https://www.itchronicles.com/security/understanding-the-active-cyber-defense-certainty-act-should-companies-be-allowed-to-hack-back/

Understanding the Active Cyber Defense Certainty Act – Should Companies Be Allowed to "Hack Back"?

Posted 9 months ago by Carlos Casanova
AddThis Sharing Buttons
Share to Twitter
Share to FacebookShare to LinkedInShare to PrintShare to EmailShare to More
Next Story

Venafi: Bringing Identity and Access Management (IAM) to Machines

Question: Should companies and computer users in the US be able to strike back actively against hackers? Until very recently, to do so would have been a risky strategy in legal terms. The Computer Fraud and Abuse Act (CFAA) of 1986 specifically prohibits individuals form taking retaliatory or defensive actions against cybercriminals, aside from standard preventative measures such as by using anti-virus or anti-malware software. But, with the proposal of the Active Cyber Defense Certainty Act (ACDC), individuals and companies would be able to "hack back" when their information is stolen or their system is breached.

It's a controversial proposal to say the least. Though the main idea behind the Active Cyber Defense Certainty Act is to enable those who have been hacked to defend themselves in an offensive manner, there are many commentators who suggest that letting companies and individuals hack back without the proper oversight will do more harm than good.

We'll drill down deeper into the controversies later. First, let's get our heads around exactly what the Active Cyber Defense Certainty Act is.

What Is the Active Cyber Defense Certainty Act?

The Active Cyber Defense Certainty Act was introduced to Congress by Rep. Tom Graves (R-Ga) and Rep. Kyrsten Sinema (D-Ariz.) in March 2017 (updated in October 2017) as legislation that would give companies and individuals the right to strike back after a "persistent unauthorized intrusion." The legislation is designed to extend the powers of cyberattack victims beyond the limits imposed by the CFAA.

At its core, the CFAA prohibits the intentional accessing of a computer without authorization and obtaining information from a protected computer involving interstate or foreign communications. As such, any “hack back” by a corporate victim of a cyberattack is prohibited under the CFAA.

But the Active Cyber Defense Certainty Act would lift this restriction, allowing a company to implement active cyber defense measures to not only identify the attackers, but even destroy information originally stolen from their network.

For Rep. Tom Graves, it is a necessary tool for companies to protect their valuable information assets. “While it doesn’t solve every problem, ACDC brings some light into the dark places where cybercriminals operate,” said Graves following the October 2017 update. “The certainty the bill provides will empower individuals and companies to use new defenses against cybercriminals. I also hope it spurs a new generation of tools and methods to level the lopsided cyber battlefield, if not give an edge to cyber defenders. We must continue working toward the day when it’s the norm – not the exception – for criminal hackers to be identified and prosecuted.”

Specifically, under the Active Cyber Defense Certainty Act, a cyberattack victim (or “defender”, to use the bill’s terminology) would be able to access “without authorization the computer of the attacker to the defender’s own network to gather information in order to”:

- Establish attribution (i.e. the nature, cause and source) of criminal activity to share with law enforcement and other US Government agencies responsible for cybersecurity
- Disrupt continued unauthorized activity against the defender’s own network (though without damaging the computer systems of the presumed attacker or anyone else)
- Retrieve and destroy any stolen data
- Monitor the behavior of an attacker to assist in developing future cyber defense techniques
- Use beaconing technology

In terms of cybersecurity, a beacon is a piece of software or a link that has been hidden in a file and can send information back to a defender with details about the structure and location of the attacker’s computer system.

Essentially, within this framework, companies and individuals will be authorized to take a more active role in cyber defense by using and developing tools which are currently restricted under the CFAA.

Controversy – ACDC, A Highway to Hell?

On the surface, the Active Cyber Defense Certainty Act allows a victim to identify an attacker, work with law enforcement to stop further intrusion, and retrieve any stolen data. All good things, right?

Well, many in the cybersecurity community aren’t so sure – after all, isn’t hacking back essentially fighting fire with fire?

Some say it is. And they also warn that the danger with hacking back is that uninformed companies typically won't have well-defined strategies or methods for their actions. As such, it's questionable what hacking back would actually achieve. Let's consider the main concerns being expressed by the cybersecurity community over the Active Cyber Defense Certainty Act.

Difficulty Determining a "Persistent Unauthorized Intrusion"

If hacking back were to become legal, an organization would have to prove that an attacker "persistently" attacked a network *before* it took action. This isn't straightforward. Attribution is extremely challenging, with traffic or commands that may appear to come from one source but in fact originate elsewhere. Organizations would first have to positively identify the attacker, pinpoint the location of its information, and retrieve it without causing harm. It would then have to notify the FBI before hacking back.

Difficulty Accurately Targeting Hackers

Hackers often hide behind third-party "zombie" computers or launch attacks from servers that don't belong to them. This means that a hack back could result in the intrusion of an innocent victim's server. This becomes a particularly tricky issue with the rise of Internet of Things (IoT), where multiple devices are often used to launch a cyberattack. If these devices were hacked back, their owners would then become innocent victims of the retaliation – and the original defender would essentially become an attacker.

Compromising Investigations and Evidence

This is a big issue. A private company's counter-hacking activities may interfere with official investigations and potentially damage investigations. The draft bill is supposed to be designed to enable victims to work together with law enforcement. However, if key evidence becomes compromised in a way that renders it inaccessible to a court as a result of hacking back, will the Active Cyber Defense Certainty Act have any real use at all?

The Active Cyber Defense Certainty Act Only Would Only Be Legal in US

The ACDC only legalizes hacking back against attackers in the US. If a company used counter-hacking techniques against an attacker in another nation, it could be breaking local laws.

Final Thoughts – Should Companies Be Allowed to Hack Back?

Data theft and the threat of cyberattacks today are massive concerns to organizations of all shapes and sizes. The Active Cyber Defense Certainty Act raises some important issues that the law could and should do more to protect individuals and companies from attackers. However, for many in the cybersecurity community, the risks of hacking back far outweigh the benefits.

The trouble is that most organizations lack the skills, basic tools, and defense mechanisms to conduct a counter-hack with the precision that would be required to keep things legal and not cause any further harm. Hack backs could hinder investigations, cost organizations time and money, and potentially put the devices of innocent victims of botnet attacks at risk. While organizations should have the support, rights and permission to defend themselves from cyberattacks, for many, the solutions proposed in the Active Cyber Defense Certainty Act aren't as water-tight as they need to be.

The following two tabs change content below.

- Bio
- Latest Posts

Carlos Casanova

Carlos Casanova is an internationally known speaker, IT architect, leadership advisor and the co-author of "The CMDB Imperative". He has over two decades of hands on experience guiding CIOs and Sr. Leadership to achieve effective IT operations and improve ROI from infrastructure investments. His expansive experience enables him to quickly assess their true needs and achieve better business outcomes. He takes the complexity out of today's cluttered IT and business environments to simplify their goals in order to accelerate achievement and success.