2014 HONEYNET PROJECT WORKSHOP

SPONSORSHIP OPPORTUNITIES

12-14 MAY 2014 | WARSAW

The Honeynet Project is a diverse, talented, and engaged group of international computer security experts who conduct open, cross-disciplinary research and development into the evolving threat landscape. It cooperates with like-minded organizations in that endeavor.

The Honeynet Project, founded in 2000, is an international, non-profit (US 501c3) volunteer research organization dedicated to improving the security of the Internet.

For the past 14 years, the Project has developed tools and conducted research in the information security field and provided it to the public at no cost. Examples of our work include the Know Your Enemy whitepaper series, numerous open-source tools and forensic challenges. We are also an active Google Summer of Code participant. Additional information about the Honeynet Project can be found at http://www.honeynet.org

Annual Workshop

Each year the Honeynet Project's annual workshop, brings together top information security experts from around the globe to present their latest research efforts and discuss insights and strategies to combat new threats. The project workshop provides participants and sponsors with significant exposure to world-class professionals and a diverse range of information security topics. We invite you to be part of our workshop in 2014 through various sponsorship opportunities.

As a non-profit organization, we depend upon external sponsors to help defray costs for the annual workshop. Sponsorship funds help reduce the workshop's expenses, sponsor scholarships for excellent students who are studying in the field, increase attendance of information security professionals by keeping admission cost low, assist in inviting renowned speakers as well as facilitating networking events.

2014 Annual Workshop in Warsaw

Organized by The Honeynet Project and coordinating with CERT Polska under NASK, the next annual workshop will be May 12th to 14th, 2014 at the Adgar Plaza Conference Center in downtown Warsaw, Poland.

The workshop is held over a three-day period and is open to the public. The program will feature an exciting line-up of world-class speakers from The Honeynet Project including Raffael Marty (security visualization), Anton Chuvakin (PCI DSS), Piotr Kijewski and Felix Leder (malware reverse engineering), Tillmann Werner (botnet mitigation), Brian Hay (virtualization security), Angelo Dell'Aera (web security), Mahmud Ab Rahman (mobile malware) and many other experts in their fields.

In addition, the workshop will feature a number of invited top keynote speakers. The preliminary list of keynote speakers includes Federico Maggi/Stefano Zanero from Andrototal, Corrado Leita/Oliver Thonnard from Symantec, and Gadi Evron from Kaspersky Lab.

As in past workshops, hands-on training opportunities will be offered on a number of topics including Malware Reverse Engineering, Android Malware Analysis, Information Visualization, Virtualization Security, Network Analysis and Forensics and other key technical areas.

Past Annual Workshops

Getting Involved: Brainstorming, Information Sharing and Learning

Our Annual workshop is a world-class, non-commercial technical security workshop that provides a collegial environment for information security professionals to exchange ideas, insights and technology.

Previous annual workshops have been held around the world including Dubai in 2013, San Francisco in 2012 with workshop sponsor Facebook, at universities in Paris in 2011 and Mexico City in 2010 and at the United Nations-backed IMPACT Center in Kuala Lumpur in 2009. These annual workshops typically attract over 400 participants and 75 Honeynet Project members from over 32 different countries around the world.

The 2013 Dubai workshop included both a one-day briefing and two-day of hands-on tutorial training . In San Francisco in 2012, our members in collaboration with Facebook presented cutting-edge information on a wide range of information security topics. Workshop courses cover a range of topics including but not limited to forensics, virtualization security, threat assessment, malware reverse engineering as well as more specialized courses such as an experts' course in "Understanding and mitigating botnets". Participants have consistently praised the quality of training and instructor professionalism in our annual Workshop training courses.

2012 SAN FRANCISCO

2011 PARIS

2010 MEXICO CITY

2009 KUALA LUMPUR

2013 Honeynet Project Annual Workshop Group Shot | Dubai, UAE

2014 Annual Workshop Planning

MAY 12–14, 2014

Bringing together world-class experts to share insights, discuss strategies and plan tactical research and development

The 2014 Annual Honeynet Project Security Workshop is being organized in cooperation with CERT Polska under NASK in Warsaw. The CERT Polska is a team of experts responsible for handling incidents related to the .pl namespace. An important part of the team's work is focused on research and developing tools and techniques for the detection and analysis of threats in the cyberspace. This is a mission shared with The Honeynet Project which has developed many tools aiding operations of incident handling teams world-wide.

Hosting the workshop for the first time in Warsaw provides an unique opportunity to interact with world-class security experts and exchange ideas and experiences about the ever-changing threat landscape.

We ask for your support to help make this workshop the most successful ever!

12 May 2014 | Monday
Day 1: Briefings

The first day is a one-day set of briefings whose purpose is to bring together security experts to share their experiences and expertise in security technologies with other local and regional information security professionals. At the end of this day, there will be a post-session networking event to facilitate further discussions among attendees and participants.

13 May 2014 | Tuesday
Days 2: Briefings combined with special demonstration sessions

Briefings continue this morning. In addition, this year we will bring out 8 real demonstration sessions to demonstrate our mature projects and tools that have been developed by Project members. These sessions give workshop participants the opportunity to see the software tools used and explained live, often by the actual authors of the tool. This is a rare opportunity to learn how to apply these free, valuable tools from the developers themselves as well as ask technical questions and gain insight into future developments for these tools and projects.

14 May 2014 | Wednesday
Day 3: hands-on Tutorial training

We will offer hands-on tutorials trainings where we will be running at least 4 concurrent classes, which are 1-day in length. Tutorial session topics will include Malware Reverse Engineering, Android Malware Analysis, Information Visualization, Virtualization Security, Network Analysis and Forensics as well as other important technical topics. Each tutorial is led by an expert in the field from the Project and provides a professional and effective environment to quickly gain experience and expertise in key technical areas.

Sponsorship and Benefits

Explore the Benefits of Sponsorship

Sponsorship is an excellent way to develop new relationships within the security community and provide a forum for sponsors to promote their brand message to the Honeynet Project members, presenters, and attendees. There are several ways to participate in sponsorship.

Scholarship Sponsorship

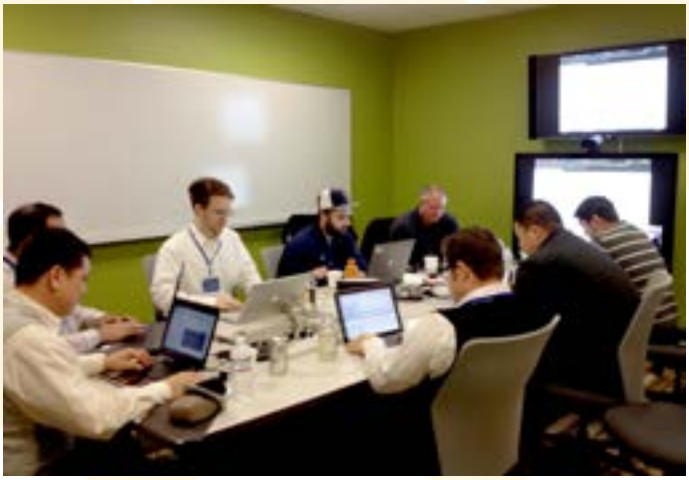
As a part of our educational mission in the field of information security, the Honeynet Project encourages companies or organizations to sponsor student scholarships. Sponsoring a scholarship will offer an excellent student who are studying in this field for a free scholarship seat so that the student can attend the workshop Briefing and a Hands-on Training session where they will learn from world-class security experts and trainers. A student scholarship can be sponsored at $475 USD. Contact us for more details.

Primary Sponsorship

Sponsorship is not limited to packages, but can also take the form of provision of hardware, software, and other logistical support. Lunches and coffee-breaks for three days can be sponsored at $3000 and $4000 USD. The Networking event can be sponsored at the $6000 level.

If you are interested in sponsorship, or have more questions, please contact the Honeynet Project's annual workshop committee for details via e-mail at events@honeynet.org

Small group training session at the Project's Annual Workshop in San Francisco 2012



Sponsorship Level	Platinum	Diamond	Gold	Individual
Cost	USD $10000	USD $5000	USD $3000	USD $1000
Acknowledgement by the Honeynet Project CEO at Welcoming, Session-opening and Closing remarks	YES	YES	YES	YES
Acknowledgement at the Dinner Reception by CEO	YES	YES	YES	YES
A Five-minute Speaking Opportunity at the Dinner Reception	YES	YES		
A Booth at the Workshop Briefings (Day 1 & Day 2)	YES	YES		
A Presentation Slot at the Workshop Briefing (Day 1)	YES			
A Slot at the Demonstration Sessions (Day 2)	YES			
A Jointly Sponsored Press Release	YES	YES		
Logo on Workshop Folder, Registration Page and Printed Brochure	YES	YES	YES	YES
Large Banners at the Venue Facility	YES	YES	YES	
Complementary Tickets to Workshop Briefings and Trainings	8	6	3	1
Advertisement in the Workshop Program	Two-Page	One-Page	Half-Page	
Logo on the Sponsoring Page of the Workshop Website	YES	YES	YES	YES
Logo on the Workshop T-Shirt	YES	YES	YES	YES
Pre-Conference Podcast Interview	YES	YES	YES	
Free Tickets to the Workshop Dinner Reception	8	6	3	1

2013 Workshop Participants

Exchange Ideas with World-Class Information Security Experts

One of the fundamental goals of the Honeynet Project is to share the lessons learned with the security community at large. We foster this goal by publishing papers and tools throughout the year and conducting specialized workshop sessions around the world. The 2014 Honeynet Project Workshop in Warsaw will include an impressive collection of internationally renowned information security professionals, in order to enable us to guide attendees in the use of cutting edge tools and techniques to help protect their constituencies, including the following:

Guillaume Arcas has worked as a threat analyst since 1997, primarily in the Internet/Telco and Banking industries. He specializes in network analysis and forensics and is currently the Team Leader at CERT Sekoia and a member of French Chapter of the Honeynet Project.

Anton Chuvakin is a recognized security expert in the field of log management, SIEM and PCI DSS compliance. He is an author of the books "Security Warrior" and "PCI Compliance".

Angelo Dell'Aera is Information Security Officer at International Fund for Agricultural Development (IFAD), an agency of the United Nations. He's currently Chief Executive Officer of the Honeynet Project. His interests are botnet tracking, honeyclient technologies and malware analysis. His previous research on TCP congestion control algorithms led to the design of the TCP Westwood+ algorithm and the implementation in the official Linux kernel. He's the lead developer of the low-interaction honeyclient Thug.

Brian Hay is a researcher with Security Works and specializes in virtualization and virtual machine introspection. He is the author of the VIX virtual machine introspection toolkit and a frequent speaker and trainer at security conferences.

Piotr Kijewski is the Head of the CERT Polska team at NASK. His main interests in the computer and network security field include threat intelligence, intrusion detection, honeypot technologies and network forensics. Piotr is the author of multiple threat monitoring systems and a frequent speaker at security conferences.

Felix Leder works as an innovation and new technologies architect for Norman ASA. He has has presented classes around the world on malware analysis, reverse engineering, and anti-botnet approaches.

Raffael Marty is a SaaS business expert, data visualization practitioner, and security data analyst. He is a widely sought speaker on visualization and is the author of the book "Advanced Security Visualization."

Mahmud Ab Rahman is a Security Researcher with NetbyteSEC and previously worked for the Malaysia Computer Emergency and Response Team (MyCERT). He has a Masters Degree in Computer Science from the National University of Malaysia. His areas of focus are network security, honeynets, botnet monitoring and malware analysis. He participates in large-scale penetration-testing exercises, training workshops and speaks at many security conferences.

Mark Schloesser is a research assistant at the RWTH Aachen University's IT security group. His main focus is malware collection and botnet monitoring, as well as distributed data sharing and processing.

David Watson the Chief Research Officer for the Honeynet Project and has served on the Board of Directors. As an active security researcher he regularly presents at international conferences or workshops and has contributed to various publications in the field of IT security.

Tillmann Werner is a researcher at CrowdStrike where his duties include the in-depth analysis of targeted attacks. He has a passion for proactive defense strategies like honeypots and botnet takeovers. Tillmann is actively involved with the global IT security community and is a regular speaker on the international conference circuit.