Editorial

The phenomenon of cybercrime is constantly evolving in the recent years, increasing in intensity and complexity. In 2013 activities based on transactions continue to be exploited, cybercriminals target new platforms and new users and hacktivism continue to grow as a principal method to commit corporate espionage or to damage the institutions or government reputation.

The first part of 2013 has proven to be busy in terms of cyber security. Most cyber security incidents are results from circumscribed cybercrime activities – targeted against integrity and confidentiality services and information processed by computer systems target. Some of the most severe incidents were Red October, Miniduke, TeamSpy and APT1.

Red October

Global cyber-espionage operation known as Red October was targeted against government agencies, diplomatic organizations and companies all around the world. Attackers have created more than 60 different domain names and many servers hosted in different countries in order to control and manage the infected systems.

Miniduke

The malware Miniduke could penetrate computer systems by using a 0-day vulnerability of Adobe Reader application. MiniDuke victims turned out to be government agencies located in Ukraine, Belgium, Portugal, Romania, Czech Republic and Ireland, as well as a research organization in Hungary, two research centers and a medical facility in the U.S. There were detected 59 victims in 23 countries.

TeamSpy

The operation called TeamSpy is a complex line of attacks targeting high-ranking politicians and human rights advocates in the CIS and Eastern Europe. The main objective of this attack was to gather information from infected computers, including passwords and encryption keys.

APT1

APT1 is the name of a group of hackers in China that seems to be a division of the Chinese military. The term APT (Advanced Persistent Threat) is still new in this field. It is assumed that APT1 operates from 2006 and over the last 6 years it has managed to steal terabytes of data from at least 141 organizations by identifying and exploiting new security vulnerabilities from software and hardware used by target institutions.

The year 2013 proved to be full of incidents involving corporate infrastructure penetrated by cyber criminals. The victims includes big companies like Apple, Facebook, Twitter and Evernote. Attacks like Man-in-the-Browser and Man-in-the-Middle continue to be preferred by cybercriminals to take control over user accounts.

Threats that aim smartphones, tablets and other mobile devices have grown significantly over last year. The number of users of mobile banking continues to grow globally. Because users continue to migrate more and more on mobile devices, it is

expected that the cybercriminals will do the same and they will direct more and more attacks on this kind of devices. Vishing (Voice phishing - via phone, most often using Voice over IP technologies) and SMiShing (phishing via SMS/text message) are two of the most common attacks that exploit mobile device. SMS spoofing, also can be used by criminals to lure mobile phone users to navigate to a malicious URL supplied via a Hyperlink.

Mobile applications have become a new threat vector that cybercriminals take advantage of the opportunity to make malware and phishing attacks under the guise of legitimate applications. Android mobile platform is the most platform and it is also the most targeted mobile threats due to its open source nature.

The hacktivism became the main form of public expression of controversial opinions - political and economic - as a means of protest and ideological conflicts. Today's hacktivist groups predominantly are non-related teams or individual hackers who attack entities according to their own political, religious, social or economic agendas. In the first half of 2013, such attacks continued against Tibetan and Uyghur activists.

In this scenery of cyber threats, IJISC – International Journal of Information Security and Cybercrime attempts to bring together the latest research and development in information security and the latest methods to prevent and to fight the cybercrime phenomenon. The Journal includes studies, analyzes and research regarding the concept of information security and cybercrime.

In the second year of activity International Journal of Information Security and Cybercrime is indexed in international databases and represent an important scientific resource for academics, experts, people in training (students, PhD students, young researchers) or people interested to improve or to update knowledge in information security and cybercrime domains.

Assistant Professor **Ioan-Cosmin MIHAI**
Editor-in-chief of IJISC