Announcement and Call for Papers USENIX

First USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET '08)

Botnets, Spyware, Worms, and More

Sponsored by USENIX, The Advanced Computing Systems Association

http://www.usenix.org/leet08

April 15, 2008 **San Francisco, CA, USA**

Co-located with the 5th USENIX Symposium on Networked Systems Design & Implementation (NSDI '08), which will take place April 16–18, 2008, and Usability, Psychology, and Security 2008, which will take place on April 14, 2008

Important Dates:

Submissions due: *February 13, 2008, 11:59 p.m. EST*
Notification of acceptance: *March 24, 2008*
Final papers due: *April 4, 2008*

Workshop Organizers

Program Chair

Fabian Monrose, *Johns Hopkins University*

Program Committee

Michael Bailey, *University of Michigan*
David Dagon, *Georgia Institute of Technology*
Thorsten Holz, *University of Mannheim*
Jaeyeon Jung, *Intel Research*
Angelos Keromytis, *Columbia University*
Christopher Kruegel, *University of California, Santa Barbara*
Vern Paxson, *International Computer Science Institute*
Niels Provos, *Google Inc.*
Moheeb Rajab, *Johns Hopkins University*
Dug Song, *Zattoo*
Helen Wang, *Microsoft*

Steering Committee

Vern Paxson, *International Computer Science Institute*
Niels Provos, *Google Inc.*
Stefan Savage, *University of California, San Diego*

Overview

As the Internet has become a universal mechanism for commerce and communication, it has also become an attractive medium for online criminal enterprise. Today, widespread vulnerabilities in both software and user behavior allow miscreants to compromise millions of hosts (worms, viruses, drive-by exploits, etc.), conceal their activities with sophisticated system software (rootkits), and manage these resources via a distributed command and control framework (botnets). This platform in turn provides economics of scale for a wide range of criminal activities including spam, phishing, DDoS, click fraud, and so on.

Topics

LEET has evolved from the combination of two other successful workshops, the ACM Workshop on Recurring Malcode (WORM) and the USENIX Workshop on Hot Topics in Understanding Botnets (HotBots), which have each dealt with aspects of this problem. However, while papers relating to both worms and botnets are explicitly solicited, LEET has a broader charter than its predecessors. We encourage submissions of papers that focus on any aspect of the underlying mechanisms used to compromise and control hosts, the large-scale "applications" being perpetrated upon this framework, or the social and economic networks driving these threats. Topics of interest include, but are not limited to:

- Infection vectors for malware (worms, viruses, etc.)
- Botnets, command, and control channels
- Spyware
- Operational experience
- Forensics
- Click fraud
- Measurement studies
- New threats and related challenges
- Boutique and targeted malware
- Phishing
- Spam
- Underground markets
- Carding and identity theft

- Miscreant counterintelligence
- Denial-of-service attacks
- Hardware vulnerabilities
- Legal issues
- The arms race (rootkits, anti-anti-virus, etc.)
- New platforms (cellular networks, wireless networks, mobile devices)
- Camouflage and detection
- Reverse engineering
- Vulnerability markets and zero-day economics
- Online money laundering
- Understanding the enemy
- Data collection challenges

Questions regarding a topic's suitability are welcome and can be directed to the workshop steering committee, leetsc@usenix.org.

Workshop Format

LEET aims to be a true workshop, with the twin goals of fostering the development of preliminary work and helping to unify the broad community of researchers and practitioners who focus on worms, bots, spam, spyware, phishing, DDoS, and the ever-increasing palette of large-scale Internet-based threats. Intriguing preliminary results and thought-provoking ideas will be strongly favored and papers will be selected for their potential to stimulate discussion in the workshop. Each author will have 15 minutes to present his or her work, followed by 15 minutes of discussion with the workshop participants.

Submissions

Submitted papers must be no longer than eight (8) single-spaced 8.5" x 11" pages, including figures, tables, and references, formatted in two (2) columns. Author names and affiliations should appear on the title page. Submissions must be in PDF format and must be submitted via the Web submission form on the LEET '08 Call for Papers Web site, http://www.usenix.org/leet08/cfp.

Papers accompanied by nondisclosure agreement forms will not be considered. All submissions will be treated as confidential prior to publication in the Proceedings.

Simultaneous submission of the same work to multiple venues, submission of previously published work, and plagiarism constitute dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may, on the recommendation of a program chair, take action against authors who have committed them. In some cases, program committees may share information about submitted papers with other conference chairs and journal editors to ensure the integrity of papers under consideration. If a violation of these principles is found, sanctions may include, but are not limited to, barring the authors from submitting to or participating in USENIX conferences for a set period, contacting the authors' institutions, and publicizing the details of the case.

Note, however, that we expect that many papers accepted for LEET '08 will eventually be extended as full papers suitable for presentation at future conferences.

Authors uncertain whether their submission meets USENIX's guidelines should contact the Program Chair, leet08chair@usenix.org, or the USENIX office, submissionspolicy@usenix.org.