King Fahd University of Petroleum and Minerals

College of Computer Science & Engineering

Information and Computer Science Department

Short Course

Malware Analysis

Malware are the threat of the future

All recent cyber-attacks (Stuxnet, Shamoon, etc.) are carried out using malwares

Security products (Antivirus, IDS,..) do not protect against malware targeted attacks

Description:

Recent attacks against Iran's nuclear facilities (Stuxnet malware) and Saudi Aramco (Shamoon malware) are the premises of devastating cyber-attacks. Attackers are now designing zero-day malwares targeting specific organizations. Typical security and antivirus products do not provide protection against such crafted and specific malwares. The targeted organization is left alone in trying to detect and clean-up such attacks.

This course focuses on two main aspects: (1) Malware development and (2) Malware Analysis. As a participant you will be exposed to the most recent techniques used by hackers to develop malware. This includes: Obfuscation, Cryptors, Security products bypassing, Hooking, Shellcoding, and much more techniques. In the second part you will learn how to analyze, detect and contain malware incidents. In particular, you will be exposed to advanced static and dynamic analysis techniques and tools. Knowledge acquired in this course will be applied to practically analyze several malware samples, in particular, Stuxnet and Shamoon samples.

Duration: 4 days (Weekend)

Dates: April 30 - May 3, 2014

Location: ICS Department (KFUPM)

Instructor: Dr. Sami Zhioua

Certificate: A graduate certificate will be awarded to participants

Information and Registration:

zhioua@kfupm.edu.sa

Short Course Overview

1. **Background material**
   - Crash-course in intel architecture and assembly
   - Windows Architecture
   - PE format (Windows Executable)
2. **Malwares and Malware Development**
   - Malware Taxonomy
   - File Infection
   - Malware Concealment Strategies
   - Process Injection
   - Call Table Hooking
   - Detour Patching
   - Shellcoding
   - DKOM
   - Anti-Virus Technologies
   - Anti-Anti-Virus Techniques
3. **Malware Static Analysis**
   - Checking file signature
   - Malware Strings
   - Imports and exports
   - Encryption and Packing
   - Advanced Static Analysis:
4. **Malware Dynamic Analysis**
   - Setting up a virtual malware analysis lab
   - Monitoring Windows Activity using Process Monitor
   - Analyzing processes using Process Explorer
   - Comparing registry snapshots with Regshot
   - Monitoring malware network traffic
   - Debugging with ollyDBG
   - Debugging with IDA Pro
5. **Analyzing Stuxnet and Shamoon Malware**
   - Analysis of the PE structure
   - Static analysis of Stuxnet and Shamoon
   - Dynamic analysis of Stuxnet and Shamoon
   - Defeating encryption
   - Analyzing the destructive features

Website: http://faculty.kfupm.edu.sa/ics/zhioua/MalwareAnalysis