Abstract

The Internet has witnessed a tremendous growth the last years. Undoubtedly, its services and mostly the World Wide Web have become an integral part in the lives of hundreds of millions of people, who use it in daily basis. Unfortunately, as the Internet’s popularity increases, so does the interest of attackers who seek to exploit vulnerabilities in users’ machines. What was primary meant to be mainly a competition among computer experts to test and improve their technical skills has turned into a multi-billion dollar business. Nowadays, attackers try to take under their control vulnerable computers that will allow them to perform their nefarious tasks, such as sending spam emails, launching distributed denial-of-service (DDoS) attacks, generate revenue from online advertisements by performing click-frauds, or stealing personal data like email accounts and banking credentials.

In this dissertation, we address the security issues online users face every day from two points of view. First, we investigate how infected computers that constitute a botnet—network of compromised machines which are remotely controlled by an entity, known as botmaster—perform their malicious activities and we propose countermeasures against them. We study two of the most fundamental Internet protocols, SMTP and HTTP, and leverage the fact that numerous entities, including cybercriminals, implement these protocols with subtle but perceivable differences, which we can accurately detect. We then develop novel mitigation techniques that utilize these discrepancies to block the compromised computers from successfully executing the commands issued by a botmaster.

Second, we examine different ways in which attackers exploit the web infrastructure to infect new victims. We initially study the formed alliances among web spammers that aim to boost the page rank of their websites. As a result, these websites gain more popularity and can potentially host exploits. We then move forward and investigate the extent to which attackers can abuse the logic of search engine crawlers in order to perform various attacks. Next, we evaluate the ecosystem of online advertisements and analyze the risks related to abuses. Finally, we propose a system that can protect users from online threats while surfing the web.