2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)
Botnets, Spyware, Worms, and More

Sponsored by USENIX, the Advanced Computing Systems Association
http://www.usenix.org/leet09

April 21, 2009   **Boston, MA**

LEET '09 will be held immediately before the 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI '09), which will take place April 22–24, 2009.

Important Dates
Submissions due: *January 23, 2009, 11:59 p.m. EST*
Notification of acceptance: *March 2, 2009*
Electronic files due: *March 30, 2009*

Workshop Organizers

Program Chair
Wenke Lee, *Georgia Institute of Technology*

Program Committee
Michael Bailey, *University of Michigan*
Nick Feamster, *Georgia Institute of Technology*
Thorsten Holz, *University of Mannheim*
Christopher Kruegel, *University of California, Santa Barbara*
Jose Nazario, *Arbor Networks*
Vern Paxson, *International Computer Science Institute and
    University of California, Berkeley*
Patrick Peterson, *Ironport/Cisco*
Phil Porras, *SRI International*
Niels Provos, *Google Inc.*
Moheeb Rajab, *Google Inc.*
Paul Royal, *Georgia Tech Information Security Center*
Angelos Stavrou, *George Mason University*

Steering Committee
Fabian Monrose, *University of North Carolina, Chapel Hill*
Vern Paxson, *International Computer Science Institute and
    University of California, Berkeley*
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 (via 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). These tools in turn provide economics of scale for a wide range of criminal activities including spam, phishing, DDoS, click fraud, and so on.

Topics
This will be the second edition of LEET, which had 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). These two workshops 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 '09 Call for Papers Web site, http://www.usenix.org/leet09/cfp.

All papers will be available online to registered attendees prior to the workshop and will be available online to everyone starting on April 21, 2009. If your accepted paper should not be published prior to the event, please notify production@usenix.org.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX LEET '09 Web site; rejected submissions will be permanently treated as confidential.

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 '09 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 chairs, leet09chair@usenix.org, or the USENIX office, submissionspolicy@usenix.org.