Marc Anders
SE 4930
Dr. Schilling
Security Summary #3

I read “A Case Study of Intelligence-Driven Defense” by Dan Guido. This article was published within IEEE Security and Privacy Magazine. This article posed a very interesting idea. The idea is that instead of trying to defend against any and all vulnerabilities within a system, the defender focuses on the most used vulnerabilities. There are thousands of vulnerabilities found each year, the author states. He talks about the fact that every defense against these vulnerabilities takes enormous amounts of manpower and money. Then he points out something very obvious, that most of the tech world should probably already know. Most hackers are lazy. He points out that it is very much impossible to properly mitigate each and every vulnerability. He also points out the fact that this large number of vulnerabilities is most likely daunting from an attackers perspective, and since they are looking for the most effective vulnerabilities they will choose from a select few that are proven to work. He points out that the massive exploitation instances that were documented in 2010 took advantage of in total 12 vulnerabilities. There were thousands of vulnerabilities, and 13 were the most effective ones.

It is a common acknowledgement among security professionals that their companies will be compromised at some point. They talk about the sheer number of holes within the system, and the futile effort to patrol all access points. Guido points out that instead of trying to defend all defects, if the defender intelligently analyzes the system, they can spend the same amount of time defending the most likely candidates

and end up catching 90% of the attacks. He backs this up with data, pointing out that the ten top exploit kits are responsible for over 99% of malicious URLs.

This idea of defending intelligently is very interesting to me. It makes sense, especially with the data provided. Attackers are often thought of as a huge group that will find any way through, but if time is taken to try to follow their line of thought, defending becomes much easier. Another point Guido makes is the fact that of the attacks that got past the basic defenses he suggests, none of the code was written by the attackers. The code used to compromise the system can either be traced back to security researchers posting found vulnerabilities, or to high end attacks that have already been discovered. Again this points out that the average attacker may not be any more intelligent than the defender. The only reason the attacker has a one up on the defender is because he has his select few vulnerabilities he uses. If the defender stops trying to watch the entire system and instead focuses on the most common exploits, I think they would find it a much more fair fight.