Cybersecurity expert analyzes Anonymous' hacking attacks on ISIS

November 20 2015, by Bjorn Carey

Following tragic terrorist attacks committed by ISIS agents in Paris last week, the online hacker group Anonymous declared in a video that it would launch a cyber-attack on ISIS.

The masked Anonymous speaker in the video warns ISIS, in French, to be prepared for a massive retaliation.

The "hacktivist" group has been tangling with ISIS since it attacked the *Charlie Hebdo* magazine's office in Paris last January, taking over email and social media accounts, or crashing public Islamic State websites by overwhelming them with traffic. Anonymous members are already boasting that they have taken down ISIS-related websites and several thousand messaging or social media accounts.

Herbert Lin, senior research scholar for cyber policy and security at Stanford's Center for International Security and Cooperation and a research fellow at the Hoover Institution, says that Anonymous' activities against ISIS provide a useful nuisance to the terror group, but aren't quite legal under U.S. laws.

What types of attacks will Anonymous likely launch?

They don't have the capability to do the kind of things that a nation-state could do. The NSA, for instance, has the ability to place implants into hardware. Anonymous is more likely to engage in hacking that is less sophisticated. For example, ISIS almost certainly doesn't have a bank account that is coupled to the international banking system; they operate outside that particular channel. But they have lots of money, some of which may be stored in a personal- or business-like bank account. If so, that means that it can be hacked the same way that your bank account can be hacked, by cracking the username and password.

Similarly, Anonymous has been successful in the past at getting into ISIS members' email and messaging accounts, or taking down their Twitter feeds, which can disrupt their ability to coordinate terrorism-related activities; we can expect more in the future.

What kind of damage can Anonymous do to ISIS, and how effective will it be?

This approach clearly isn't the silver bullet that takes down ISIS, but attacking messaging abilities or bank accounts are useful harassing activities. Repairing these systems and accounts wastes ISIS's time and annoys them – the same way it does to you when your personal accounts are hacked. Having to untangle these messes can disrupt their overall operations, which is a perfectly good thing to do.

Do governments frown upon private citizens taking this type of action?

I think that the official line of the U.S. government on this is that it violates U.S. law for Anonymous to take on ISIS. It's vigilante justice in cyberspace, which is illegal under the Computer Fraud and Abuse Act. On the other hand, while the U.S. government might not be favorably disposed to it, I think it is unlikely that any prosecutor would actually indict an American for harassing ISIS in this way. And maybe the Anonymous hacker will uncover some information that is really useful to the U.S. government and be inclined to pass it along.

Provided by Stanford University

Citation: Cybersecurity expert analyzes Anonymous' hacking attacks on ISIS (2015, November 20) retrieved 25 April 2024 from https://phys.org/news/2015-11-cybersecurity-expert-anonymous-hacking-isis.html