How to Steal a Botnet and What Can Happen When You Do

Richard A. Kemmerer

University of California, Santa Barbara, USA
kemm@cs.ucsb.edu

Abstract. Botnets, which are networks of malware-infected machines that are controlled by an adversary, are the root cause of a large number of security threats on the Internet. A particularly sophisticated and insidious type of bot is Torpig, which is a malware program that is designed to harvest sensitive information (such as bank account and credit card data) from its victims. In this talk, we report on our efforts to take control of the Torpig botnet for ten days. Over this period, we observed more than 180 thousand infections and recorded more than 70 GB of data that the bots collected.

While botnets have been hijacked before, the Torpig botnet exhibits certain properties that make the analysis of the data particularly interesting. First, it is possible (with reasonable accuracy) to identify unique bot infections and relate that number to the more than 1.2 million IP addresses that contacted our command and control server during the ten day period. This shows that botnet estimates that are based on IP addresses are likely to report inflated numbers. Second, the Torpig botnet is large, targets a variety of applications, and gathers a rich and diverse set of information from the infected victims. This allowed us to perform interesting data analysis that goes well beyond simply counting the number of stolen credit cards. In this talk we will discuss the analysis that we performed on the data collected and the lessons learned from the analysis, as well as from the process of obtaining (and losing) the botnet.

S. Qing, C.J. Mitchell, and G. Wang (Eds.): ICICS 2009, LNCS 5927, p. 1, 2009.