Announcement and Call for Papers USENIX

5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '12)

Botnets, Spyware, Worms, New Emerging Threats, and More

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/leet12

April 24, 2012 **San Jose, CA**

LEET '12 will be co-located with the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI '12), which will take place April 25–27, 2012.

Important Dates

Submissions due: *February 23, 2012, 11:59 p.m. PST*
Notification of acceptance: *March 12, 2012*
Final papers due: *March 26, 2012*

Workshop Organizers

Program Chair
Engin Kirda, *Northeastern University*

Program Committee
Michael Bailey, *University of Michigan*
Davide Balzarotti, *Eurecom, Sophia Antipolis, France*
David Brumley, *Carnegie Mellon University*
Marco Cova, *Lastline Inc. and University of Birmingham*
Mihai Cristoderescu, *IBM Watson Research Center*
Manuel Egele, *University of California, Santa Barbara*
Ulfar Erlingsson, *Google Inc.*
Thorsten Holz, *Ruhr-Universität Bochum*
Jaeyeon Jung, *Microsoft Research, Redmond*
Christian Kreibich, *International Computer Science Institute*
Tim Leek, *MIT Lincoln Laboratory*
Corrado Leita, *Symantec Research, France*
Kirill Levchenko, *University of California, San Diego*
Benjamin Livshits, *Microsoft Research, Redmond*
Niels Provos, *Google Inc.*
William Robertson, *Northeastern 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 distributed command and control frameworks (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 fifth year, LEET continues to be a unique 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. This year, LEET is seeking two types of submissions: 2–4 page industrial position and work-in-progress papers, and regular papers as in the past. Each author will have 10–15 minutes to present his or her work, followed by enough time for discussion with the workshop participants.

Submission Instructions

Submitted regular 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 '12 Call for Papers Web site, http://www.usenix.org/leet12/cfp.

Submitted industrial position and work-in-progress papers 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 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 '12 Call for Papers Web site, http://www.usenix.org/leet12/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. The papers will be available online to everyone beginning on the day of the workshop, April 24, 2012.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX LEET '12 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/submissionspolicy. Note, however, that we expect that many papers accepted for LEET '12 will eventually be extended as full papers suitable for presentation at future conferences.

Questions?

Contact your program chair, leet12chair@usenix.org, if you have questions about this Call. For questions related to the USENIX submissions policy in particular, contact leet12chair@usenix.org or the USENIX office, submissionspolicy@usenix.org.