6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '13)

Sponsored by USENIX, the Advanced Computing Systems Association **August 12, 2013, Washington, D.C.**

Important Dates

Submissions due: *May 15, 2013, 11:59 p.m. PDT*
Notification to authors: *June 7, 2013*
Final paper files due: *June 9, 2013*

Conference Organizers

Program Chair

Vern Paxson, *University of California, Berkeley, and International Computer Science Institute*

Program Committee

Boldizsar Bencsath, *Budapest University of Technology and Economics, CrySyS Lab*
Marc Dacier, *Symantec Research Labs*
Christopher Kruegel, *University of California, Santa Barbara*
Jose Nazario, *Invincea Labs*
Christian Platzer, *Vienna University of Technology*
Peiter Mudge Zatko, *mudge@uidzero.org*

Steering Committee

Fabian Monrose, *University of North Carolina, Chapel Hill*
Vern Paxson, *University of California, Berkeley, and 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 a highly attractive medium for online criminal enterprise and disruptive nation-state activity. Today, widespread vulnerabilities in both software and user behavior allow miscreants to compromise millions of hosts, conceal their activities deeply within their victims' systems, and manage these resources via distributed command and control frameworks. These tools and techniques provide economies of scale for a wide range of malicious activities, including identity theft, spam, phishing, DDoS, extortion, and espionage. Much of this activity is driven by economic incentives, but recently we have also seen the emergence of politically motivated attacks, both highly visible and surreptitious. Fundamentally, our global society faces a wide range of large-scale Internet threats that require diligent study leading to effective defenses.

Topics

Now in its sixth year, LEET provides a unique forum for the discussion of the landscape of modern attacks: threats to the confidentiality of data, the integrity of digital transactions, and the dependability of the technologies we increasingly rely upon. We encourage submissions of presentations and papers that focus on the malicious activities themselves (e.g., reconnaissance, exploitation, toolkits, services); our responses as defenders (prevention, detection, mitigation, forensics); the social, political, and economic structures driving these malicious activities; and the legal and ethical considerations guiding our defensive responses. Topics of interest include but are not limited to:

- Malware infection vectors (drivebys, worms, mobile exploits, etc.)
- Botnets, command-and-control channels
- Operational experience and case studies
- Measurement studies
- New threats and related challenges
- Manipulation of social networks
- Boutique and targeted malware
- Miscreant counterintelligence
- Phishing
- Spam
- Forensics
- Underground markets and social structures
- Bitcoin fraud and abuse
- Carding and identity theft
- Denial-of-service attacks
- Hardware vulnerabilities
- Legal issues
- The arms race (rootkits, anti–anti-virus, etc.)
- Camouflage and detection
- Reverse engineering
- Vulnerability markets and zero-day economics
- Online money laundering
- Data collection and other research challenges

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 the ever-increasing palette of large-scale Internet-based threats. Intriguing preliminary results, illuminating experiences, and thought-provoking ideas will be strongly favored; presentations and papers will be selected for their potential to stimulate discussion in the workshop.

This year, LEET is seeking two types of submissions:

1. Presentation proposals for talks discussing novel research or detailed experiences meant to elicit extensive discussion. Please remember that we are only seeking original research work; LEET is not an appropriate venue for marketing material of any kind, nor for re-presenting a talk previously given.
2. Extended abstracts (no more than 4 pages) describing your work in an academic style suitable for publication.

USENIX will publish both the presentations and the extended abstracts on the LEET '13 Web site, the latter with "Extended Abstract" in the title. After the event the workshop Web site will include recordings of all presentations as well. Authors/presenters will have 10–20 minutes each to present their work (as determined by the program committee), followed by adequate time for discussion with the workshop participants.

Submission Instructions

For presentation proposals, include either a draft slide deck (PDF or PowerPoint) or a short (1 page tops) description of what your talk will cover and why it is interesting. For either format, please state how long you would prefer to speak. If you have past speaking experience, please document where you have recently presented.

Extended abstracts must be no longer than four (4) 8.5" x 11" pages, including figures, tables, and references, formatted in two (2) columns, using 10-point type, reasonable margins, and no annoying formatting tricks. Include author names and affiliations on the title page. Submissions must be in PDF.

All submissions should be made via the Web submission form on the LEET '13 Call for Papers Web site, www.usenix.org/leet13/cfp.

Papers will be available online to registered attendees before the workshop. If your accepted paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the day of the workshop, August 12, 2013. We will place talks that are ready in advance online, too, but this is not a requirement unless the program committee specifically requests it.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX LEET '13 Web site; rejected submissions will be permanently treated as confidential.

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may take action against authors who have committed them. See the USENIX Conference Submissions Policy for details. Note, however, that we expect that many papers accepted for LEET '13 will eventually be extended as full papers suitable for presentation at future conferences. In addition, we require presentation proposals to include significant new material compared to any previous version of a talk. Questions? Contact your program chair, leet13chair@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Rev. 5/6/13