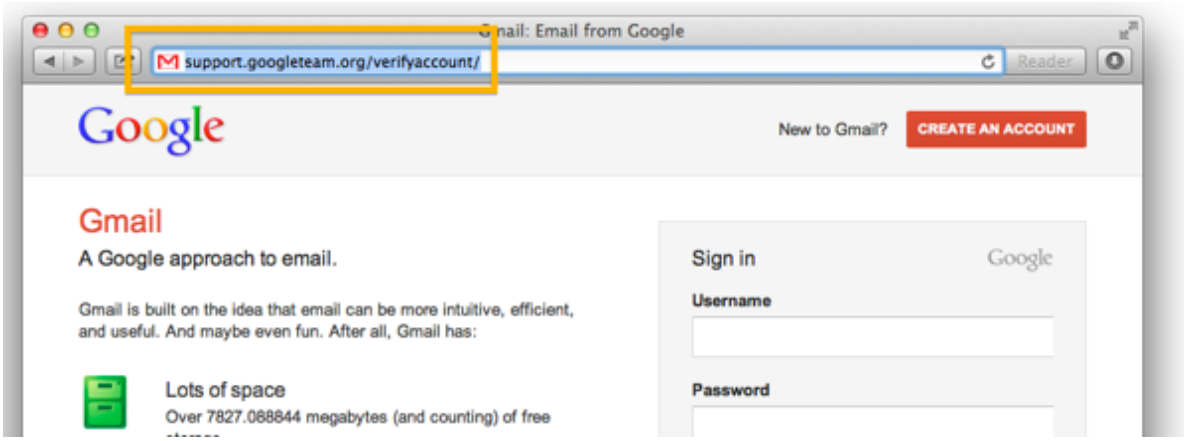
MALWARE AND PHISHING

Within the past several weeks, diaspora civil society activists, journalists and students have been the target of attempts to obtain account credential and propagate malware, with the source directly originating from networks in Iran. In order to trick the victim, the messages and file names of the attacks appeared to celebrate Nowruz, contain software to bypass Internet filtering, or satire the political establishment. In one case, malware was sent to former Broadcasting Board of Governors staff, posing content from an opposition news site and uploaded to fake site hosted on compromised servers based in California and the United Kingdom. While the user would appear to have opened an image, the malware would make a query for the address of the state news broadcaster, IRIB, notify an unrelated server of the success compromise, and upload the victim's password database for Mozilla Firefox. This malware had appeared to have compromised about 30 hosts at the time of publication.

In another case, a phishing attempt was sent to civil society activists, site posing as a warning that the user's account was going to be shut down. Although these types of schemes are a common occurrence on the Internet, including with the grammatical and spelling errors, the email could be traced back to a computer on the network of the Information Technology Company and an Iranian web host. While the server for the main phishing domain is hidden behind the Cloudflare service, the subdomain linked in the original email appears to point to a free service provider, VVS.ir. After the victim enters their username and password, the form is submitted through a high school site hosted on a foreign server provided by the domestic company. It is likely, based on a cursory audit, that all of the machines involved in the attack are compromised or hacked servers.

Conducting phishing and malware campaigns does not require a high-level of skills or resources, and the history of Iranian cyberspace is filled a multitude of different strategies to interfere with or gain access to email and social networks. While such online attacks are often immediately attributed to the highly-publicized "Iranian Cyber Army," active in the months following the 2009 protests, according to the tracking of Zone-H, during March 2013 alone there was a total of 1,387 website defacements attributed to Iranian hackers, with a similar number in February. The majority of these are attributed to the Ashiyane Digital Security Team, which ranks as the second most active group in world, with thousands of government and high-level defacements (Source: 1, 2). It is also noteworthy that the head of Ashiyaneh, Behrouz Kamalian was sanctioned under the European Union's human rights sanctions regime, for being linked with the IRGC and responsible for "an intensive cyber-crackdown both against domestic opponents and reformists and foreign institutions" (Source PDF).


~3 - Windows Picture and Fax Viewer
خدا خیرت بده! از همون
فاصله رد شو، دستت رو هم دراز
نکن که فردا فیلمون رو مونتاژ
شده در میارن!
FARS
start
~3 - Windows Picture...
7:03 AM


Gmail: Email from Google
support.googleteam.org/verifyaccount/
Reader
Google
New to Gmail?
CREATE AN ACCOUNT
Gmail
A Google approach to email.
Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:
Lots of space
Over 7827.068844 megabytes (and counting) of free
Sign in
Google
Username
Password

THROTTLING OF SECURE TRAFFIC

As noted in previous reports, it appears that SSL services are subject to throttling, particularly for Google products. In one observation of the throttling, requesting a 1.5 Mb image from Wikimedia, the speed of secure web traffic was 6.5% of the standard connection, and the download was terminated after two and a half minutes. While it remains unclear where in the network the throttling is occurring, Iranians have reported on social networking sites that they have had the same problems accessing local services, such as banks.

WIKIMEDIA THROUGHPUT	
HTTP	171 KB/s
HTTPS	11.1 KB/s

RUMORS

// The blocking of VPNs was ordered by the Secretary of the Supreme Council of Cyberspace, and directly approved by the Supreme Leader.

NEEDS AND EDUCATION

- After the blocking of VPNs, the demand for circumvention tools has increased, however this interest has not been matched by due diligence on the tools being used or the manner that people are obtaining them. In our examples of recent attacks, malware was being distributed through a Google Group claiming to help users by distributing circumvention tools. There remains a pressing need to teach users to be careful about the source of their circumvention tools and to never download them from untrusted sources. (Source)

- Since standard VPN services are built into modern smartphones, the most common anti-filtering method for phones and tablets were VPNs. With their blocking, there is a need for more tools and education targeted to smartphone users.

- The adoption of anti-filtering tools has been based on conditions of accessibility, speed, and awareness, rather than actual security. Several of the services and tools shared online appear to have little assurance of privacy of communications, including one service that was found to have its traffic logs, tagged to usernames, publicly available (Source). While some organizations have compiled lists of working tools, it is criterial at this time to evaluate the integrity of the working tools and encourage users to make personal evaluations based on security, as much as performance.

NETWORK ANALYSIS

UPDATES

At the time of reporting, attempts to utilize the ICSI Netalyzer network suite returned errors on multiple networks. It is not clear whether the disruption is intentional, and no clear changes had occurred on traceroutes or where we were able to successfully conduct Netalyzer tests.

RESULTS

TCI DSL SERVICE		PISHGAMAN TOSEH ERTEBAT		MOBINNET	
TRACEROUTE 4.2.2.2					
6 ***		**7** 10.152.32.249	167.415ms	**5** 10.47.33.2	75.252ms
7 ***		**8** 78.38.240.90	66.183ms	**6** 78.38.250.1	76.198ms
8 10.21.22.97	409.042ms	**9** 217.218.154.250	99.562ms	**7** 10.10.53.134	73.672ms
10.21.28.97	120.395ms	**10** 10.10.53.26	90.637ms	**8** 63.218.109.249	359.871ms
9 10.21.21.65	110.748ms	10.10.53.6	75.746ms	213.248.92.133	255.424ms
10 ***		10.10.53.26	94.378ms	**9** 87.226.139.57	284.348ms
11 ***		**11** 79.133.75.161	160.180ms	80.91.248.90	356.879ms
12 ***		**12** 87.226.139.57	169.605ms	**10** 67.17.199.177	305.029ms
13 ***		**13** ***		213.242.110.37	268.719ms
14 ***		**14** 4.69.200.250	196.370ms	213.155.132.195	216.131ms
15 4.2.2.4	191.586ms			**11** 67.16.145.33	291.398ms
				4.69.200.250	897.665ms
TRACEROUTE 8.8.8.8					
6 ***		**8** 78.38.240.90	99.733ms	**5** 10.47.33.2	78.999ms
7 ***		**9** 217.218.154.250	78.249 ms	**6** 78.38.250.1	74.272ms
8 10.21.22.97	132.493ms	**10** 10.10.53.26	96.858ms	**7** 10.10.53.134	70.269ms
10.21.28.97	117.942ms	10.10.53.6	70.005ms	**8** 92.50.194.237	244.822ms
9 10.21.21.65	104.776ms	10.10.53.26	85.908ms	213.248.92.133	254.944ms
10 ***		**11** 213.248.92.137	203.431ms	**9** 63.216.0.38	350.017ms
11 ***		**12** 80.91.248.90	195.205ms	**10** 79.133.94.86	305.380ms
12 ***		**13** 213.155.133.31	203.304ms	74.125.49.77	1365.742ms
		14 213.248.67.66	195.472ms	80.91.247.86	238.624ms

TRACEROUTES