Proceedings of the 12th European Conference on Information Warfare, University of Jyväskylä, Finland, 11-12 July 2013

Dangers of Social Networking Sites- the Propagation of Malware

WA Labuschagne, N Veerasamy

Council for Scientific and Industrial Research, Pretoria, South Africa
wlabuschagne@csir.co.za
nveerasamy@csir.co.za

Abstract

Users sometimes lack the security knowledge to protect themselves whilst carrying out activities online. One of the most popular tools used online is social networking tools. The popularity of Facebook and Twitter has become exponential with users making regular posts and updates. Due to the popularity of these sites, users easily engage and communicate with each other. Users may place personal details, hobbies and preferences in posts- all of which may look legitimate. Catchy phrases, controversial words and emotive language are all ways of enticing users into clicking on links. However, social networking site users may currently be unaware of the dangers, threats, attacks and malware that can stem from these popular forums. Malware, phishing attacks and digital attacks are emerging from these popular forums. The aim of this paper is to help uses protect themselves against malware on the social networking platforms. Various shifts in malware have taken place which include piggy-backing off files, email, spamming and now the instant messaging capabilities of social media sites provides an ideal avenue from which to dispense the next generation of malware which includes psychological tactics to influence users to perform undesired actions. Users may seemingly be unaware that a simple click on a spam message or obfuscated uniform resource locator (URL) can be triggering the download of malicious malware that will command their computer to form part of botnets. It is therefore essential to create some awareness of these dangers and explore how users can protect themselves. The paper will illustrate the dangers of social networking malware through examples. In addition, the paper will discuss propagation techniques used in social networking malware. The aim of the paper is to create user awareness to minimise the risk of falling prey to malware in popular social networking platforms. The paper will recommend best practices to users to guard against falling prey to social networking malware. In addition, the design of a high-level system to identify potential social network media malware will be proposed. Through this paper, users can better identify potential malware before they infect themselves.