In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Understanding and Detecting Malicious Activities in Internet

by

Dr. Zhou Li
RSA Laboratories, U.S.A.

Date	**:**	**13 Jan., 2015 (Tue.)**
Time	**:**	**11:00am – 12:00noon**
Venue	**:**	**Room 833, Ho Sin Hang Engineering Building** **The Chinese University of Hong Kong**

Abstract

The technological progress in today's web not only fosters a booming Web industry, but also provides new opportunities to criminals who are industrializing their dark business. This talk will review popular attack vectors in web space and present several new detection mechanisms. First, an attack against vulnerable websites will be presented, in which the adversary compromises vulnerable sites and injects redirection scripts that bring visitors to malicious sites. Our study shows that attackers blindly inject their malicious payloads into various web contents, including copies of popular open-source libraries. By comparing those libraries' original copies and compromised ones, we built a new technique capable of extracting malicious content in a large scale. Second, we examine the attacks against enterprise network. In particular, the emerging Advanced Persistent Threat (APT) will be described and we propose a new detection mechanism based on belief propagation algorithm which is able to identify the compromised hosts and malicious sites involved.

Biography

Zhou Li is a research scientist at RSA Laboratories, The Security Division of EMC. His research areas cover web security, mobile security, and genome privacy. Before joining RSA Labs, Zhou worked as a Research Assistant at Indiana University Bloomington from 2009 to 2013 and as a Research Intern at Microsoft Research Silicon Valley in 2011. Zhou received a B.S. degree and M.S. degree in Computer Science from Wuhan University, China, and obtained a Ph.D. degree in Computer Science from Indiana University Bloomington. Zhou has published research papers in top security conferences including IEEE S&P, Usenix Security and CCS.

**** ALL ARE WELCOME ****

Host: Professor Kehuan Zhang (Tel: 3943-8391, Email: khzhang@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)
O:\Seminar (SEM)\2015_PDF\IE Seminars\sem0115_Zhou Li_KHZ_130115.docx