OFFENSIVE OR DEFENSIVE

Adam D. Tuchband

University of Advancing Technology

The security industry is prospering with new techniques for defensive and offensive hardware and software. Grand as it may be, the wide separation of people's knowledge and experiences in the industry leads to diverging opinions on many subjects. The beliefs for what people should do in security diverges further when politicians and security analysts meet. One widely used and debated security style is called Active Defense. The Active Cyber Defense Certainty Act (ACDC), a recently purposed bill, has been drafted to improve companies' security by making various concepts of Active Defense more available. The ACDC Act has people's ideologies split on allowing some ability to "hack-back," where the industry will grow, and the consequences of deploying these Active Defense tactics.

ACDC purposes amendments to 18 U.S.C. 1030 (also known as the Computer Fraud and Abuse Act). The most controversial change from the bill is a person's ability to "hack-back." ACDC permits victims of cybercrimes to access the attacker's system to gather information about who he is and destroy any information stolen from the victim's computer (Kulik, 2018). However, the victim is not allowed to destroy any other data that was originally on the computer (Kumar, 2017). In Garret Hawken's interview with the bill's main supporter, Tom Graves states "[t]his bill is about empowering individuals to defend themselves online, just as they have the legal authority to do during a physical assault." He also believes that this makes room for the industry to grow in a new direction where more tools are developed for individuals and industry, such as the safe and effective tools the FBI uses (O'Neill, 2017). For clarification, the term "Active Defense" has little agreed upon meaning, but hacking-back is one of the widely agreed on concepts in it (Jarko, 2016). Thus hacking-back will be the focus of this paper.

A few companies have already shown interest in doing Active Defense in the industry. SANS Institute has developed a course dedicated to teaching Active Defense and the offensive

techniques it entails (Strand); Ey.com provides an active defense service to protect companies; and “Active Defense,” by VioPoint, is a program that was made to service the Active Cyber Defense industry. These three groups are evidence that people have taken note of their ability to use Active Defense and already created a business with it. However, they currently do not have jurisdiction to implement hack-back without permission from the attacker. Companies have already started the development of tools for active defense; Tom Graves has ample material proving the industry’s interest.

Despite the clear interest towards Active Defense from various groups and businesses, not everyone believes that the ACDC act is in the security industry’s best interest. Even though ACDC may increase the cyber attack conviction rate to above 1.5 percent (O’Neill, 2017), many writers in the cybersecurity industry do not see enough benefit to outweigh the problems that would arise from the bill. One purpose of the purposed bill is to help victims find the people who attacked. Attackers have many methods of masking where they came from, such as the use of a proxy server, allowing the attacker to easily hide from attribution. Therefore, people are understandably worried about innocent people getting hacked by a company. The attacker could have redirected the victim to a different computer, or the company’s defensive team could accidentally go after the wrong individual (Dittrich 2017; Kumar, 2017; Myers, 2013). If a company wants a hack-back Active Defense team, they would likely need to specialize these individuals in training, as most organizations do not currently have the staff and it is a specific part of the field few people currently know. Companies do not always have data that needs to be recovered or kept secret. Assuming it is needed at all, the transparency would make this task part-time, resulting in the already employed individuals taking the responsibility. The work that has to be put into hacking-back, as well as completing the regular tasks is currently unfeasible

for a company to consistently succeed in doing (Kulik, 2018).

The concept of Active Defense is not a clear one for anybody who is attempting to learn about it, either. Wikipedia has a page on what it calls “Proactive cyber defense.” In every section of this page, “Proactive” was never in the term used, but Wikipedia clarified an alternative name “active cyber defense” and “active defense” in the first sentence. The Wikipedia article emphasizes the military science throughout the article, attaching military roots to active defense since they were one of the first groups to implement the defense procedure. The section about the current status of active defense is describing outdated information about information warfare and marketing techniques. The most recent year in the section is 2008, which is not what was researched in this essay. However, the age may explain use of “Proactive cyber defense,” rather than “Active Cyber Defense.” In the final section, the article describes the government’s actions, as they relate to active security. The commonplace use of Active Defense Security is hardly touched on. Conversely, information is not out of date in the final section; it is describing the government’s use of “zero-day vulnerabilities,” which are offensive exploits, not defensive software nor techniques. Lastly, the article details proactive, pre-emptive operations of the government, however, the section describes more attacks effecting prevention. These points remove the description of defense, thus losing the modern day credibility to “active defense” by most people’s definitions.

The industry is divided by how to act in defense of its data, even though everyone has the same end goal. Many journalists will write anger pieces on this subject, when they do not fully know the changes that ACDC will enact, such as not destroying the attacker’s data. Others do not want the bill simply because it does not resolve all of the security world’s problems. Security is meant to protect data, but no method is an ultimate, bullet-proof method. Security experts will

attempt to prevent damage, and they will repair as problems happen. Whether or not this bill passes, what people design for security is meant to keep individuals and their companies safe.

Bibliography

Dittrich, D. (2017, June 16). Thoughts on the Active Cyber Defense Certainty Act 2.0. Retrieved March 11, 2018, from https://medium.com/@dave.dittrich/thoughts-on-the-active-cyber-defense-certainty-act-2-0-d0b456a56d8b

Hawkins G. (2017, March 5). Rep. Tom Graves Proposes Cyber Self Defense Bill. Retrieved March 24, 2018, from http://www.thedallasnewera.com/local-news/1657-rep-tom-graves-proposes-cyber-self-defense-bill.

Jarko, C. (2016, February 6). Finding the Fine Line-Taking an Active Defense Posture in Cyberspace without Breaking the Law or Ruining an Enterprise's Reputation. Retrieved March 11, 2018, from https://www.sans.org/reading-room/whitepapers/legal/finding-fine-line-%E2%80%93-active-defense-posture-cyberspace-breaking-law-36807

Kulik, T. (2018, January 29). Why The Active Cyber Defense Certainty Act Is A Bad Idea. Retrieved March 11, 2018, from https://abovethelaw.com/2018/01/why-the-active-cyber-defense-certainty-act-is-a-bad-idea/?rf=1

Kumar, M. (2017, March 08). Proposed Bill Would Legally Allow Cyber Crime Victims to Hack Back. Retrieved February 22, 2018, from https://thehackernews.com/2017/03/hacking-back-hackers.html

Myers, L. (2013, November 19). Active Defense: Good protection doesn't need to be offensive.

Retrieved March 11, 2018, from https://www.welivesecurity.com/2013/11/19/active-defense-good-protection-doesnt-need-to-be-offensive/

O'Neill, P. H. (2017, November 27). Rep. Tom Graves: 'Hack back' bill will launch a new industry. Retrieved March 11, 2018, from https://www.cyberscoop.com/tom-graves-active-defense-hack-back-bill-new-industry/

Proactive Cyber Defence. (2018, January 8). Retrieved March 11, 2018, from https://en.wikipedia.org/wiki/Proactive_cyber_defence

Strand, J. (n.d.). SEC550: Active Defense, Offensive Countermeasures and Cyber Deception. Retrieved March 10, 2018, from https://www.sans.org/course/active-defense-offensive-countermeasures-and-cyber-deception

Text - H.R.4036 - 115th Congress (2017-2018): Active Cyber Defense Certainty Act. (2017, November 1). Retrieved March 10, 2018, from https://www.congress.gov/bill/115th-congress/house-bill/4036/text

18 U.S. Code § 1030 - Fraud and related activity in connection with computers. (n.d.). Retrieved March 10, 2018, from https://www.law.cornell.edu/uscode/text/18/1030