UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 02 – November 2011

Behind Blue Coat:

An Update from Burma

BACKGROUND

Citizen Lab research into the use of commercial filtering products in countries under the rule of authoritarian regimes has previously documented the use of devices manufactured by U.S.-based Blue Coat Systems in Syria and Burma. In *Behind Blue Coat: Investigations of commercial filtering in Syria and Burma*, we identified Blue Coat devices in Burma through the error messages, hostnames and filtering behaviour on Burmese Internet service provider (ISP) Yatanarpon Teleport.

Since the publication of *Behind Blue Coat*, it has been reported that the U.S. Commerce Department has launched an investigation to determine if the company had prior knowledge that its equipment was being used by the Syrian government.[1] This action was launched following a call from three U.S. Senators for an investigation into Blue Coat and NetApp, another U.S. company whose equipment has been implicated in surveillance activities by the Syrian government.[2]

Additional evidence gathered by the Citizen Lab from Burma since the publication of that report has provided further confirmation that Blue Coat's devices are presently in use in the country. A message displayed to users by Yatanarpon Teleport references Blue Coat in the URL and is consistent with how Blue Coat devices display notification messages to users. Combined with the evidence presented in *Behind Blue Coat*, these new findings present a strong case that Blue Coat's devices are actively in use in Burma.

FINDINGS

In mid-October 2011, users of the Burmese ISP Yatanarpon Teleport were automatically directed to a service-related message in their web browser.[3] The message, displayed both in English and Burmese, stated the following:

"Dear Valued Customers,

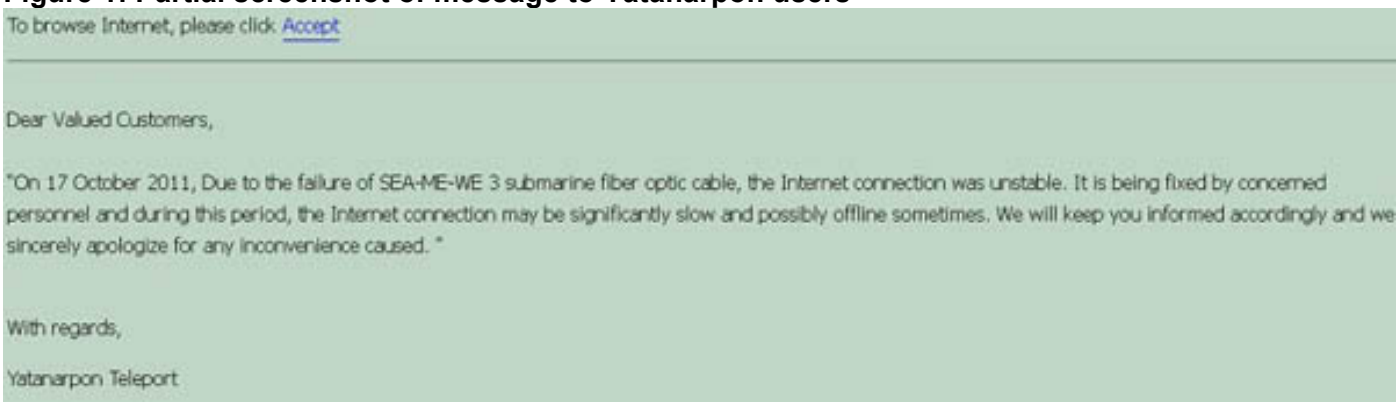
On 17 October 2011, Due to the failure of SEA-ME-WE 3 submarine fibre optic cable, the Internet connection was unstable. It is being fixed by concerned personnel during this period, the Internet connection may be significantly slow and possibly offline sometimes. We will keep you informed accordingly and sincerely apologize for any inconvenience caused."

With regards,

Yatanarporn Teleport"

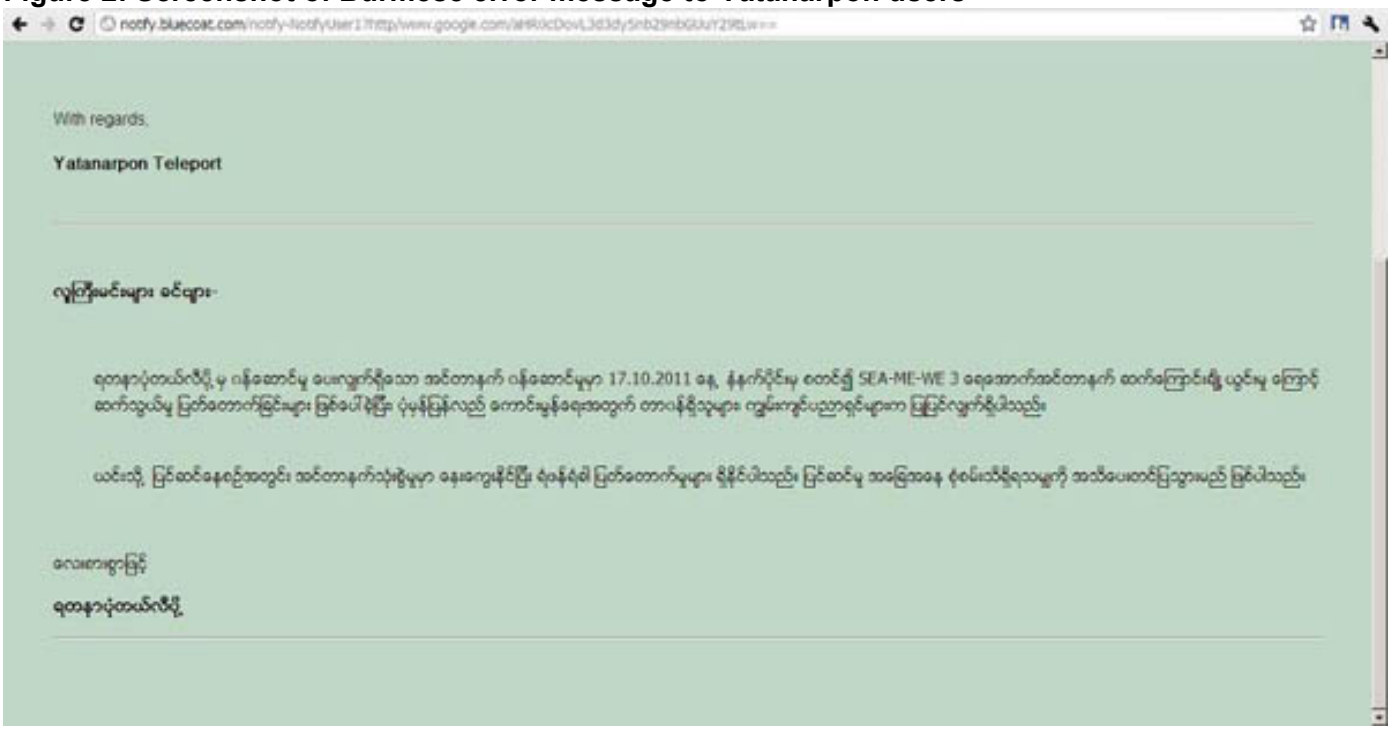
A partial screenshot of this error message can be seen in Figure 1:

Figure 1: Partial screenshot of message to Yatanarpon users



The full text of the Burmese error message can be seen in Figure 2:

Figure 2: Screenshot of Burmese error message to Yatanarpon users



Users were required to click "Accept" in order to continue browsing, as seen in Figure 1. The disruption of this undersea cable and the ensuing Internet connectivity disruption in Burma has been documented by others.[4]

The content of this error message provides further confirmation that Blue Coat devices are actively in use on Yatanarpon Teleport. Figure 3 shows an enlarged version of the error message from Figure 2:

Figure 3: An enlarged version of the address bar shown in Figure X [Burmese] above

As can be seen in Figure 3, the URL displayed by the browser begins with "http://notify.bluecoat.com/", providing further evidence that Yatanarpon Teleport is using Blue Coat technology.

This URL does not, however, indicate that this content is hosted on Blue Coat's servers. Blue Coat identifies the notify.bluecoat.com domain as a "default 'virtual hostname' for user notification pages produced by

security appliances from Blue Coat Systems, Inc."[5] The format of this URL is also consistent with Blue Coat documentation referring to the display of user notification pages by ProxySG devices.[6] Thus, although the URL suggests that the page is being hosted on Blue Coat's servers, it is likely being generated by their devices located in Burma.

Anecdotal reports of Blue Coat messages on Burmese ISPs from users date back to at least 2009, including discussion board threads[7] and information relayed to the Citizen Lab from colleagues in the field. Similar user notification messages appearing to originate from "http://notify.bluecoat.com" can be seen in Figures 4 and 5:

Figure 4: Additional user notification message referencing a Blue Coat URL

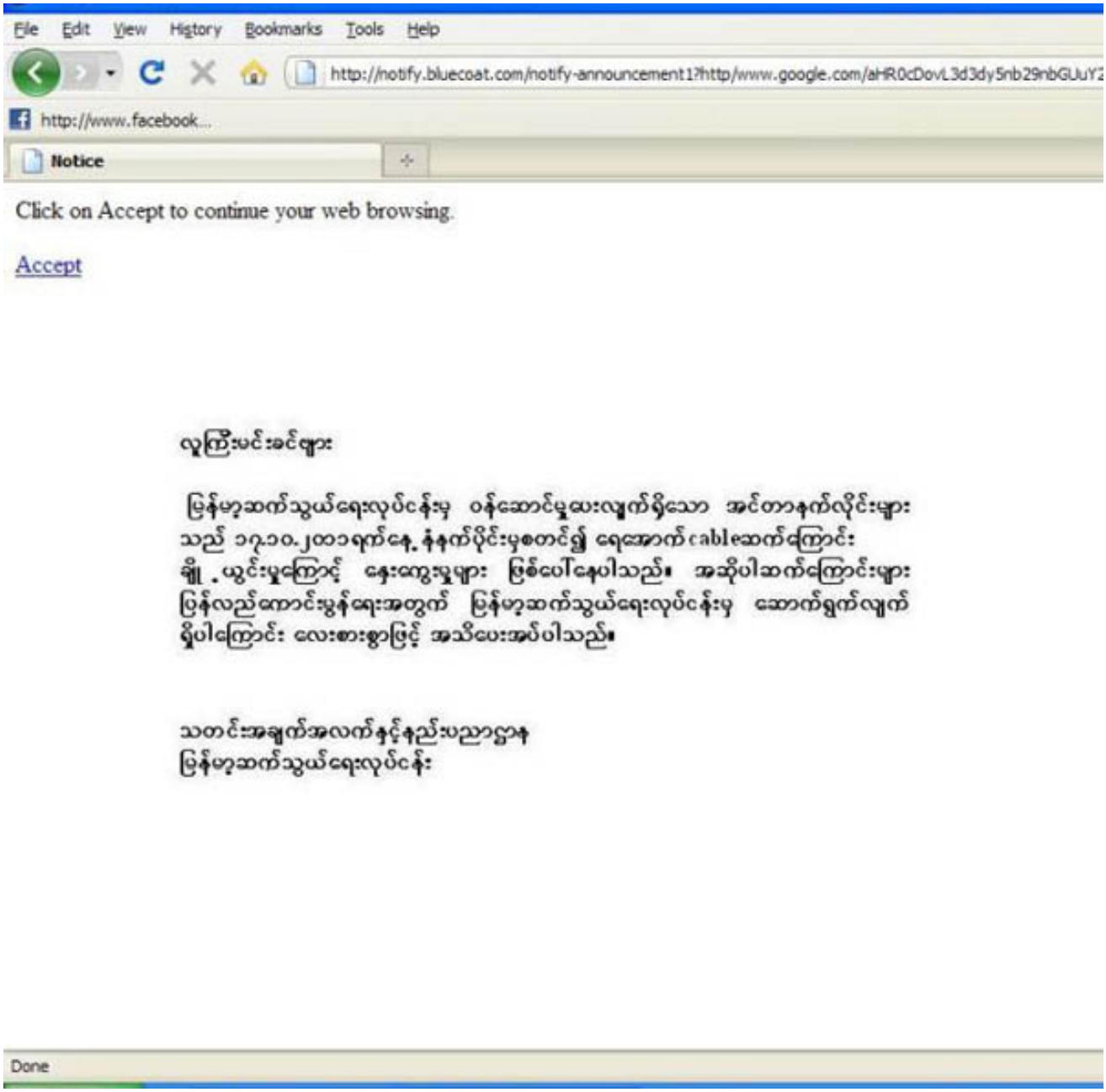
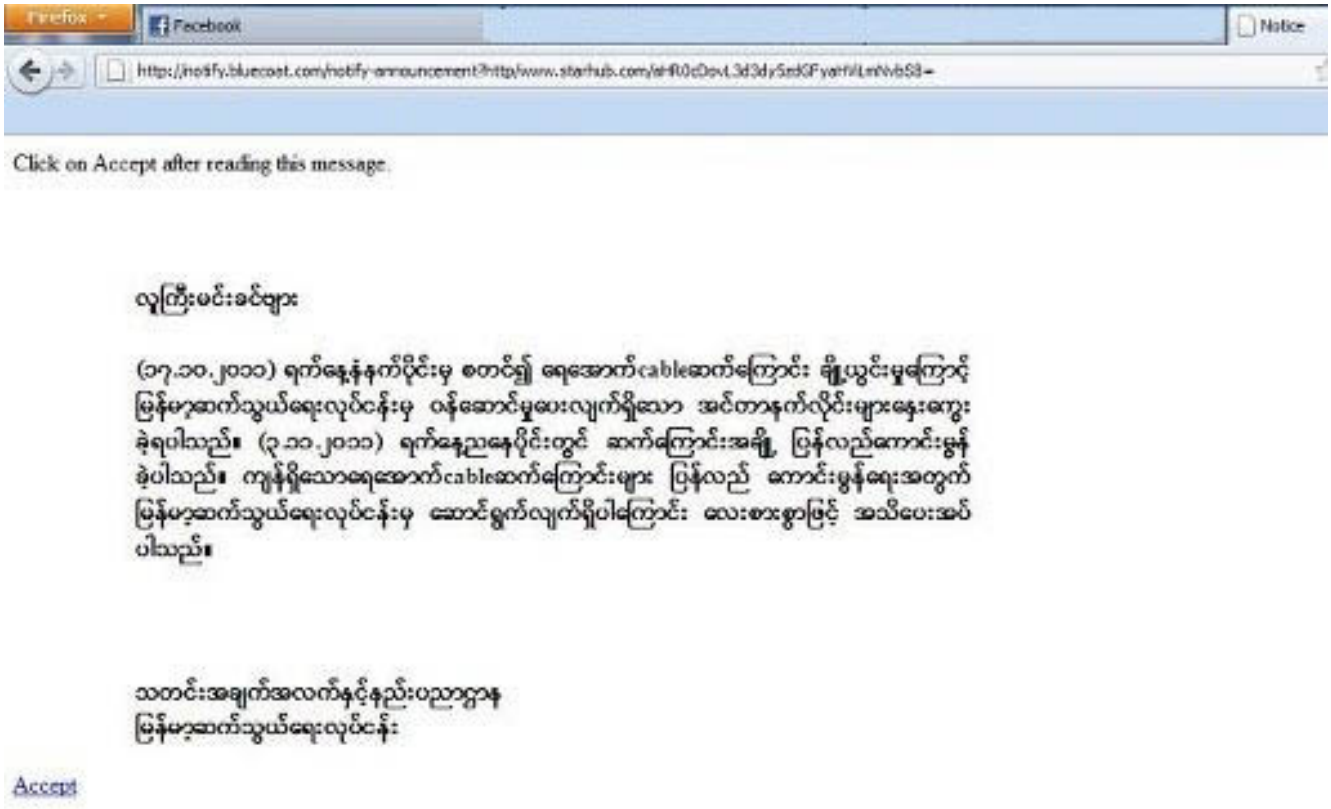


Figure 5: Additional user notification message referencing a Blue Coat URL



Translations of these messages indicate that they are also network status messages notifying users of a connectivity disruption caused by issues with an undersea cable.

DISCUSSION

The use of censorship and surveillance technology in countries under the rule of authoritarian regimes raises a number of concerns. Companies who find that their products are being used for the purposes of censorship in countries like Syria or Burma, regardless of how those products may have arrived there, are faced with a number of technical, legal and ethical challenges. Our report *Behind Blue Coat* identified a number of these issues and raised questions about the use of Blue Coat technology in Burma, including:

- Is Blue Coat aware of the use of their products and/or services in Burma/Myanmar?
- If so, has Blue Coat taken any steps to restrict the functionality of those devices?
- In light of these recent findings, will Blue Coat actively monitor the devices that contact its servers to prevent Blue Coat technology from being used in embargoed countries?
- If Blue Coat forbids its resellers from selling to embargoed countries, what actions will Blue Coat take with respect to the reseller who brought the 13 devices identified by Blue Coat to Syria?

- Does Blue Coat have a policy for evaluating the sale of products and services to government, government-controlled or government-affiliated entities that engage in filtering of political content? If so, will Blue Coat share that policy?

Citizen Lab contacted Blue Coat Systems on October 27, 2011, requesting more information regarding the use of their technology in countries against which U.S. trade sanctions are imposed. As of November 29, 2011 we have not received any further information on this issue from the company.

The Citizen Lab continues to strongly urge Blue Coat to investigate these findings and to take all necessary steps to limit the functionality of their products in Syria and Burma.

Acknowledgments: The Citizen Lab would like to thank colleagues who wish to remain anonymous for sharing information collected from Burma.

FOOTNOTES

[1]Horwitz, Sari and Asokan, Shyamantha, "U.S. probing use of surveillance technology in Syria," Washington Post, November 17, 2011, http://www.washingtonpost.com/world/national-security/us-probes-use-of-surveillance-technology-in-syria/2011/11/17/gIQAS1iEVN_story.html

[2]Elgin, Ben and Silver, Vernon, "U.S. calls for NetApp probe on Syria spy tech," Bloomberg, November 10, 2011, http://www.bloomberg.com/news/2011-11-10/netapp-role-in-syria-spy-project-spurs-demands-for-u-s-inquiry.html

[3]Aung, Htoo and Stuart Deed, "Cable fault causes 'unstable' net: ISP" The Myanmar Times, November 6, 2011, http://www.mmtimes.com/2011/info/599/

[4]See Sai Zom Hseng, "Burma's Internet, newly opened, slows to a crawl" Irrawaddy, November 3, 2011, http://www.irrawaddy.org/article.php?art_id=22379

[5]See http://notify.bluecoat.com/

[6]Blue Coat, "Why is the ProxySG not serving the notify user page when I have the default policy set to deny?" January 10, 2011, https://kb.bluecoat.com/index?page=content&id=FAQ1223&actp=RSS

[7]See http://www.mysteryzillion.org/discussion/comment/34670#Comment_34669