Related Posts

malwaretech.com/2021/11/an-in-depth-look-at-hacking-back-active-defense-and-cyber-letters-of-marque.html

MalwareTech

November 17, 2021

There has been much discussion in cyber security about the possibility of enabling the private sector to engage in active cyber defense, or colloquially “hacking back”. Several house bills have been introduced to study or enable this, such as the “Study on Cyber-Attack Response Options Act” and “Active Cyber Defense Certainty Act”.

What is hacking back?

Hacking back is an umbrella term for various proposed exceptions to the Computer Fraud and Abuse Act (CFAA), which is the United States’ main law against computer hacking. These exceptions would allow security experts to engage in retaliatory hacking against criminal actors, for purposes such as attribution or disruption.

Whilst the Active Cyber Defense Certainty (ACDC) Act is highly specific, the more general discussion extends far beyond its’ bounds. Opinions range from allowing limited intrusions within a pre-approved scope, to an all-out free-for-all with no prior approval or oversight. More recently, there have been several opinion pieces calling for “cyber letters of marque” allowing security professionals to engage in privateering.

The main provisions of the ACDC act enable defenders to engage in hacking against attacker-controlled infrastructure for the following purposes:

1. Attribution of attackers
2. Disrupting attacks against the victim’s network
3. Recovering or destroying stolen victim data
4. Learning about attacker behavior for purposes of building better defenses

At the core of all these beliefs is that by leveling the playing field, defenders could better respond to intrusions and deter attacks.

Prominent Issues with active cyber defense

Prosecution

The ACDC Act uses the language “as a defense to prosecution”, which implies it does not prevent charging or prosecution, but simply acts as a potential defense at trial. This would be similar to how self-defense may not stop you being arrested and charged, only potentially avoid conviction.

Statistically only about 5% of federal cases even make it to trial. Cybercrime cases often spend years in the pretrial phase and can cost upwards of one million dollars in legal fees. Furthermore, prosecutors offer significantly lower punishments for defendants who plead guilty. It’s often better for defendants to accept a certainty, rather than leave their fate in the hands of 12 random citizens. The combination of time, cost, risk, and emotional burden leads to many innocent defendants pleading guilty to avoid trial.

The ACDC act also specifically states that it is not a defense to civil action, which could lead to a whole host of problems. For example, victims prevented from paying ransomware ransoms due to ACDC enabled disruptions could sue disruptors to recover losses. Damages could also be sought by ISPs hosting attacker infrastructure, other active defenders, or even threat actors themselves.

Given the global nature of the internet, bills such as the ACDC act would also offer no protection against international law. If active defenders intrude into foreign systems, or US systems owned by foreign companies, they may still find themselves in hot water.

Whilst many large companies can afford to bankroll legal defenses and shield employees from direct prosecution, small firms, contractors, and individuals would not be so lucky. Overall the act offers flimsy protections, and would simply be handing more powers to large corporations who can afford lengthy court proceedings.

Conflicts of interest

Whilst risk of prosecution may be mitigated by the ACDC act’s requirement of advanced approval from the Department of Justice (DOJ), this gives rise to a major conflict of interest.

Law enforcement’s goal is to gather intelligence with the intention of arresting perpetrators, which means monitoring attackers as quietly as possible. Law enforcement operations can take many months or years to complete and whilst they may be of little help to victims in the short term, the arrest of key players can prevent many further attacks.

On the other hand, uncoordinated active defense is a much shorter sighted goal. Many defenders will be looking to disrupt individual attacks against their clients at the expense of long-term intelligence gathering. Whilst disruption can be good, it also forces attackers to evolve and adapt, making further monitoring and disruption more difficult.

Any disruption against attacker systems is certain to alert the attackers to a breach. Even passive intelligence collection for identification purposes is not guaranteed to go unnoticed. The more intrusions into an attacker system, the more likely attackers are to notice. With no way of coordinating and synchronizing access across private industry and government at scale, the risk of discovery is extremely high.

It will likely be in law enforcement’s best interest to simply deny all active defense requests, as they pose a direct threat to their primary mission. The suggested notification process would not be enough to mitigate such risks, and anything short of direct oversight is doomed to fail.

Perverse Incentives & deconfliction

Bills such as the ACDC act would create a lucrative new market, allowing security testing companies to offer services acting as cyber-mercenaries on behalf of attack victims. Whilst many hacking skills translate well to active cyber defense, they do not provide the whole picture.

Active cyber defense introduces new variables such as the need for deconfliction to avoid damaging operations other than one’s own. Active defenders would need to tread carefully to also avoid disrupting both domestic and foreign military or intelligence operations. The sensitive nature of such operations means that without strong ties to the military and intelligence community, this will be nigh-impossible. Furthermore, a combination of varying objectives and financial incentive may mean there is little desire to even attempt deconfliction from the perspective of private industry.

Some considerations when accessing attacker-controlled infrastructure are:

1. Am I at risk of polluting or destroying logs, making it harder for others to discern actual attackers from friendly intruders?
2. Is this infrastructure attacker owned? Am I sure it’s not a compromised system, an IP address that has since changed hands, a proxy, false flag, or currently under the control of law enforcement?

3. Could my activities result in negative changes in attacker behavior, such as increased aggression in order to recuperate losses?
4. Am I at risk of doing something that could lead to discovery, burning access for everyone or resulting in attacker retaliation?
5. Am I even likely to gain anything novel and objectively beneficial from this intrusion?
6. Is it likely that nobody is already quietly doing what I intend to do (attributing attacks, alerting victims, improving security guidance based on attacker behavior, disrupting intrusions)?

Things get extremely messy when you have potentially hundreds of defenders all trying to make these same determinations, based on their varying insight and goals, with little to no coordination between each other. It will fast become a scenario of far too many cooks.

It already exists

Whilst not anyone can just pick up a laptop and start throwing hands at the nearest threat actor, active defense is already commonplace. Law enforcement already possess abilities to grant legal protections to private individuals or companies assisting with operations.

Botnet takedowns, like the recent action against Emotet, are just one example of private industry engaging in active defense.

The Emotet takedown was a highly coordinated operation involving individual researchers, private companies, and law enforcement agencies spanning nine countries. The operation was spearheaded by law enforcement to avoid duplicate or conflicting operations, but leaned heavily on the capabilities of private industry. The synergy between private sector and government allowed for a multifaceted approach, causing maximum impact. The action involved a complete takeover of the botnet, shutting down distribution channels and actor infrastructure, as well as simultaneous law enforcement raids aimed at hindering future reconstruction.

Despite years of planning, and being one of the largest public/private sector operations ever conducted, the Emotet takedown resulted in only ten months of downtime. Now, a ten month outage is no small feat. The operation was a huge success and likely averted billions of dollars in damage. But, this goes to show that even the most well planned and well-executed operation can only do so much. We need to focus on strong conventional defenses to complement existing active defense, rather than create a digital wild west of cyber mercenaries. The last thing we need is large coordinated operations being disrupted by handfuls of poorly thought out attacks, which serve as only a minor nuisance to threat actors.

Is it necessary for private industry to engage in active defense?

Perhaps most telling is the fact that not a single person I spoke to in law enforcement, military, intelligence, or cyber threat intelligence thought such legislation was a good idea. Much of the support came from other parts of the industry where hacking prowess is common, but experience dealing with real world threat actors is extremely rare.

It’s my belief that much of the push for active cyber defense was born out of a growing frustration with the constantly increasing volume and severity of cyberattacks. Many believe that enough isn’t being done to combat them, but why is that? And does active cyber defense solve this problem?

The immunity window

Currently there exists a major blind spot in the government’s ability to respond to cyberattacks. Law enforcement deal with cybercrime within their jurisdiction, meanwhile the military and intelligence community target hostile state actors and other national security threats. But what happens when a threat actor falls into neither category?

The immunity window exists when a threat actor is shielded from law enforcement by their home nation; however, they do not meet the threshold for classification as either a state actor or a national security threat. This is the sweet spot in which many ransomware actors operate.

Ransomware actors residing in countries unfriendly toward the US may find themselves immune to prosecution, so long as they do not target their home nation or its allies. Whilst ransomware actors who pose a clear and present threat to public safety may find themselves in the crosshairs of Cyber Command Et. al., until then they are essentially free to operate with impunity.

Allowing private industry to engage in active cyber defense admittedly could close this window, albeit at a great cost. Such activities would jeopardize operations against threat actors already within reach of the US government, cancelling out any potential benefit. Active cyber defense may also be seen as an act of aggression by the host nations, leading to escalation and the potential of state backed retaliation against US private industry.

Future discussion

An ideal solution should aim to close the immunity window without detriment to law enforcement, military, or intelligence operations, and ideally without drastically increasing the reach of such agencies. Whilst active cyber defense by private industry should not be a solution in and of itself, there may be some situations in which it could be of use as a last resort; however, this should only be done under direct governmental oversight.

For now, I leave this open as I work on a follow up piece. Congratulations are in order if you made it this far.