Application Service Attacks

If you have heard of the hacker group “Anonymous”, you have probably heard of them rendering servers of their targets being disabled for extended for periods of time. If you have heard of this, you already have seen an application service attack in action. The term application service attack can encompass a few different types of attacks including DDOS attacks, and cross site scripting.

One of the more common attacks is called a DDOS (distributed denial of service) attack.A distributed denial of service attack starts with an attacker usually getting a group of infected computers (usually infested with malware) to attack a computer of some sort (usually a server). Once the attacker floods the server with service requests, the server can’t handle all the good requests (from authenticated users) and all the bad requests from the attacker, and usually the server will crash. The reason for attacking the servers can vary, in some situations it can be revenge (for being laid off for instance), it could be for political reasons, or it could be purely malicious in origin. One telltale sign that you are under a DDOS attack would be the duration of stress on your website or server. If it continues for days or even weeks (instead of an hour or so), you might be experiencing a DDOS attack.

Another vulnerability that is easy for users to fall into is cross site scripting. This is when a malicious user finds a vulnerable website that allows script injection into fields (example being a comments field). These scripts execute when a user browses the page, triggering the script and stealing the user’s cookies (the small amount of data used to store info for specific client or website, which can include passwords and usernames), which can be then used to log in to various websites. The dangerous part about cross site scripting is that users will never know when it is triggered. Thankfully, most major websites have blocking cross site scripting into the security portion of web development. Having a good router or web filter would help alleviate these issues, as it would prevent users from accessing sites that may have lax security policies.

While you may look at these applications with the question “how can I help avoid these”? As for DDOS, you can help by avoiding phishing attempts (usually the infected computers come from malware infections on PC’s, some of those being from phishing). As you can see, these application issues can stem from just simple steps such as avoiding suspicious emails or sites. Application attacks usually have their roots in malware, so taking time to make sure your employees are educated on phishing and other scamming attacks, and making sure your web filters are up to date might save you from application attacks altogether, or at least minimize the impact these attacks make on applications.

If you have any questions about the application attacks, please give us a call at 509.433.7606 or submit a service request online at http://support.simplepowerit.com/