Detecting Advanced Persistent Threats through Deception Techniques

Nikolaos Virvilis-Kollitiris

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business
76 Patission Ave., Athens GR-10434, Greece
nvir@aueb.gr

Abstract

The number and complexity of cyber-attacks has been increasing steadily in recent years. The major players in today’s cyber conflicts are well organized and heavily funded teams with specific goals and objectives, working for or supported by a nation-state. A commonly used term to describe such teams/groups is Advanced Persistent Threat (APT). APT target the communication and information systems of government, military and industrial organizations and are willing to use vast amounts of money, time and expertise to reach their goals. A clear indication of the level of sophistication of APT is their impressive arsenal. The complexity and capabilities of recently discovered malware used to facilitate such attacks are remarkable: Stuxnet, Duqu, Flame, Red October, MiniDuke and more recently Regin are examples of highly sophisticated malware, the development of which required skillful individuals - in some cases (e.g. Stuxnet) with expertise in multiple technology fields - as well as substantial financial resources. In addition, serious insider attacks have occurred that resulted in the publication of several thousand classified documents, highlighting the fact that even in sensitive institutions, the effectiveness of the existing security safeguards is insufficient. Advances in attacker sophistication have not been matched by similar defensive advances. The concept of keeping the internal, trusted network separated from the external, untrusted one (i.e. boundary protection) has become obsolete. The use of blacklists or signatures for attack detection is practically useless against sophisticated attackers. The security industry, having spent decades developing security products such as anti-malware solutions and intrusion-detection/prevention systems, refuses to admit the shortcomings of these products. It is not uncommon for security companies to advertise that their products can detect and stop APT, even though the same products have been unable to detect such attacks for several years. Furthermore, C-level executives fail to understand the need for more robust security mechanisms, as they believe that by following vendor recommendations and making significant investments in traditional security solutions, they will keep their organization secure. However reality has proven them wrong, over and over again. In order to defend against such sophisticated adversaries, it is necessary to redesign our defenses and develop technologies focused more on detection than prevention. The purpose of this thesis is to offer a comprehensive view of the APT problem by analyzing the most common techniques, tools and attack paths that attackers are using, and highlighting the shortcomings of current security solutions. The use of deception techniques for attack detection is one of the integral focal points of this thesis. Based on this concept, a novel APT detection model is proposed, implemented and evaluated. The evaluation results highlight the significant efficacy of the model in detecting sophisticated attacks, with a very low false positive rate.

A dissertation submitted for the partial fulfillment of a Ph.D. degree

October 2015
References


62. Fisher, D., 2012. What have we learned: FLAME malware,


Google, 2013. Safe Browsing API. Available at: https://developers.google.com/safe-browsing/.


114. Kelley, M., 2012. The Stuxnet Virus at Iran’s Nuclear Facility was Planted by an Iranian Double Agent,


187. Reed, T., 2007. At the abyss: an insider’s history of the Cold War, Random House LLC.


231. TOR, 2015. TOR. Available at: https://tor.eff.org/.


247. Weiss, G.W., 1996. The Farewell Dossier,


