GlobalResearch
Center for Research on Globalization

The White House's New Executive Order On Cyber Crime is (Unfortunately) No Joke

By Nadia Kayyali and Kurt Opsahl
Global Research, April 08, 2015
Electronic Frontier Foundation 6 April 2015

Region: USA
Theme: Law and Justice

On the morning of April 1st, the White House issued a new executive order (EO) that asserts that malicious "cyber-enabled activities" are a national threat, declares a national emergency, and establishes sanctions and other consequences for individuals and entities. While computer and information security is certainly very important, this EO could dangerously backfire, and chill the very security research that is necessary to protect people from malicious attacks.

We wish we could say it was a very well-orchestrated April Fool's joke, it appears the White House was serious. The order is yet another example of bad responses to very real security concerns. It comes at the same time as Congress is considering the White House's proposal for fundamentally flawed cybersecurity legislation.

That perhaps shouldn't be surprising, since so far, D.C.'s approach to cybersecurity hasn't encouraged better security through a better understanding of the threats we face (something security experts internationally have pointed out is necessary). Instead of encouraging critical security research into vulnerabilities, or creating a better way to disclose vulnerabilities, this order could actually discourage that research.

The most pernicious provision, Section 1(ii)(B), allows the Secretary of the Treasury, "in consultation with" the Attorney General and Secretary of State, to make a determination that an person or entity has "materially … provided … technological support for, or goods or services in support of any" of these malicious attacks.

While that may sound good on its face, the fact is that the order is dangerously overbroad. That's because tools that can be used for malicious attacks are also vital for defense. For example, penetration testing is the process of attempting to gain access to computer systems, without credentials like a username. It's a vital step in finding system vulnerabilities and fixing them before malicious attackers do. Security researchers often publish tools, and provide support for them, to help with this testing. Could the eo be used to issue sanctions against security researchers who make and distribute these tools? On its face, the answer is…maybe.

To be sure, President Obama has said that "this executive order [does not] target the legitimate cybersecurity research community or professionals who help companies improve their cybersecurity." But assurances like this are not enough. Essentially, with these words, Obama asks us to trust the Executive, without substantial oversight, to be able to make decisions about the property and rights of people who may not have much recourse once that decision has been made, and who may well not get prior notice before the hammer

comes down. Unfortunately, the Department of Justice has used anti-hacking laws far too aggressively to gain that trust.

As several security researchers who spoke up against similarly problematic terms in the Computer Fraud and Abuse Act recently pointed out in an amicus brief:

> There are relatively few sources of pressure to fix design defects, whether they be in wiring, websites, or cars. The government is not set up to test every possible product or website for defects before its release, nor should it be; in addition, those defects in electronic systems that might be uncovered by the government (for instance, during an unrelated investigation) are often not released, due to internal policies. Findings by industry groups are often kept quiet, under the assumption that such defects will never come to light—just as in Grimshaw (the Ford Pinto case). The part of society that consistently serves the public interest by finding and publicizing defects that will harm consumers is the external consumer safety research community, whether those defects be in consumer products or consumer websites.

It's clear that security researchers play an essential function. It was researchers (not the government) who discovered and conscientiously spread the news about Heartbleed, Shellshock, and POODLE, three major vulnerabilities discovered in 2014. Those researchers should not have to question whether or not they will be subject to sanctions.

To make matters worse, while most of the provisions specify that they apply to activity taking place outside of or mostly outside of the US, Section 1(ii)(B) has no such limitation. We have concerns about how the order applies to everyone. But this section also brings up constitutional due process concerns. That is, if it were to apply to people protected by the U.S. Constitution, it could violate the Fifth Amendment right to due process.

As we've had to point out repeatedly in the discussions about reforming the Computer Fraud and Abuse Act, unclear laws, prosecutorial (or in this case, Executive Branch) discretion, coupled with draconian penalties are not the answer to computer crime.

Articles by: **Nadia Kayyali**
and **Kurt Opsahl**