NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **"Meet the Equation: The most advanced cyberattack in history."**

Speaker: Vitaly Kamluk
Principal Security Researcher, Global Research & Analysis Team, Kaspersky Lab;
Cyber Security Reseacher, INTERPOL.

Date/Time: 3 March 2015, Tuesday, 12:00 PM to 01:30 PM

Venue: SR1, COM1-02-06

Chaired by: Dr Roychoudhury, Abhik, Professor, School of Computing (abhik@comp.nus.edu.sg)

Abstract:

Once upon a time in China, some believe around the year 1003, head priest of the White Lotus Clan, Pai Mei, was walking down the road - contemplating whatever it is that a man of Pai Mei's infinite powers would contemplate (which is another way of saying, "who knows?") - when a Shaolin monk appeared on the road, traveling in the opposite direction. As the monk and the priest crossed paths, Pai Mei, in a practically unfathomable display of generosity, gave the monk the slightest of nods. The nod was not returned.

Now, was it the intention of the Shaolin monk to insult Pai Mei? Or did he just fail to see the generous social gesture? The motives of the monk remain unknown. What is known were the consequences.

The next morning Pai Mei appeared at the Shaolin Temple and demanded of the Temple's head abbot that he offer Pai Mei his neck to repay the insult. The Abbot at first tried to console Pai Mei, only to find Pai Mei was ... inconsolable.

So began the massacre of the Shaolin Temple and all sixty of the monks inside at the fists of the White Lotus. And so began the legend of Pai Mei's five-point-palm-exploding-heart technique.

The presentation will tell about the deadliest of all cyberattacks and the masters of advanced persistent threats, The Equation Group, that has been announced just a couple of weeks ago.

Biodata:

Vitaly has been working with Kaspersky Lab for 10 years. He has dealt with major malware outbreaks such as Conficker worm in 2009, struggling against RSA-encrypting ransomware back in 2008, analyzing advanced cyberespiponage operations such as RedOctober, Duqu, Flame, Careto, NetTraveler, Icefog, DarkHotel and more. In 2010, Vitaly spent working in Japan as a Chief Malware Expert, leading a group of local researchers. He specializes in threats focusing on global network infrastructures, malware reverse engineering and cybercrime investigations. He is an author of patented technologies used at Kaspersky Lab for automated malware analysis and discoverer of 0-day attacks against anti-theft software embedded in most of modern PC BIOS/UEFI firmware.

Vitaly lives and works in Singapore as a member of INTERPOL Digital Forensics Lab team, doing malware analysis and investigation support.

He has been a speaker at many information security/hacker conferences, such as Defcon, Blackhat, FIRST, Underground Economy, PHDays, ZeroNights and more.