The dangers of the dark web

March 30 2017

Credit: AI-generated image ([disclaimer](#))

The dark web—which utilizes a technology created by military researchers in the 1990s to allow intelligence operatives to exchange information completely anonymously—is unknown to many. It's been said to be a breeding ground for organized crime, sex traffickers, and hackers. But it's also used by good actors, including whistle-blowers and activists.

We asked professor Engin Kirda—a systems, software, and network security expert who holds joint appointments in the College of Computer and Information Science and the College of Engineering—to discuss the dangers of this little-known corner of the internet.

First and foremost, how do you access the dark web?

To access the [dark web](#), one needs a special type of anonymization software found on the internet. Tor is a good example of such software. Using special Tor addresses and the Tor browser, one can anonymously connect to these "dark" web pages and surf them.

Cyberexperts say the dark web is used by a range of bad actors. But it's also been used by whistle-blowers as well as activists during the Arab Spring, who harnessed the platform's power to organize demonstrations and disseminate information anonymously. In your opinion, do the positives of the dark web outweigh the negatives?

As a scientist, it is difficult to answer a question like this without having scientific data. I don't know of any studies that have measured how much of the dark web is being used for illegal activities, and how much of it is being used by good people who just want to remain anonymous.

The Senate has just voted to allow ISPs to sell your browsing history to third parties. I find this development very concerning. Anonymization services such as Tor that also allow the dark web to exist help in such cases to hide who is accessing a website. I, for example, would be concerned if my ISP is informing a third party that I am researching a certain medical condition on WebMD. Of course, at the same time, we

also need to be vigilant and try to go after illegal activities on the dark web.

A recent NBC News report suggested that would-be hackers could visit the dark web to purchase do-it-yourself crime tool kits in order to launch attacks through phishing emails, malware, and ransomware. What security measures have been put in place to prevent the average Joe from carrying out massive hacks?

There have been cases where "average Joes" have indeed bought illegal services from the dark web. But I'm not very concerned about the average Joe buying a malware or hacking service. Sophisticated hacks, as the name suggests, are sophisticated. I don't think an average person can just buy and use them for massive hacks. I, personally, would be more concerned about more sophisticated attacks being sold to more sophisticated actors.

Right now, there are no security measures on the dark web. If you sell something, if you know what you're doing, you can hide your tracks quite efficiently. However, luckily, bad guys do make mistakes and that's how the guy who was running SilkRoad got arrested. If you want to hide your tracks, you need to know quite well what you're doing.

Not long ago, researchers made a surprising discovery on the dark web, finding government-made malware that could be used to target energy grids. What would you say are the biggest dangers posed by the dark web?

I think illegal activity on the dark web is the biggest danger right now. Clearly, we want to have a dark web that provides privacy guarantees for users, but at the same time, we don't necessarily want this technology to be misused for illegal activity. There is no easily solution I am afraid. This discussion is the same discussion that we have around encryption. Governments would love to read every encrypted communication. But should we allow that to happen? What is an individual's right to privacy?

Provided by Northeastern University