CPJ Committee to Protect Journalists
Defending Journalists Worldwide

Tunisia invades, censors Facebook, other accounts

By **Danny O'Brien/CPJ Internet Advocacy Coordinator (/blog/author/danny-obrien)**

Tunisian authorities have tried to censor photos just like this one, which shows civil unrest in Tunis. (AFP/Fethi Belaid)

The Tunisian government has been a notorious censor for many years, for journalists online and off. In the wake of widespread domestic protests in December, however, the authorities appear to have turned to **even more repressive tactics (http://cpj.org/2011/01/tunisia-must-end-censorship-on-coverage-of-unrest.php)** to silence reporting. In the case of Internet bloggers, this includes what seems a remarkably invasive and technically sophisticated plan to steal passwords from the country's own citizens, in order to spy on private communications and squelch online speech.

Based on reports of users in the country, Tunisian authorities appear to be modifying web pages on the fly to steal usernames and passwords for sites such as Facebook, Google and Yahoo. Unknown parties have subsequently logged onto these sites using these stolen credentials, and used them to delete Facebook groups, pages, and accounts, including **Facebook pages (http://atunisiangirl.blogspot.com/2011/01/you-cant-stop-us-from-writing.html)** administrated by Sofiene Chourabi, a reporter with Al-Tariq al-Jadid, and the account of local online video journalist **Haythem El Mekki (http://twitter.com**

/%23!/bylasko) . Local bloggers have told CPJ that their accounts and pictures of recent protests have been deleted or otherwise compromised.

Usually in such hacking attacks, it's hard to pin responsibility, except circumstantially, on local governments. Those conducting this particular attack, however, needed an extraordinary amount of privileged access to Tunisia's network infrastructure. Looking at the clues left by the attack, I'm among those who think all the evidence points to a state-controlled operation.

Here's how it worked, as uncovered by the online news site ***The Tech Herald*** ***(http://www.thetechherald.com/article.php/201101/6651/Tunisian-government-harvesting-usernames-and-passwords)*** : When Tunisians visit, say, Facebook, the page they receive has 10 extra lines of code, as compared to the normal login page originally sent by Facebook itself.

When Tunisians hit the Facebook "login" button, this extra code takes their user names and passwords, scrambles them, and then calls for another Web page, with the scrambled data included in the new Web address it requests. Tunisians don't see this new page, but their browser still attempts to load it, sending their private credentials across the Net.

How did these extra 10 lines get there? It's possible that they could be inserted by local viruses or malware, but widespread accounts from Tunisians strongly suggest these lines are being dropped into the Facebook page by the state-run Internet service provider, the Tunisia Internet Agency.

Where is the private username and password being secretly sent? The extra code within the Facebook page doesn't send the password data to another rogue Internet server, as you'd expect if this code was inserted by criminal hackers. Instead, the user's browser attempts to load a non-existent page on Facebook's own site, called "http://www.facebook.com/wo0dh3ad".

A page access like that would normally only reveal your user name and password to Facebook itself. Unless that is, the Tunisian Internet Agency is logging all web addresses visited by its customers, and keeping a record of visits to this particular address. Such logs are not difficult for an ISP to create or maintain. Indeed, if you were building a local censorship system, you could easily generate such a log as a side effect of your filtering systems.

From every piece of evidence CPJ has seen, this looks nothing like a criminal hacking attack, and everything like a state-run attempt to gain access to private online accounts. Certainly, it explains the rash of hacking attacks on activists and reporters in the region.

What can be done? Fortunately, because the fake "wo0dh3ad" page accessed was on their site, Facebook may well have a log of everyone whose account was compromised and can take steps to warn and protect their Tunisian users. As we have **previously advised (http://cpj.org/internet/2010/07/using-https-to-secure-the-web-for-journalism.php)** , Internet companies should deploy encrypted "https" versions of their sites, which prevent intermediaries from meddling with their data in transit. And Internet infrastructure providers and foreign governments should publicly demand an explanation from the Tunisian Internet Agency for their violation of every principle of Internet management, as well as their own citizen's right to privacy and a free, uncensored online press.

San Francisco-based CPJ Internet Advocacy Coordinator Danny O'Brien has worked globally as a journalist and activist covering technology and digital rights. Follow him on Twitter **@danny_at_cpj (http://twitter.com/danny_at_cpj)** .

Categories:

- **Middle East & North Africa (http://cpj.org/internet/mideast/)** ,
- **Tunisia (http://cpj.org/internet/mideast/tunisia/)**

Tags:

- **Censored (/tags/censored)** ,
- **Facebook (/tags/facebook)** ,
- **Hacking (/tags/hacking)** ,
- **Internet (/tags/internet)**