US mulls stiffer sentences for common Net proxies

April 14 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- "Proxy" servers are an everyday part of Internet surfing. But using one in a crime could soon lead to more time in the clink.

A key vote Wednesday on new federal sentencing guidelines would classify the use of proxies as evidence of "sophistication," increasing sentences by about 25 percent - which could mean years or even decades longer behind bars, depending on the crime. It's akin to judges handing down stiffer sentences when a gun is used in a robbery.

Yet digital-rights advocates are worried. Although they aren't absolving criminals, they complain that the proposal is so broad, it could lead to unnecessarily harsh sentences for tech neophytes who didn't know they were using proxies in the first place or who were simply engaging in a practice often encouraged as a safer way of using the Internet.

"It sends a bad message about protecting your own privacy," said John Morris, general counsel for the Center for Democracy and Technology. "This is the government saying, 'If you take normal steps to protect your privacy, we're going to view you as a more sophisticated criminal.'"

Proxies are computers that sit between a user and the Internet at large. They can be used to disguise that person's numeric Internet Protocol address, which is akin to a street address for a computer. Proxies are scattered around the Internet and are routinely used to relay Internet traffic, often unbeknownst to Internet users.

Corporations routinely use proxies to let their employees work from home; virtual private networks, or VPNs, make traffic look like it's coming from within the company's internal network, thus bypassing its security firewalls.

Cell phone providers use proxies to connect devices to the Internet, while people in repressive countries use them to circumvent Internet censors. Internet service providers also use proxies to speed traffic, by storing copies of frequently accessed Web pages locally, avoiding the need for users to reach out to the original site every time.

Privacy-minded users also rely on proxies to surf the Internet anonymously. With the free service Tor, for example, people install software to turn their computers into relay points for routing traffic between other people's computers. Thus, a Web site only knows the identity of the last relay point, not the user actually accessing it.

But such anonymity proxies can be used for both good and bad, and a debate is stirring as the government proposes to impose stiffer penalties for crimes committed by someone who had been using those and other proxies.

The U.S. Sentencing Commission is to vote Wednesday on a series of amendments to the sentencing guidelines, which heavily influence the sentences that judges hand down. The amendment in question would treat the use of proxies as evidence of "sophistication" in planning certain types of crimes, from embezzlement to forgery and other types of fraud.

If the commission approves it, the change takes effect Nov. 1 unless Congress takes the rare step of blocking it beforehand.

Opposing the change requires a delicate touch, because the rule would

apply only to people already convicted of crimes and facing sentencing.

"It's kind of a fine line we're dancing around, because we're not trying to coddle cybercriminals, but we also really don't think the government should be creating and institutionalizing a disincentive, a penalty for routine, safe privacy practices," Morris said.

The Justice Department pushed for the change as a way to exact a harsher punishment on criminals who set up extensive proxy networks in multiple countries to evade law enforcement. Investigators can spend months, if not years, unraveling the networks. Sometimes, it's impossible if they can't get cooperation from foreign governments.

Officials pointed to several recent cases that illustrate the complexity of investigations involving proxies.

One probe - into a spamming operation specializing in "pump and dump" schemes involving Chinese penny stocks - took three years to complete and resulted in the indictment of 11 people in federal court in Michigan last year.

Investigators said the defendants bought lists of known proxies and used them to send millions of pieces of spam e-mail, earning millions of dollars by selling the stock they were promoting at inflated prices.

Criminals often tap into legitimate proxies that are misconfigured. Businesses, universities and home users who own such proxies usually aren't aware their bandwidth is being sucked up by spammers or other criminals trying to hide their tracks.

A criminal could throw off an investigation by making traffic appear to come from a country with weak law enforcement. U.S. investigators could waste months trying to get cooperation only to hit a dead end - by

then, the criminal has long moved on.

"So much of the initial challenge in an investigation is determining attribution - where are the transmissions coming from?" Michael DuBose, chief of the computer crime and intellectual property section of the Justice Department's criminal division, said in an interview.

DuBose said the change is meant to punish people who knowingly use proxies to hide their identity and execute a criminal scheme.

But the current wording has been criticized as vague, and its opponents want a clearer statement of its application only to people who use proxies with criminal intent. Some also say that calling the use of proxies "sophisticated" is a stretch, given their ubiquity. The commission could change the language when it votes Wednesday.

"Even if someone did use a technology that made law enforcement's life harder, and even if they did have criminal intent, technologically it may not be sophisticated at all," Seth Schoen, staff technologist with the Electronic Frontier Foundation, a San Francisco-based nonprofit focused on online free speech and privacy. The EFF also helped fund development of the Tor anonymity proxy service.

"They're proposing to make a kind of judgment that this is something unusual or remarkable, which just doesn't match my experience with the technology. This is an everyday technology."

©2009 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: US mulls stiffer sentences for common Net proxies (2009, April 14) retrieved 26 April

2024 from https://phys.org/news/2009-04-mulls-stiffer-sentences-common-net.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.