

# NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

Advanced Systems Seminar

**Title:**        **Finding Malware at Web Scale**

Speaker:      Dr. Ben Livshits  
                 Microsoft Research (Redmond)

Date/Time:    18 December 2015, Friday, 03:00 PM to 04:30 PM

Venue:        SR2, COM1-02-04

Chaired by:   Dr Saxena, Prateek, Dean's Chair Assistant Professor, School of Computing  
                 (prateeks@comp.nus.edu.sg)

Registration: <https://goo.gl/EaWnHF>

Refreshment provided; Limited seats: 40 pax; First come first serve

Abstract:

Over the last several years, JavaScript malware has emerged as one of the most insidious ways to attack unsuspecting users through their web browsers. This talk covers a series of projects that use ideas from program analysis, both static and runtime, to find --- and fight --- JavaScript malware.

A number of these academic projects have been successfully deployed within Bing and have been used daily to find and block malicious web sites, constituting one of the largest-scale deployments of such techniques. This talk will focus on the complex interplay between static and runtime analyses and outline some of the lessons learned in migrating research ideas to real-world products.

I will present the key ideas and insights behind four of the systems with increasingly dazzling names we have created: Nozzle, Zozzle, Rozzle, and Kizzle. Nozzle is a runtime malware detector that focuses on finding heap spraying attacks. Zozzle is a mostly static detector that finds heap sprays and other types of JavaScript malware. Rozzle leverages a novel technique we call multi-execution to address the problem of client-side cloaking, an avoidance tactic used by malware to escape detection. Lastly, Kizzle is a system that finds exploit kits, the most sophisticated form of JavaScript malware to date.

These systems all share two characteristics that are key to their deployability: they are fast and extremely precise. For example, Zozzle's false positive rate is about one in a million,

while Nozzle's is close to one in a billion.

#### Biodata:

Ben Livshits is a research scientist at Microsoft Research in Redmond, WA and an affiliate professor at the University of Washington. Originally from St. Petersburg, Russia, he received a bachelor's degree in Computer Science and Math from Cornell University in 1999, and his M.S. and Ph.D. in Computer Science from Stanford University in 2002 and 2006, respectively. Dr. Livshits' research interests include application of sophisticated static and dynamic analysis techniques to finding errors in programs.

Ben has published papers at PLDI, POPL, Oakland Security, Usenix Security, CCS, SOSP, ICSE, FSE, and many other venues. He is known for his work in software reliability and especially tools to improve software security, with a primary focus on approaches to finding buffer overruns in C programs and a variety of security vulnerabilities (cross-site scripting, SQL injections, etc.) in Web-based applications. He is the author of several dozen academic papers and patents. Lately, he has been focusing on topics ranging from security and privacy to crowdsourcing an augmented reality. Ben generally does not speak of himself in the third person.

#### About Advanced Systems Seminar (ASS):

ASS is a new seminar series comprising of prominent researchers working in systems areas. It's a low-volume seminar series, with about 1 talk per month, and will overlap with important school talks (e.g. faculty candidate talks). We will have a mix of folks from industry and academia, on topics of emerging interests. The series is open to all invitees and School of Computing - NUS members. All graduate students working in systems, PL/ SE, networking, security, OS, architecture, databases and allied areas are strongly encouraged to attend these talks and converse with the speakers.