Revised

Malware Forensics Workshop
Dynamic and Code Analysis of Slackbot and ZeuSbot
26 March 2011, Sat, 9:30 am – 4:30 pm

Venue : Room 707, 7/F, Fortress Tower, 250 King's Road, North Point, Hong Kong
(Exit B, Fortress Hill MTR Station)

Equipment Required :
Participants are required :
(1) to come with laptop installed with VMware, VMPlayer or VMFusion
(2) to prepare a 10G -15G hard disk spare space for holding all virtual machines

Outline :
The workshop is designed to share examination procedures and results of malicious software that runs on Microsoft Windows XP. By applying reverse-engineer techniques and the helps of various tools, utilities and debugger, a forensics examiner, should benefit from knowing how to analysis the basic functionality of malware. The selected samples are two different versions of malware that can control victims' machines and/or collect victims' credential information during online banking transactions.

Prerequisites :
- Member of ISFS
- Law Enforcement
- Individuals responsible for incident handling, forensics investigation or Windows systems administration
- Security Professionals
- Participants are expected to have good understanding of Windows system and networking concepts
- Preferable to have some programming knowledge, such as variables, loops and functions calls or some exposure to assembly concepts
- During the workshop, the participants will learn to use some dynamic analysis tools and OllyDbg

Fee :
- ISFS members - Free of charge
- Non-ISFS members - an admin fee of HK$100.00 is required to be paid at the workshop

Registration and Enquiry :
- Due to limited space of the venue, pre-registration is required. FIRST COME FIRST SERVED
- Please send information of Full Name and Telephone No. via email to Ms Catherine Chan at catherine_chan@isfs.org.hk **on or before 25 March 2011, noon.**
- Please email to Mr Frankie Li at fukayli@gmail.com or Mr Ricci Ieong at ricci.ieong@gmail.com

Suggested readings and online materials before the workshop
http://www.sans.org/reading_room/whitepapers/malicious/clash-titans-zeus-spyeye_33393
http://www.mnin.org/write/ZeusMalware.pdf
Slackbot:
http://www.symantec.com/security_response/writeup.jsp?docid=2001-100912-0421-99&tabid=2
Zeusbot:
https://zeustracker.abuse.ch/faq.php
Tutorial for you, Reversing for Newbies :
http://tuts4you.com/download.php?view.122