23 APRIL 2013

FLASH NOTE: SYRIA

SYRIAN REGIME TIGHTENS ACCESS TO SECURE ONLINE COMMUNICATIONS

The Syrian regime continues to block popular internet-based secure communication tools. In the past three months, the regime's likely use of deep packet inspection (DPI)[1] has required more sophisticated digital security methods to avoid online detection and blocking.

Virtual Private Networks (VPNs)[2] and purpose-built systems such as Tor and Psiphon[3] have been the target of regime blocking efforts since 2011.[4] In September 2011, the regime successfully blocked default VPN ports, knocking out access to most commercial VPN systems.[5] By December 2012, only those systems using SSH continued to function.[6]

Since 10 February 2013, SSH-based traffic in Syria has also been subject to blocking.[7] Regular Tor connections have also been blocked. By contrast, Psiphon3 traffic has increased (see chart below). Psiphon3 uses a protocol that obfuscates the SSH connection (SSH+), which makes it difficult to detect or block using DPI methods.[8] The Tor Project also deploys an obfuscated application – obfsproxy[9] – however user statistics are not made public[10] so it is difficult to ascertain whether users who were blocked using regular Tor have shifted to the obfuscated version.

Accessing secure communication tools in Syria is becoming difficult. In addition to blocking popular services, the regime is also censoring websites that provide access to these technologies.[11] The SecDev Foundation monitors censorship on the Syrian internet using a system called Black Watch.[12] Tests conducted in Syria during February 2013 confirm the blocking of a variety of content, including independent news, human rights information, and sites devoted to Kurdish independence. Also blocked are the websites of well-known secure communication providers such as Guardster, Hidemyass, Proxify, and Proxyweb.[13]

About This Project

The Syria Digital Security Project seeks to improve the online safety and security of the Syrian people, and to enhance the free flow of information in Syria. To this end, it provides information, analysis, tools and resources dedicated to enhancing digital safety and openness in Syria. The project is administered by The SecDev Foundation, a Canadian not-for-profit organization, with funding from granting bodies in North America.

About The SecDev Foundation

The SecDev Foundation is a not-for-profit organization that seeks to broaden global public awareness and understanding in three core programme areas: cyber empowerment; the sources of security and resilience; and armed violence prevention and reduction. The SecDev Foundation supports local partners, research and advocacy in regions at risk from fragility, violence and underdevelopment in Asia, Africa, Eurasia, the Middle East and Latin America.

www.secdev.com

www.twitter.com/secdev

TheSecDev FOUNDATION

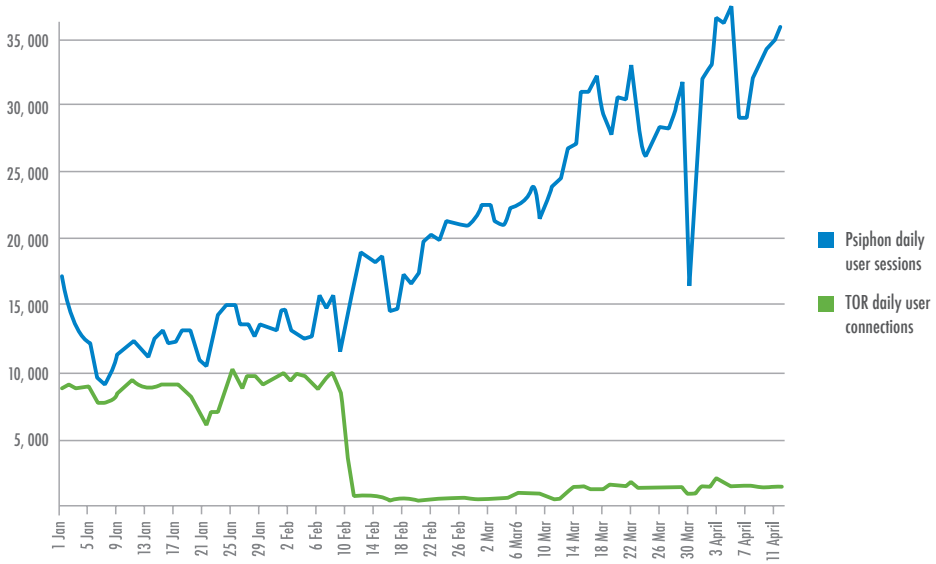
ASSESSMENT

Despite the increasing difficulty of accessing secure communications, demand for these tools and services is increasing. Syrian awareness of the dangers of unsecured communication has likely been fueled by reports of online activists being arrested[14] and of the regime's sophisticated capabilities for censorship and cyber warfare.[15]

These facts point to the importance of the internet to ordinary Syrian citizens in the deepening civil war. In 2012, almost half a million more Syrians subscribed to cell phone and internet services than in the year prior to the conflict.[16] An overwhelming majority of respondents to a recent poll carried out by The SecDev Foundation – 84 % – indicated that the internet is vitally or very important to them. The same poll also revealed a strong demand for further information on how to access and use digital security tools such as Tor and Psiphon.

The Syrian civil war reveals the importance of the internet to all parties in the conflict. The fact the regime has chosen to throttle rather than shut off access to the internet suggests that it is sensitive to the impact closure would have for a country where some 5,113,749 Syrians are online.[17] Shutting down the internet would also diminish the state's capacity for online surveillance. This suggests that providing Syrians access to robust and resilient secure communication technologies is important to preserving the connections between people and communities that will be vital to Syria's future once the fighting ends.

FIGURE 1



[1] https://en.wikipedia.org/wiki/Deep_packet_inspection

[2] https://en.wikipedia.org/wiki/Virtual_private_network

[3] http://www.psiphon.ca and https://s3.amazonaws.com/0ubz-2q11-gi9y/kk.html

[4] The SecDev Foundation. 25 November 2012, *Syria Cyber Watch*. https://docs.google.com/a/secdev.com/file/d/0B-szos-lFcMSaWpnUGJRZlpQYzg/edit. Best VPN Service. September 30 2011. "Syria blocked all VPN services after Iran and China!!," on *Best VPN Service*, http://www.bestvpnservice.com/blog/syria-blocked-all-vpn-services-after-iran/

[5] Best VPN Service. 30 September 2011. "Syria blocked all VPN services after Iran and China!!," on *Best VPN Service*, http://www.bestvpnservice.com/blog/syria-blocked-all-vpn-services-after-iran/

[6] The Tor Project. December 2012. See https://trac.torproject.org/projects/tor/wiki/doc/OONI/censorshipwiki/CensorshipByCountry/Syria

[7] http://en.wikipedia.org/wiki/Secure_Shell
See figure 1.

[8] Psiphon 3 uses SSH plus obfuscation, a randomized layer on top of SSH to avoid protocol fingerprinting.

[9] The Tor Project. "Obfsproxy." https://www.torproject.org/projects/obfsproxy.html.en

[10] Tor confirmed this fact via a private email to SecDev, 15 April 2013.

[11] http://www.freedomhouse.org/report/freedom-net/2012/syria

[12] BlackWatch was developed by SecDev to actively measure access to specific internet resources and determine patterns of internet censorship and filtering across different ISPs, including wireless providers.

[13] SecDev will release a FlashNote detailing Black Watch testing results in Syria in April 2013.

[14] David Rosenberg. 23 May 2011. "Syria adopts two-faced strategy with social media," in *Jerusalem Post*. http://www.jpost.com/MiddleEast/Article.aspx?id=221847

[15] Jennifer Valentino-Devries, Paul Sonne, and Nour Malas. "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web," in *The Wall Street Journal*. http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

Justin Salhani. 18 January 2013. "In Syria, the cyberwar intensifies," on *DefenseNews*. http://www.defensenews.com/article/20130118/C4ISR01/301180018/In-Syria-Cyberwar-Intensifies

[16] BuddeComm. "Syria - Telecoms, Mobile, Broadband and Forecasts," on *BuddeComm*. http://www.budde.com.au/Research/Syria-Telecoms-Mobile-Broadband-and-Forecasts.html

[17] Madar Research and Development. 2012. *Arab ICT Use and Social Network Adoption Report*. http://www.madarresearch.com/default.aspx