

# 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11)

## *Botnets, Spyware, Worms, and More*

Sponsored by USENIX, the Advanced Computing Systems Association

<http://www.usenix.org/leet11>

March 29, 2011

Boston, MA

LEET '11 will be co-located with the 8th USENIX Symposium on Networked Systems Design and Implementation (NSDI '11), which will take place March 30–April 1, 2011.

### Important Dates

Submissions due: *Friday, January 28, 2011, 11:59 p.m. PST*

Notification of acceptance: *Wednesday, February 23, 2011*

Final papers due: *Sunday, March 6, 2011*

### Workshop Organizers

#### Program Chair

Christopher Kruegel, *University of California, Santa Barbara*

#### Program Committee

Michael Bailey, *University of Michigan*

David Dagon, *Independent*

Nick Feamster, *Georgia Institute of Technology*

Chris Grier, *International Computer Science Institute and University of California, Berkeley*

Guofei Gu, *Texas A&M University*

Thorsten Holz, *Ruhr-University Bochum, Germany*

Engin Kirda, *Northeastern University*

Paolo Milani Comparetti, *Vienna University of Technology, Austria*

Fabian Monrose, *University of North Carolina, Chapel Hill*

David Moore, *Cisco, Inc.*

Jose Nazario, *Arbor Networks, Inc.*

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

Phil Porras, *SRI International*

Stefan Savage, *University of California, San Diego*

Yinglian Xie, *Microsoft Research*

#### 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 economies of scale for a wide range of malicious activities, including spam,

phishing, DDoS, and click fraud. Much of this activity is driven by economic incentives, but recently we have seen the emergence of highly visible, politically motivated attacks. While the motivations for malicious behavior and the technical mechanisms that enable them remain rich areas of research, it is clear that, today, our global society is faced with a wide range of cyber criminal activities that need to be studied and defended against.

### Topics

Now in its fourth year, LEET continues to be a unique and leading forum for the discussion of threats to the confidentiality of our data, the integrity of digital transactions, and the dependability of the technologies we increasingly rely upon. We encourage submissions of papers that focus on the malicious activities themselves (e.g., reconnaissance, exploitation, privilege escalation, rootkit installation, attack), our responses as defenders (e.g., prevention, detection, and mitigation), or the social, political, and economic goals driving these malicious activities and the legal and ethical codes guiding our defensive responses. Topics of interest include but are not limited to:

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

### **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; 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.

### **Submission Instructions**

Submitted papers must be no longer than eight (8) 8.5" x 11" pages, including figures, tables, and references, formatted in two (2) columns, using 10 point type on 12 point (single-spaced) leading, with the text block being no more than 6.5" wide by 9" deep. 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 '11 Call for Papers Web site, <http://www.usenix.org/leet11/cfp>.

All 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](mailto:production@usenix.org). The papers will be available online to everyone beginning on the day of the workshop, March 29, 2011.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX LEET '11 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 at <http://www.usenix.org/submissionpolicy>. Note, however, that we expect that many papers accepted for LEET '11 will eventually be extended as full papers suitable for presentation at future conferences.

### **Questions?**

Contact your program chair, [leet11chair@usenix.org](mailto:leet11chair@usenix.org), if you have questions about this Call. For questions related to the USENIX submission policy in particular, contact [leet11chair@usenix.org](mailto:leet11chair@usenix.org) or the USENIX office, [submissionpolicy@usenix.org](mailto:submissionpolicy@usenix.org).