PHYS.ORG

US mulls new tactics to stem wave of cyberattacks

November 6 2014, by Rob Lever

As hacking attacks reach epidemic proportions, the US cybersecurity community is looking at new ways to step up defense, including counterattacking the hackers themselves

As hacking attacks reach epidemic proportions, the US cybersecurity community is looking at new ways to step up defense, including counterattacking the hackers themselves.

US cybersecurity firms have begun unprecedented levels of cooperation to shore up America's key computer networks, and some experts argue in favor of "hacking back," or using offensive tools to improve defense.

Last month, dozens of cybersecurity firms and partners pooled resources in an effort to root out malware believed to originate from a Chinese state-sponsored group, dubbed Axiom.

"We wanted to make absolutely sure we did something that caused them some level of pain," said Zachary Hanif at iSight Partners, one of the cybersecurity firms involved in the operation.

Although the operation stopped short of "hacking back," the coordination aimed to "throw a large wrench into their engine," according to iSight's Brian Bartholomew, by coordinating defense to remove malicious software from and fortify defenses. The group cleaned up some 43,000 infections over two weeks.

Some experts argue tougher defense is not enough, and that some kind of offensive action is needed to halt the worst attacks in cyberspace.

Stewart Baker, a former assistant secretary of homeland security who now practices law in Washington, argues that limited "hacking back" could be justified, even though the legal issues are unclear.

Morally justified?

Baker said any actions a company takes outside its own network could be viewed as illegal, but there is a strong case to be made for reaching out to networks of third parties used by hackers to transit stolen data.

"I think you are morally justified for sure" in taking such actions, Baker told AFP. "And I think the probability of being prosecuted is very low."

Baker said if a firm can locate its stolen data and has a way to recover it, "they would be crazy not to."

"They can't wait for the government to get a court order. By the time that happened, everything is going to be gone."

But going beyond that, such as seeking to take out a hacker network, would mean "taking on risks" of legal liability.

US Justice Department guidelines caution against any retaliation.

Baker said the guidelines "don't quite say it's illegal, they say it's a bad idea."

A 2013 presidential commission report on intellectual property theft suggested some types of retaliatory actions should be legal.

"Without damaging the intruder's own network, companies that experience cyber-theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information," the report said.

American firms wrestle with legal and other implications of any type of cyber-retaliation.

"We have the capability to hack back," said Jody Denner, a cybersecurity and digital forensics consultant for Hewlett-Packard who has worked with government agencies and the corporate sector.

"The same open-source tools that are available to these state-sponsored groups are also available to everyone else."

Denner said he is aware of some "cyber-bandit" firms that will take offensive measures, keeping the matters quiet.

In the meantime, other governments are active on this front.

"The services of such 'mercenaries' are actively purchased by third-world governments like Pakistan and Nigeria," said Denis Makrushkin of the security firm Kaspersky.

'A lot like counterespionage'

Kristen Eichensehr, a national security law specialist at the University of California-Los Angeles and former State Department adviser, said private firms appear to be expanding their range of actions.

"The terms 'hacking back' or 'active defense' are used to describe a variety of actions ranging from planting fake data to 'beaconing' proprietary data so that it can be tracked if taken off a corporate network," she said on the Just Security blog.

"Depending on where on the spectrum a 'hacking back' action is, the private entity's actions could look a lot like counterespionage, law enforcement, or even military action."

The US military's Cyber Command charged with protecting the country's "critical infrastructure," which includes computer networks for finance, utilities and transportation, often gets blamed when there are gaps in cyber defenses.

Admiral Mike Rogers, who heads the Pentagon's Cyber Command as well as the National Security Agency, said recently the military is eyeing a policy of "deterrence," the same concept used for avoiding nuclear war.

Rogers said that as part of his role leading Cyber Command, he wants potential cyber-attackers to know there are consequences for their actions and that the US holds powerful weapons it can use.

But James Lewis, a cybersecurity specialist at the Center for Strategic and International Studies, said deterrence is unlikely to work.

"The idea of a deterrent effect is not plausible because you can't deter espionage and crime," Lewis said.

"What is the threat to get them to stop breaking into banks? There is no threat."

American officials are hesitant to carry out an offensive cyberattack "because what happens if they accidentally turn off the electricity at a hospital and kill a dozen people?"

With no easy answers, Lewis said improving cybersecurity will require not only better hardware, software and coordination, but diplomatic measures.

Citation: US mulls new tactics to stem wave of cyberattacks (2014, November 6) retrieved 11 May 2024 from https://phys.org/news/2014-11-mulls-tactics-stem-cyberattacks.html