Abstract

Nowadays Internet is the fulcrum of our world, and the World Wide Web is the key to access it. We develop relationships on social networks and entrust sensitive documents to online services. Desktop applications are being replaced by fully-fledged web-applications that can be accessed from any devices. This is possible thanks to new web technologies that are being introduced at a very fast pace. However, these advances come at a price. Today, the web is the principal means used by cyber-criminals to perform attacks against people and organizations. In a context where information is extremely dynamic and volatile, the fight against cyber-crime is becoming more and more difficult.

This work is divided in two main parts, both aimed at fueling research against cyber-crimes. The first part is more focused on a forensic perspective and exposes serious limitations of current investigation approaches when dealing with modern digital information. In particular, it shows how it is possible to leverage common Internet services in order to forge digital evidence, which can be exploited by a cyber-criminal to claim an alibi. Hereinafter, a novel technique to track cyber-criminal activities on the Internet is proposed, aimed at the acquisition and analysis of information from highly dynamic services such as online social networks.

The second part is more concerned about the investigation of criminal activities on the web. Aiming at raising awareness for upcoming threats, novel techniques for the obfuscation of web-based attacks are presented. These attacks leverage the same cutting-edge technology used nowadays to build pleasant and fully-featured web applications. Finally, a comprehensive study of today's top menaces on the web, namely *exploit kits*, is presented. The result of this study has been the design of new techniques and tools that can be employed by modern honeyclients to better identify and analyze these menaces in the wild.