TECHNOLOGY

Tor's ex-director: 'The criminal use of Tor has become overwhelming'

(Getty Images)

Patrick Howell O'Neill May 22, 2017 | CyberScoop

Nearly two years to the day since Andrew Lewman quit his job as executive director of Tor, the anonymity software meant to shield users from government intervention, he found himself rushing between meetings with European law enforcement.

Boosted by endorsements from internet activists like Julian Assange and Edward Snowden, Lewman had been at the helm of Tor as it became synonymous with internet user privacy. Now, as the newly minted vice president of dark web intel firm OWL Cybersecurity, his meetings with governments have gone from educating officials on how people use Tor to helping law enforcement investigate criminal activity occurring on Tor. As Lewman spoke to CyberScoop last month in between two of those meetings, it became clear that his perspective on the software has shifted.

“What’s changed most about Tor is the drug markets have taken over,” Lewman said. “We had all these hopeful things in the beginning but ever since Silk Road has proven you can do it, the criminal use of Tor has become overwhelming. I think 95 percent of what we see on the onion sites and other dark net sites is just criminal activity. It varies in severity from copyright piracy to drug markets to horrendous trafficking of humans and exploitation of women and children.”

In the last two years, dark web black markets have grown richer selling malware, data, drugs and more. The multimillion-dollar criminal outfits that operate on the dark web, which began six years ago as an ideologically-driven invention of a libertarian 20-something based in San Francisco, have since been co-opted by global organized crime. Child exploitation has in many ways thrived on Tor — but, as defenders of Tor are quick and right to point out, the public internet is home to to its own mountainous pile of drugs, child exploitation and crime that pales in comparison to what’s found on the dark web.

Proponents of Tor, including prominent journalists who use the software to anonymously communicate with sources, also hit back against the criticism by saying the technology is used in some of the biggest and most influential newsrooms in the world.

Hidden and un-hidden on the dark web

> Both Bitcoin and Tor Hidden Services have produced substantial negative impacts far outweighing any benefits #StateYourUnpopularOpinion
>
> — Nicholas Weaver (@ncweaver) April 26, 2017

stand in contrast to the more common use of Tor — the part that acts like a free virtual private network to anonymously visit the public internet.

Nicholas Weaver, a security researcher at UC Berkeley, echoed Lewman's criticism.

"I've long been down on hidden services," Weaver told CyberScoop. "It gratifies me to hear that some around the Tor community have come to the same realization."

Weaver did point out exceptions to his criticism. In 2014, Facebook launched a Tor website that was "un-hidden" (users know the server's IP address) but remained within the Tor network, allowing improved speed for the software's privacy-seeking users. That kind of "un-hidden" website, which has become increasingly common since then, was pioneered by Alec Muffet who previously worked as a security and network engineer at Facebook. Earlier this year, Muffet launched a tool allowing enterprises to mirror their sites to Tor.

Muffet strongly disagreed with Lewman's assessment.

"Andrew's schtick is pretty much what I would expect from people who have bought into the mythos of 'the dark web' as being something from which folk need to be protected, or similar," Muffet told CyberScoop. "I'm an optimist. I'm a builder. I like having more tools so that I can give people more security, more options and more help. So, for me, Onion Routing and Tor are a fabulous new ingredient to cook with."

Andrew Lewman (Knight Foundation/Flickr)

public. After leaving Tor, Lewman bounced around cybersecurity companies like Norse and Farsight Security before joining OWL.

The career path Lewman traveled will no doubt draw comparisons to Matt Edman, a former Tor developer who became a FBI contractor developing anti-Tor malware used in criminal investigations related to child pornography.

Lewman, along with Tor's project leader Roger Dingledine, has worked with law enforcement agencies for years and made frequent visits to places like the FBI Academy. Under Lewman's watch, Tor developed ExoneraTor, software to designed to tell a cop if an IP address is a Tor exit node. It's meant, Lewman explained, to prevent raids against Tor exit node operators.

"It's very hard to change a mindset if the first time you're introduced to Tor is while tracking down a criminal," Lewman explained in a 2010 blog post. "You may assume only criminals use Tor (you would be wrong). If we can talk to law enforcement first, they may look at Tor in a different light."

What he tells law enforcement now would seem to be markedly different.

The Tor Project, a nonprofit which has received the vast majority of its funding from the U.S. government, was first released in 2002, but it was under Lewman's leadership from 2009 to 2015 that the software exploded in both bandwidth and fame. The hidden services, as opposed to the overall network, receive disproportionate public attention considering they account for less than 8 percent of the Tor network's total traffic, according to network statistics. But the tech earns a lot of that attention by enabling powerful and secure web tools for use by everyone from human rights activists to journalists to criminals.

Good dark web, bad dark web

Tor developers at the highest levels have discussed getting rid of hidden services, Lewman said, and they've generally struggled to gain financial sponsors for the technology.

"We discussed [eliminating hidden services] and at the time we couldn't really find a good usage of hidden services," Lewman said. "There's all sorts of theoretical ones but there's no actual ones. SecureDrop, that seems to be the only usage and even then when I've worked with media organizations they say effectively no one uses it."

SecureDrop, first launched in 2013, is Tor-powered software designed for anonymous and secure communication between sources and journalists. It's been adopted by many of the world's largest news organizations including the New York Times and Washington Post.

"It's a marketing thing," Lewman said. "You have it because it sounds good, but effectively no one uses it at all. And almost every time if someone does manage to upload some documents they end up doing it by email because they get so sick of the back and forth over the hidden service."

actually use SecureDrop.

The Times and Post didn't respond to questions, but The Intercept, which was founded in the wake of Snowden's leaks, and Gizmodo both weighed in.

"We definitely get a lot of good stuff through SecureDrop," Micah Lee, a technologist at the Intercept, told CyberScoop. "We also get a lot of useless stuff. It's sort of like a tips email address. Maybe you occasionally get good stuff and you get a lot of not actual tips or people who are wanting to contact Glenn Greenwald or whatever. But we do actually get some stories from SecureDrop. It's definitely a very useful resource and I know we're not the only ones."

"We have definitely gotten useful, actionable material through our SecureDrop," John Cook, who runs digital investigations for Gizmodo Media Group, told CyberScoop. "It's not a flood everyday, but it's definitely worth having in terms of what's come in."

Cook agreed that SecureDrop had a marketing element to it: "It's just a way to communicate with sources that you're sophisticated and care about protecting their identity and anonymity in any digital communications."

For Tor's part, hidden services are not going anywhere. Now dubbed "onion services" as part of a public-friendly rebranding, the technology is currently in the midst of a long-term security overall, including improved cryptography. The newer, more secure version is scheduled to land later this year. The marketing work is a longer haul as the team tries to separate Tor from the widespread boogieman that is the dark web. That effort will take much longer.

"I think you can have numbers about how many onion services exist, but I don't think it's easy to know what the onion services are," Lee said, citing anecdotes about technologist friends who use Tor hidden services for their own secure work. By the nature of it, you can't really gather data about it."

Tor watches certain key metrics about its network. There are about 2 million daily concurrent users and around 5,000 hidden services. But zeroing in on the exact use of the network is, by design, a difficult task. That's what makes it an anonymity network.

"I think [Lewman] does have a point," Lee said. "There is a lot of criminal use of it. I think there is also a lot of innocuous use. We just don't have the data to say what the percentages are."

-In this Story-

Dark net, dark web, Edward Snowden, Facebook, Farsight Security, FBI, Julian Assange, law enforcement, malware, Micah Lee, Norse, onion routing, Owl Cybersecurity, Tor

RELATED NEWS

TECHNOLOGY

Super-stealthy attackers...

by **Shaun Waterman** • 3 days ago

GOVERNMENT

Should the government...

by **Shaun Waterman** • 3 days ago

GOVERNMENT

Ransomware aimed at South...

by **Chris Bing** • 3 days ago