NETWORKWORLD

Criminals on Tor is the price of global liberty

By Antone Gonsalves, CSO
March 07, 2014 09:38 AM ET

CSO - Research pointing to rising criminality on Tor shows the cost of having a network that provides anonymity to whistleblowers, journalists, political dissidents and others trying to avoid government surveillance.

Experts agreed on Thursday that nothing could be done to prevent cybercriminals from using Tor without raising the risk to legitimate users. Recent research by Kaspersky Lab expert Sergey Lozhkin found that "the cybercriminal element is growing" on the anonymity network.

The way Tor is used by Chinese dissidents to skirt the Great Firewall and oppressive censorship is the same way criminals cloak the operators of marketplaces and forums where criminals can rent botnets for DDoS attacks or to distribute malware, buy stolen credit card numbers and launder bitcoins, the most widely used currency on the dark Web.

"If it were possible to stop criminals from using Tor, it would be useless," Julian Sanchez research fellow at the Cato Institute, said. "After all, the dissidents who use it to protect themselves are considered criminals by their own regimes."

While the number and breadth of criminal resources is not on the same scale as the traditional Internet, Lozhkin did find 900 hidden online services and 5,500 nodes and a 1,000 exit nodes used in criminal activity.

A node is any processing location on a network. It can be a computer or some other device. An exit node allows for exiting the network to a specified IP address and port combination.

"Like all technologies, Tor is dual use," Jerry Brito, head of the Technology Policy Program at the Mercatus Center at George Mason University, said. "Fire can be used to cook and to keep warm, but it can be used to destroy a village as well. The key is to target those who would misuse the technology, and not the technology itself."

Jason Smolanoff, vice president of Stroz Friedberg, said the digital forensics firm has used sophisticated technologies and investigative techniques to identify individuals involved in computer intrusion and copyright infringement.

"While TOR does provide anonymity on the Internet, it is not foolproof and many cybercriminals often leave other investigative clues as to their identity and motivation, and are ultimately caught by investigators," Smolanoff said.

One of the most notorious Tor marketplaces busted by U.S. authorities was Silk Road, which was shutdown last year and the creator arrested in San Francisco. Sellers primarily traded in illegal drugs with thousands of listings for marijuana LSD, heroin, cocaine, methamphetamine and ecstasy.

While Silk Road-like operations should not be tolerated, shutting down or compromising Tor would have a more serious impact on society.

"The gamble our own government made when funding Tor was that a decentralized anonymity network resistant to state power would ultimately be enough of a net benefit to global liberty that it was worth accepting the protection it would also necessarily afford genuine bad actors," Sanchez said.

Tor originated from a U.S. Navy project aimed at protecting government communications. The technology developed by the Naval Research Lab was eventually used in building the anonymity network in existence today.