Announcement and Call for Papers USENIX

3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '10)

Botnets, Spyware, Worms, and More

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/leet10

April 27, 2010 **San Jose, CA**

LEET '10 will be co-located with the 7th USENIX Symposium on Networked Systems Design and Implementation (NSDI '10), which will take place April 28–30, 2010.

Important Dates

Submissions due: *Sunday, February 28, 2010, 11:59 p.m. PST*
Notification of acceptance: *Wednesday, March 24, 2010*
Final papers due: *Monday, April 5, 2010*

Workshop Organizers

Program Chair
Michael Bailey, *University of Michigan*

Program Committee
Dan Boneh, *Stanford University*
Nick Feamster, *Georgia Institute of Technology*
Jaeyeon Jung, *Intel Labs, Seattle*
Christian Kreibich, *International Computer Science Institute*
Patrick McDaniel, *Pennsylvania State University*
Fabian Monrose, *University of North Carolina, Chapel Hill*
Jose Nazario, *Arbor Networks, Inc.*
Stefan Savage, *University of California, San Diego*
Matt Williamson, *AVG Technologies*
Yinglian Xie, *Microsoft Research*
Vinod Yegneswaran, *SRI International*

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

Information technology (IT) adds $2 trillion annually to the US economy alone. While these technologies have enabled significant global economic growth, they have become rich targets for malicious activity. The US Federal Bureau of Investigation (FBI) indicated that cyber crime reached an all-time high in 2008; cyber crime now ranks as the FBI's third highest priority, behind such dramatic threats as counter-terrorism and counter-espionage. Much of this malicious 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: spam, phishing, denial of service, click fraud, etc.

Topics

Now in its third year, LEET continues to provide 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 on. 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
- 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; 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) 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 '10 Call for Papers Web site, http://www.usenix.org/leet10/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 27, 2010.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX LEET '10 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 '10 will eventually be extended as full papers suitable for presentation at future conferences. Questions? Contact your program chair, leet10chair@usenix.org, or the USENIX office, submissionspolicy@usenix.org.