Incident Response

I wanted to take this week to review a very important part of the world in Cyber Security by discussing the incident response. With the eventuality that an infection or compromise is next to impossible to prevent, it is important to know what to do when it happens. To better understand this, let's look at the steps that everyone should take and find areas for improvement. In this we will look into staying calm, identifying the attack type or vector being used and most importantly knowing who to involve and the path of escalation.

Whether it is on your own work device or a client's device, the first and probably most important thing will be to remain calm. The very nature of a cyber-attack can be scary, and keeping a level head will help with the investigation and remediation process but will also help keep those around you, be it the client or your other teammates assisting with the incident on the same page. Knowing that your reaction can affect those around you and that the mindset and attitude that you tackle the issue at hand can mean the difference between properly diagnosing the issue and overreacting. As Canelo Alvarez puts it, "I have to stay calm, cool and collected." Keeping this at the forefront of your mind will allow you to best address the situation at hand.

When you believe that you have been infected or a user reports a potential infection, with the calm mentality, now you will need to start the investigation. Start with determining what system is being infected. Did this come from a user clicking a spam link? Was a malicious site visited either on purpose or accident? Is this affecting an end point or is this affecting a network appliance? Determining the infection will help you as the technician formulate the best plan of attack. While working through this step and remaining calm will allow you to put a meaningful plan of attack together. The attack may be able to become resolved by simply changing a user's password and running an antivirus scan or may need a more in-depth remediation but the only way to know this is to have a clear understanding of the effects and the scope of the attack.

Now that you have determined the scope of the incident, knowing the proper escalation path can be the difference between resolving an incident and just slowing the attackers down. By this point you have determined or started to determine the scope and the systems being targeted. Now is the time to start asking who else may need to be involved in the incident. Are there indicators that a server is apart of the attack vector? Is this attack bringing down networking appliances? Is there a potential that privileges were escalated? These questions will help you to plan who else may need to be involved. Another question to ask is to determine if there is a financial or business impact. While many people will think of escalation as solely getting the correct technical team involved to fix the issue, it can be just as important to know when you need to notify management to notify stakeholders. While this MAY be needed, you should never make those decisions lightly but instead a discussion between the technical team should be had to determine if that needs to happen and who should be the one to have that discussion.

While there will always be things that you will need to know regarding the week or even day in cyber-security, knowing how to handle these things can be just as important. Staying calm, attack identification and proper escalation are the fundamental steps for all cyber-attacks. Howard Shultz says it best, "Success is the by-product when you work toward a target." Using these ideals as the basis for any incident will allow you to correct issues with poise and grace.

Caleb Leggett – Technical Specialist