LCN 2011 Keynote by Peter Martini

Wednesday, 5 October 2011

Botnets - Detection, Classification and Countermeasures

Prof. Dr. Peter Martini

Institute of Computer Science, University of Bonn, and
Director of Fraunhofer-Institut fuer Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)

ABSTRACT

Different species of malicious software (malware) have been around for quite a while. Add a command and control structure — and here you are: A "cyber army" of hijacked machines waiting for the commands of the so-called "bot herder" ready to serve the master's will. Botnets may be used for distributing spam, for installing additional malware, for information harvesting, for distributed denial of service attacks and for other actions initiated and controlled by the bot herder.

Today, thousands of botnets are well understood. Their actions are observed and in some cases controlled/limited. In addition, experts active in this field argue that there is a very large number of botnets escaping tracking efforts by mechanisms such as frequent reconfiguration and frequent migration of command-and-control structures.

In his keynote, Peter Martini will comment on the challenge of detecting botnets, on aggregation and clustering of similar species of malicious software and on countermeasures used today. He will comment on the relevance of botnet size and the problem of measuring the current size of well-known botnets. Finally, he will comment on legal issues and missing pieces in the fight against botnets: Botnets have come to stay.

ABOUT THE SPEAKER

Professor Peter Martini is director of the Fraunhofer Institute for Communication, Information Processing, and Ergonomics (FKIE) in Wachtberg (near Bonn), Germany. The Fraunhofer-Gesellschaft is the largest organization of applied research in Europe. With its staff of 300 people, FKIE is proud to be a member of the Fraunhofer organization and the Fraunhofer Group for Defense and Security. In addition, Prof. Martini is head of the Institute of Computer Science 4 at the University of Bonn.

After studying computer science and electrical engineering at the Technical University of Aachen, Germany, Peter Martini spent four years as scientific assistant at the Technical University of Aachen. During that time, he finished his Ph.D. in computer science. From 1990 to 1996, Prof. Martini was professor of computer science at the University of Paderborn, Germany, before he changed to Bonn. At the University of Bonn, he established a research group active in the areas of performance engineering, IT security, mobile communication and high speed networks.

From 2003, Prof. Martini was a member of the scientific advisory council of FKIE, from 2005 he chaired this committee until he became director of FKIE in 2010. Prof. Martini's group became widely known from its research in the areas of security in tactical communication systems and countermeasures against botnets. The demystification of the conficker worm was one of the most popular examples of successful research in his group.

Prof Martini is a member of the scientific advisory council of the German MoD.