Print This Page

TRIBLIVE

Protesters, criminals get around government censors using secret Web network

Rasha Abdulla, a professor at the American University of Cairo, attends an anti-government protest outside the Culture Ministry in Cairo on Wednesday, June 21, 2013.

By Andrew Conte
PITTSBURGH TRIBUNE-REVIEW

Published: Saturday, June 22, 2013, 9:00 p.m.
Updated: Sunday, June 23, 2013

As hundreds of thousands protested for democracy during the 2011 Arab Spring uprising, Egyptian authorities cut access to Twitter to prevent demonstrators from quickly communicating.

Protesters then flocked to Facebook, where — in the two hours before the government blocked that social media site — they could find instructions on how to avoid government scrutiny of their electronic communications by accessing the "hidden Internet."

In that time, hundreds of people learned how to get on Tor , an online network created by the U.S. government that allows people to surf the Web anonymously, beyond the reach of government censors.

The number of Tor users in Egypt quadrupled over the following days to more than 2,000 — until the authorities shut down Web access.

"They realized the core activists that they wanted to prevent from communicating were communicating anyway," said Rasha Abdulla, a journalism professor at The American University in Cairo who joined the protests two years ago. "It gives you an idea of how freaked out the regime was. You don't go to that kind of extreme unless you really feel that you're falling apart."

Now after revelations about widespread U.S. government surveillance of social media and cellphone

records, Egyptians are able to lecture Americans about Internet privacy. What once seemed unnecessary to most Americans might make sense, even to people not doing anything illegal or even embarrassing.

More than 80,000 people in the United States log onto the Tor network to access the Web each day, according to its metrics . Edward Snowden, a former employee of a U.S. government contractor who leaked information about U.S. intelligence agency snooping, had a Tor sticker on his laptop.

Tor protects users by encrypting their Internet traffic and routing it through servers around the world, making the information appear to come from somewhere else. About a half-million people a day use the network worldwide, with the United States and Italy topping the list. But it has been popular in Iran, Syria and other places where governments try censoring the Web.

Because it provides anonymity, Tor also has become a haven for computer criminals dealing in drugs, child pornography, illegal guns and even murder, if advertisements for hit men can be believed. Anarchists, skinheads and hackers use the network for discussion and recruitment.

Officials at the Massachusetts nonprofit that runs Tor said it plays an important role in places where governments seek to control the Web. "Tor continues to defeat censorship and allow citizens access to the open Internet," executive director Andrew Lewman told the Tribune-Review.

Abdulla, heading out the door to attend a recent sit-in at Cairo's Ministry of Culture, told the Trib she sees a duty in seeking Internet privacy.

"You should not be subject to government surveillance anyway, at least not without a court order," she said. "If that's happening, then it's definitely your right to protect yourself against that by trying to maintain your anonymity."

How Tor began

Tor started out as a project of the Naval Research Laboratory in the early 2000s for military communications and command and control even in hostile areas. Originally known as The Onion Router, the name derives from the metaphor of peeling away layers of encryption at each server so that no one eavesdropping on the communication can identify the user, the content and the end destination.

Anyone can download the Tor software for free and surf the web anonymously from a computer or a cellphone. Service providers can create hidden websites that end in .onion — rather than .com or .org. Users can access them only on the network. Because Tor sends information through other nodes, traffic on it moves slower than on the rest of the Web.

There are other programs that allow users to hide an email address, encrypt messages or operate through proxy servers to hide their identity, but none is as sophisticated or widely used as Tor, cyber experts told the Trib.

Though the network was created for the military, its founders made the software public to further conceal the reasons people use Tor, said Seth David Schoen, senior staff technologist at the Electronic Frontier Foundation, a San Francisco-based nonprofit that works to protect Internet privacy. The foundation initially helped fund Tor research.

"If the Navy ran (Tor) and made it available only to Navy sailors, anyone seen using Tor would clearly be working for the Navy," Schoen told the Trib. "If Tor is public and widely used for many different purposes, no one can tell for sure why a given person is using Tor."

On the front end, an initial server in the Tor network might see that someone is using Tor on their computer but not what they're doing or where they're going. A middle server bounces the information along without seeing who sent it or where it's going. The exit server can see the destination and possibly the content but not who sent it.

To hide the content and your email address or identity, experts recommend using encryption software.

Not even Tor's creators have a back-door way of watching traffic on the network, said Alexander Volynkin, a researcher at CERT, a computer security research arm of Carnegie Mellon University's Software Engineering Institute.

"Because the network is designed the way it is," he said, "you don't have the ability to police and say, 'I'm going to allow legal activities and I'm going to disallow illegal activities.' You don't have any visibility into that traffic whatsoever."

Paul Cesarini, a technology education professor at Bowling Green State University in northwest Ohio, had been using Tor from his campus computer until campus police and IT officials visited his office one day to ask what he was doing. They could see that he and one other user on campus were using the service but they could not tell why.

"It's essentially like the user is saying, 'Talk to the hand,' " Cesarini said. "So you're not hiding the fact that you're using Tor or a similar product. You're just hiding what you're doing while you're using it."

Cesarini told BGSU officials he was using Tor to prepare for a class on Internet censorship.

Guaranteed anonymity?

Tor gives the illusion of total anonymity but the network cannot guarantee it because the system relies on

volunteers to control the nodes where the information passes, Volynkin said.

"You do not know what, in fact, is actually happening on those nodes and therefore you cannot predict and say, 'There's a 100 percent certainty nobody, in fact, knows about who you are,' " he said.

Tor does have potential vulnerabilities, Schoen said.

Someone watching both ends of a communication through the network might be able to correlate the information going in and coming out. A powerful attacker might try to locate a hidden service on Tor by knocking the Internet offline in certain geographic areas to see what websites disappear.

Protest organizers using Tor in Egypt are not so naïve to think their identities are completely anonymous, Abdulla said. But they realize that using the network gives them more protection than nothing.

"You have two options — either to use it, or to not use it," she said. "I was still on Twitter and on Facebook after they blocked it, and I could see a lot of my friends were still on there. But I could also see that a lot were not."

Andrew Conte is a staff writer for Trib Total Media. He can be reached at 412-320-7835 or andrewconte@tribweb.com.