Thinly Disguised New Law Designed to Target Hackers and Hacktivists

by staff report via jazq - Reuters *Saturday, Apr 4 2015, 9:38pm*
international / prose / post

U.S. targets 'overseas' cyber attackers with sanctions program

> *One of the first things kiddie hackers learn is how to direct the source of their attacks to other parties, known as 'spoofing' in the scene. Doing so is simplicity itself as the nature of digital traffic makes it virtually impossible to trace a professional hack. This is very well known even among fifth rate hackers that traitorously work for the State. This new law therefore allows governments to blame anyone they choose, another State, person, or entity, of illegal hacking. Everyone in the underground is aware of the ruse, however, the cardinal rule of anonymity maintains security, so those seeking notoriety like Julian Assange beware, fame is anathema to hackers. In view of the reality this absurdly broad new law is nothing more than an extension of police State oppression. Be aware!*

WASHINGTON (Reuters) - President Barack Obama launched a sanctions program on Wednesday to target individuals and groups outside the United States that use cyber attacks to threaten U.S. foreign policy, national security or economic stability.

In an executive order, Obama declared such activities a "national emergency" and allowed the U.S. Treasury Department to freeze assets and bar other financial transactions of entities engaged in destructive cyber attacks.

The executive order gave the administration the same sanctions tools it deploys to address other threats, including crises in the Middle East and Russia's aggression in Ukraine. Those tools are now available for a growing epidemic of cyber threats aimed at U.S. computer networks.

"The Obama administration is really getting serious now. This order brings to bear the economic might of the United States against people who are robbing us blind and putting us in danger," said Joel Brenner, who headed U.S. counterintelligence during President George W. Bush's second term.

The effort to toughen the response to hacking follows indictments of five Chinese military officers and the decision to "name and shame" North Korea for a high-profile attack on Sony. Officials said they hoped U.S. allies would follow suit.

China, which routinely denies accusations by U.S. investigators that hackers backed by the Chinese government have been behind attacks on U.S. companies, said cyber attacks were generally cross-border incidents with origins hard to track.

"China consistently does not approve of any one country using its domestic law to implement sanctions at every turn against the people or entities in another country," Chinese Foreign Ministry spokeswoman Hua Chunying told a daily news briefing.

Senior U.S. administration officials said the new program was focused on activities rather than countries or regions.

U.S. lawmakers and security and legal experts welcomed the move as an encouraging step after a

steady stream of cyber attacks aimed at Target, Home Depot and other retailers, as well as military networks.

But they said the executive order was surprisingly broad, which could result in a compliance nightmare for companies, and warned that it remained difficult to definitively "attribute" hacking attacks and identify those responsible.

Obama said in a statement that harming critical infrastructure, misappropriating funds, using trade secrets for competitive advantage and disrupting computer networks would trigger the penalties.

Companies that knowingly use stolen trade secrets to undermine the U.S. economy would also be targeted.

"From now on, we have the power to freeze their assets, make it harder for them to do business with U.S. companies, and limit their ability to profit from their misdeeds," Obama said.

The program was designed as a deterrent and punishment, filling a gap in U.S. cybersecurity efforts where diplomatic or law enforcement means were insufficient, Michael Daniel, Obama's cybersecurity adviser, told reporters. He said there was no timeline for determining an initial round of targets.

BIG BANG

Under the program, cyber attackers or those who conduct commercial espionage in cyberspace can be listed on the official sanctions list of specially designated nationals, a deterrent long sought by the cyber community.

"This sends a signal that the days of free-range hacking are over," said James Lewis, a cyber expert with the Center for Strategic and International Studies.

But Lewis said it would take time for the system of penalties to take hold. "People keep looking for a 'Big Bang' moment, but this will take years," he said.

John Reed Stark, a former head of Internet enforcement for the Securities and Exchange Commission, expressed skepticism, citing the high number of state-sponsored cyber attacks and the difficulty of identifying hackers.

Mark Rasch, a former Justice Department trial attorney and former executive with defense contractor SAIC, said the breadth of the order gave the executive branch vast new powers to respond to even routine criminal hacking.

Even denial-of-service attacks that knock websites offline with meaningless traffic, which can be orchestrated over the Internet for a few hundred dollars, could officially qualify for sanctions, he said.

If used widely, he said, the order could spell "a compliance nightmare for companies."

Representative Michael McCaul, chairman of the House Homeland Security Committee, said many questions remained about the administration's overall strategy, and what underlying definitions would be used to govern implementation of sanctions.

Dmitri Alperovitch, chief technology officer of Crowdstrike, a cybersecurity firm, said the order could have a "momentous" effect by preventing cyber criminals from spending the proceeds of their attacks, and closing off companies based in China and elsewhere from the U.S. financial market.

"If ABC Corp has had intellectual property stolen and then it's showing up in products of So and So Co of Shenzhen, you can tell them that it's been misappropriated and that their property in the U.S. is now subject to seizure," Brenner said.

Obama has moved cybersecurity toward the top of his 2015 agenda after recent breaches. Last month, the Central Intelligence Agency announced a major overhaul aimed in part at sharpening its focus on cyber operations.

(Additional reporting by Joseph Menn in San Francisco, Susan Heavey in Washington and Michael Martina in Beijing; Editing by David Storey, David Gregorio and Simon Cameron-Moore)

http://ca.reuters.com/article/technologyNews/idCAKBN0MS4DZ20150402
