Questions about Active Response

Sergio Caltagirone
University of Idaho
scaltagi@acm.org

1. Introduction

The purpose of this document is to present some of the questions of active response. This list of questions has been compiled from my own contemplation as well as questions/comments/discussions that I have had with others during presentations on the issue. Along with the question I have provided some brief discussion. These are not answers to the questions, but merely thoughts on where the discussion of these questions may take us. I hope that this document and the questions presented are of use in the general discussion about active response and provide an additional viewpoint.

2. Why even respond?

Our systems are far from secure. It is easy to argue from experience that for most systems, it is not if they will be compromised, but when. So what happens when they are compromised? Currently, the focus is placed on protection, and then forensics – but very little is discussed of what actions are taken during the attack (or between when an attack is detected and determined to be finished). Therefore, a response policy is necessary – especially in life/safety/national security critical systems – so that appropriate action can be take in such situations.

Additionally, response is not an option. If an attack is detected a determination must be made if to respond, and if the answer is in the affirmative, how to respond. Even if an organization decides not to respond, that in itself is an action – that of non-action.

3. Which threats require a response?

It is not the threat that is important in the decision to respond, but rather the asset being protected and its value (both tangible and intangible). Because of the subjectivity, each organization must decide for themselves which assets will be protected using active response. This involves the perceived level of comfort in both the ability to respond, and the ability to analyze the risks.

4. How do we respond?

Determining how to respond should be planning-centric – meaning that any organization wishing to utilize response should involve all stakeholders and a thorough risk analysis in an attempt to devise an active response policy and plan. Caltagirone and Frincke developed an active response decision model, called ADAM, in [1]. This is an question that requires further attention.

5. What actions are considered a response?

Here I present a potential taxonomy of active response actions. There are seven categories, partially adapted from [2]. Some actions may fit into multiple categories.

1. **Internal Notification**: Using the organizational structure to notify the appropriate persons of an active defense situation
2. **Internal Response**: Applying active defense actions within an organization's boundaries (e.g. shutting down the port on a firewall)
3. **External Cooperative Response**: Employing the assistance of other entities outside of an organization to mitigate a threat
4. **Non-cooperative Intelligence Gathering**: Using external services (finger, nmap, netstat) to gather intelligence on the attacker
5. **Non-cooperative `Cease and Desist'**: Shutting down harmful services that do not affect usability on a network or host.
6. **Counter-strike**: An offensive action designed to deny an attacker the ability to continue an attack.
7. **Preemptive Defense**: With knowledge of a forthcoming attack, execute active defense actions to preempt (and disable) the upcoming attack

6. What are the primary problems with response?

I have identified five primary problems with response. These are problems that come up during most of my active response discussions and presentations.

1. **Legal**: The questions of utilizing certain actions during a response need to be answered from a legal standpoint. This involved civil, criminal, domestic and international law.
2. **Ethics**: The question of response from an ethical viewpoint is also a serious consideration. Which actions should be taken in some scenarios, which should be discussed from both the teleological and deontological frameworks.
3. **Risk Analysis**: Can we provide a thorough enough risk analysis to actually perform active response comfortably? Can the ethical and legal risks truly be evaluated?
4. **Technical**: Does the technological environment preclude true active response? Can we decide and respond quickly enough? Can intrusion detection systems provide reliable alerts? Can we accurately trace-back the attacker?
5. **Unintended Consequences**: There are three potential categories of unintended consequences.
    a. **Attacker Response**: Instead of response stopping an attacker, the attacker may instead change their tactics. If an attacker detects a response, what if they divert their activities to another, potentially more valuable, asset? What if they jump on IRC and contact their friends to launch an even more vigorous attack?
    b. **Damage to non-attackers**: If we decide to respond, there is always the probability that we will accidentally respond against the wrong target. What if we respond against Grandma May because her desktop computer is used as a zombie in an attack?
    c. **Damage to own resources**: Attackers may use response to their own advantage, or a defender may inadvertently cause damage to their own resources. This includes a self-imposed denial-of-service attack by blocking certain ports or IP addresses.

7. What is the purpose (goal) of response?

Information warfare and active response are very similar in many respects, but it is the goal of each that clearly delineates them. Information warfare seeks to gain a military advantage, where active response is only intended to mitigate the current threat and return a system to a more secure state. The purpose of response should always be mitigation of the current threat, and never for retribution, retaliation, or the prevention of future yet-unknown attacks.

8. What are key areas for future work?

This is a topic that includes many avenues for future work. More discussion in general is needed first. The ethics and legality of response need to be seriously considered (as they have been in previous workshops and discussions) with academic rigor to decide the appropriate questions. Additional work needs to be done with decision modeling, so that formal and proven models of response strategy are developed. Work also needs to be done to answer important questions regarding unintended consequences, risk-analysis, and the role of active response in an intrusion detection framework. These are just some of the areas for future work.

9. References

[1] S. Caltagirone and D. Frincke, "ADAM: Active Defense Algorithm and Model," in Aggressive Network Self-Defense, N. R. Wyler, Ed. Rockland, MD, USA: Syngress Publishing, 2005, pp. 287-311.

[2] D. Dittrich, Active Defenses To Cyber Attacks. University of Washington Information School: Agora Workshop, September 12, 2003.