RAPID

Rapid7 Position on Private Sector Hack Back

April 2017, updated in June 2021

As cyber attacks against the private sector continue to proliferate, many organizations feel powerless to balance the scales between themselves and attackers. Some of these organizations are seeking ways of discouraging attacks beyond the more traditional defensive activity to protect themselves. Whether organizations are aiming to deter and disrupt attacks in progress, find ways to retrieve stolen information, or better identify and prosecute their attackers, many of the actions they are pushing for fall under the category of private sector hack back. This paper documents Rapid7's position on private sector hack back, which we believe cannot work in practice without causing unintended harm, escalating aggression, and creating legal liability confusion and risk.

Background

Definition and nomenclature

For the purposes of this document, we understand 'hack back' to mean an organization taking intrusive action against a cyber-attacker on technical assets or systems not owned or leased by the person taking action or their client. The action may be taken to neutralise the threat, recapture lost data, better understand the nature of the attack, or as an act of revenge. We do not include hacking activities undertaken by, or on behalf of, the government in this classification, only those undertaken specifically by private sector entities. We also do not include mere scanning of connected assets, which is neither intrusive nor disruptive.

Hack back activities may be described under threat hunting, threat intelligence, or detection and response activities. It is sometimes referred to as 'Active Defense' or 'Active Cyber Defense'; however, this can cause confusion as these terms can also refer to a range of other defensive measures. For example, the UK government uses the term 'Active Cyber Defence' to refer to a range of defensive security services and tools it provides.¹ More broadly, Active Defense covers activities ranging from defensive measures to stop people getting in - e.g. intrusion prevention systems - to deception technologies designed to confuse attackers and gain greater intelligence on them, e.g. honeypots.

¹ <u>https://www.ncsc.gov.uk/section/products-services/active-cyber-defence</u>

Rapid7 encourages organizations to employ active defense techniques within their own environments.

Legal status

Since hack back activities revolve around taking an action on a third party asset without consent of the asset owner, they are generally illegal in countries with anti-hacking laws, including the United States² and the other 5 Eyes nations. Advocates for hack back maintain that existing anti-hacking laws should be modified to create an exemption for private sector organizations to take intrusive action to better understand their attackers,³ retrieve or track stolen data, or to prevent crime.⁴

Today, operations to investigate attackers, or deter or disrupt attacks are undertaken by law enforcement or government agencies under an oversight framework that includes strong evidentiary requirements and leverages robust intelligence networks and investigative processes. Private sector entities may participate in these operations in partnership with the government entity and under their oversight.

Rapid7's position

As stated above, Rapid7 does not believe hack back can work in practice without causing unintended harms, legal confusion, and liability complexity. We strongly urge policymakers not to authorize private sector hack back. Below we have detailed our concerns.

Impracticalities of attribution and application

One of the most widely stated and agreed upon tenets in security is that "attribution is hard." We can go further – in many cases, it is essentially impossible to know for certain that we have accurately attributed an attack. Even when we find indications that point in a certain direction, it is very difficult to ensure they are not red herrings intentionally planted by the attacker to either throw suspicion off themselves, or to specifically incriminate another party for some purpose. We like to talk about "digital fingerprints," but the reality is that there is no such thing: in the digital world there is nothing that cannot be spoofed or obfuscated with enough time, patience, skill, and resources. Attackers are constantly evolving their techniques to stay one step ahead of defenders and law enforcement, and the emergence of deception capabilities is just one example of this. So being certain we have the right actor before we take action is extremely difficult.

In addition, where do we draw the line in determining whether an actor or computing entity could be considered a viable target? For example, if someone is under attack from devices that are being controlled as part of a botnet, those devices – and their owners – are as much victims of the attacker

² <u>https://www.law.cornell.edu/uscode/text/18/1030</u>

³ https://www.congress.gov/bill/116th-congress/house-bill/3270/text

⁴ <u>https://www.cyberupcampaign.com/</u>

as the target of the attack. Rapid7's Project Heisenberg⁵ observes exactly this phenomenon; the honeypots often pick up traffic from legitimate organizations whose systems have been compromised and leveraged in malicious activity⁶. Should one of these compromised systems be used to attack an organization, and that organization then take action against those affected systems to neutralise the threat against themselves, that would mean the organization defending itself was revictimizing the entity whose systems were already compromised. Depending on the nature of the action taken, this could end up being catastrophic and costly for both organizations.

Motivations, which are often unclear or easy to misunderstand, should surely also be taken into account. For example, research projects that scan ports on the public-facing internet do so in order to help others understand the attack surface so exposure and opportunities for attackers can be reduced. This activity is benign and often results in security disclosures that have helped security professionals reduce their organization's risk. However, it is not unusual for these scans to encounter a perimeter monitoring tool, throwing up an alert to the security team. If an organization saw the alerts and in their urgency to defend themselves, took a "shoot first and ask questions later" approach, they could end up attacking the researcher.

Impracticalities of limiting reach and impact

The internet does not operate in neatly defined and clearly demarcated boundaries. If we take action targeted at a specific actor or group of actors, it would be extremely challenging to ensure that action taken will not unintentionally negatively impact innocent others. Many people have likened hack back to the idea of a homeowner defending their property against an intruder. They evoke images of malicious, armed intruders breaking into your home to do you and your loved ones harm. They call to you to arm yourself and stand bravely in defense, refusing to be a victim in your own home. It's an appealing idea; however, the reality is more likely to be akin to standing by your fence spraying bullets out into the street hoping to get lucky and stop an attacker as they flee the scene of the crime. With such an approach, even if you do manage to reach your attacker, you are recklessly risking terrible collateral damage too.

Rapid7 believes the possibility of unintended consequences should not only concern lawmakers, they should also disincentivize participation. Organizations that believe they can avoid negative outcomes in the majority of cases need to understand that even just one or two errors could be extremely costly. Imagine for example that a high-value target organization, e.g. a bank, undertakes 100 hack backs per year and makes a negatively impactful error on two occasions. A two percent fail rate may not seem that terrible; however, if either or both of those errors resulted in compromise of another company or harm to a group of individuals, the hack-backer could then see themselves tied up in expensive legal

⁵ https://www.rapid7.com/research/project-heisenberg/

⁶ https://www.rapid7.com/c/2018-ICER-Fortune-500/

proceedings, reputational damage, and loss of trust. Attempts to make organizations exempt from this kind of legal action are problematic as it raises the question of how we can spot and stop abuses.

The potential negative consequences of a hack back gone awry could be far reaching. We frequently discuss damage to equipment or systems, or loss of data, but in the age of the Internet of Things, there is always the potential that negative consequences could include physical harm to individuals. And let's not forget that cyberattacks can be considered acts of war.

Impracticalities of providing appropriate oversight

To date, proposals to legalize hack back have been overly broad and non-specific about how such activities should be managed, and what oversight would be required to ensure there are no abuses of the system. Advocates have proposed a licensing system whereby actors would be vetted and authorized to conduct hack back activities, and some advocates have pointed to the example of how privateers were issued Letters of Marque⁷ to capture enemy ships - and their associated spoils. Putting aside fundamental concerns that we are taking as our standard a 200 year-old law passed during a time of prolonged kinetic war and effectively legalizing piracy, there are a number of pragmatic issues with how this would work in practice.

Indeed, creating a framework and system for such oversight is highly impractical and costly, with many issues that would need to be addressed. The government would need to determine basic administrative issues such as who would run it and how it would be funded, and it would need to identify a path to addressing far more complex issues around accountability and oversight to avoid abuses. For example, it would need to address who will determine where the line should be on what action is acceptable, and how an authorizing agent would ensure standards are met and maintained within approved organizations. Existing cybersecurity certification and accreditation schemes have long raised concerns,⁸ and this will only be worsened when certification results in increased authorities for activities that can result in significant harm and escalation of aggressions on the internet. An authorizing agent cannot have eyes everywhere and at all times, so guaranteeing standards are maintained and there are no accidental or intentional abuses of the system is not practical. These issues of real-world execution also raise questions around who will bear the responsibility and liability if something goes wrong.

As mentioned above, when a government takes action against attackers, it is with a high degree of oversight and accountability. They must meet evidentiary standards to prove the action is appropriate, and even when that has been done, there are parameters determining the types of targets that can be pursued, and the kind of action that can be taken. Authorizing the private sector to participate in these

⁷ https://www.csiac.org/journal-article/rebooting-letters-of-marque/

⁸ https://www.theregister.com/2021/05/17/crest_not_publishing_cert_exam_cheat_report/

activities without this oversight undermines the checks and balances in place for the government and is likely to lead to unintended harms.

Impracticalities of legal liability and jurisdiction

While the internet is a borderless space accessed from every country in the world, each of those countries has its own legal system and expects its citizens to abide by it. It would be very risky for companies and individuals who hack back to avoid running afoul of the laws of another country and international law.

When national governments take this kind of action, it tends to occur within existing international legal frameworks and under some regulatory oversight, but this may not apply in the private sector, begging the question of where the liability rests. For example, if a company hacks back and accidentally harms another company or individual, the entity that undertook the hacking may incur expensive legal proceedings, reputational damage, and loss of trust. They could become embroiled in complicated and expensive multi-jurisdiction legal proceedings, even if the company is provided a license to hack back in its home jurisdiction. In scenarios where hack back activities are undertaken by an organization or individual on behalf of a third party, both the agent and their client may bear these negative consequences. There may also be an argument that any licensing authority could also bear some of the liability.

Making organizations exempt from this kind of legal action around unintended consequences is problematic. For example, it would be highly impractical to create a system for oversight that would enable the governing authority to spot and stop accidental or intentional abuses of the system in real time. It would be imperative for the government to develop and maintain a process for vetting organizations, as well as deterring, identifying, and halting accidental or intentional abuses of the system. This would be costly and unlikely to succeed in practice as it would be very impractical for governments to have adequate visibility to apply effective oversight.

It is also worth noting that once one major power authorizes private sector hack back, other governments will likely follow and legal expectations or boundaries may vary. This raises questions of how governments will respond when their citizens are being attacked as part of a private sector hack back gone wrong, and whether it will likely lead to escalation of political tensions.

Inequalities of applicability

Should a viable system be developed, and hack back authorized, effective participation is likely to be costly as it will require specialist skills. Not every organization will be able to participate. If the authorization framework is not stringent, many organizations may try to participate with insufficient expertise, which is likely to be either ineffective or damaging, or potentially both. However, there are other organizations that will not have the maturity or budget to participate even in this way.



These are the same organizations that sit below the "cybersecurity poverty line"⁹ and cannot afford a great deal of in-house security expertise and technologies to protect themselves – in other words, these organizations are already highly vulnerable. As organizations that do have sufficient resources start to hack back, the cost of attacking these organizations will increase. Profit-motivated attackers will eventually shift towards targeting the less-resourced organizations that reside below the security poverty line. Rather than authorizing a measure as fraught with risk as hack back, we should instead be thinking about how we better protect these vulnerable organizations, for example, by subsidising or incentivizing security hygiene.

Responses to Justifications for Hacking Back

As stated above, a number of justifications or goals are cited for hacking back. Rapid7 does not believe any represent a valid argument for authorizing hack back, as detailed below:

"Track the attackers" - This is a fairly broad term and could relate to a number of activities, including beaconing, "interrogating" assets, and viewing metadata. The scope for unintended consequences depends on which specific activities are being recommended, but in general, implanting code or penetrating third party assets should be viewed as potentially harmful for all the reasons stated above. There is a great deal of scope for this to result in escalation of activity, re-victimizing victims, or unintended harm.

There is also a privacy aspect here; many countries have laws to protect access to personal, sensitive, or confidential data. Authorizing activity that interrogates third party assets used in attacks could contradict the spirit of these laws and violate the privacy of other victims of the attacker.

"Get data back that was stolen" - We do not believe this is practical as there is no way to know if the first hop point that the data was exfiltrated to is actually its final destination. Again, implanting beacons to follow the data raises the issues outlined above. There is also no way to know if the data was already copied and moved somewhere else.

"Stop attacks in progress" - On the surface, this sounds appealing and reasonable. In reality though, there are many more fundamental defensive measures organizations should take to stop attacks, and today we see widespread misapplication or lack of adoption of these measures. This does not bode well for the private sector taking more intrusive action and executing without issues, such as the aforementioned misattribution, escalation, or unintended harm. It also sets a strange tone and expectation, as if saying that it is reasonable for people to lay mines around their property to deter intruders when they have not even closed their doors and windows. Stopping attackers with more offensive activities is the domain of governments, applied with oversight and within an international legal framework.

⁹ https://duo.com/blog/rising-above-the-security-poverty-line

Also, while hack back may protect a specific victim, it's unlikely to deter attacks at scale; attackers will simply move on to another target.

"Hit back at safe harbor states" - Addressing the issue of nation states that provide safe harbors for attackers is a matter of foreign policy and under the purview of governments. This is not an area for the private sector to step in, and doing so could lead to an escalation of aggression with nation states that have significant offensive resources. In addition, if specific states are targeted, attackers will take more steps to obfuscate their origins, making our view of the threat landscape less clear.

"We are at an economic disadvantage" - There is no real evidence that a lack of hack back authorities is creating an economic disadvantage or that authorizing hack back would create economic growth. While some security companies may benefit in the short term from being able to offer additional services, the associated overhead of managing the system, coupled with the high cost of addressing any errors, makes the potential for gain theoretical at best. Even if hack back were to be successful, the likely negative impact on small-to-medium businesses that cannot afford to protect themselves in this way, would likely harm the economy.

"We must avenge ourselves!" – This is vigilantism at best and should not be condoned; engaging law enforcement is a far more appropriate response.

*

*

*