

**30**  
high quality security papers  
in a 2 day conference

13th Association of anti Virus Asia Researchers  
INTERNATIONAL CONFERENCE

# AVAR 2010 BALI

Grand Hyatt Nusa Dua Bali



Conference in  
*Paradise*



Ultimate Sponsor :



Premium Sponsor :



Classic Sponsor :



Media Partners :



# Conference Profile

---

<b>AVAR2010</b>	: AVAR 13th Conference
<b>Host</b>	: AVAR (Association of anti Virus Asia Researchers)
<b>Organizer</b>	: PT. Vaksincom
<b>Date</b>	: 17th (Wednesday) to 19th (Friday) November, 2010
<b>Venue</b>	: Grand Hyatt Nusa Dua, Bali, Indonesia

---

## Conference Fee

Conference Fee	For members of AVAR, ACS, ISIG and SAGE-AU, fee per delegate	For all other delegates, fee per delegate
Early Bird (registration by Friday, October 15, 2010)	USD 450	USD 500
Full Registration	USD 500	USD 550
Optional Hospitality Program	USD 100	USD 120

*Note: When you wire the conference fee, please make sure that you transfer the full amount and that it clearly states that the bank costs will be paid for by you as well. The conference fee is listed above. If total amount received is less than the above specified amount, we will notify you and you can pay the remaining part of the conference fee in cash at the conference registration desk*

**Registration for AVAR 2010** : <http://www.aavar.org/avar2010/registration.html>

---

# Welcome Message



Welcome to the 13th Association of anti Virus Asia Researchers International Conference 2010 in Bali Indonesia, the largest Asia Pacific conference on anti Malware.

I am happy to announce you that it is a first time to take place in Bali Indonesia.

AVAR is not only a conference for virus researchers, but also for corporate IT professionals, students, educators, law enforcement legislators and all who work toward the goals of safe computing and the secure internet.

AVAR is also a conduit for the sharing of information and the building of cooperative relationships with experts from all over the world and from many disciplines. Exposure to this type of information and networking is valuable to those who protect corporate environments, those who study to become the new generation of security experts, and those who already work to secure our digital environment.

AVAR is the ideal event to come to learn and share information with professionals from across the globe.

At the end, I believe Southeast Asia is one of the early success regions which recovered from the world economy recession and I hope this event will be the one of the changes to create an opportunity for expanding the market.

I am looking forward to meeting each of you and to ensuring you have the opportunity to meet the experts who will attend this conference.

## Seiji Murakami

*Chairman  
Association of anti Virus  
Asia Researhders (AVAR)*

# Speakers



**Keynote Speaker :**  
**State of the Net**  
**Mikko H. Hypponen**  
F-Secure

**Getting rich with mobile malware: the how, the where, and the \$\$\$**

**Denis Maslennikov**  
*Mobile Research Group  
Manager, Kaspersky Lab*



**The Difference Between False Positives and False Positives in Testing**

**Mark Kennedy**  
*Distinguished Engineer, Security Technology  
And Response, Anti-Virus/Anti-Spyware  
Engines, Behavior Blocking, Symantec  
Corporation*



**Test Files and Product Evaluation: the Case for and against Malware Simulation**

**David Harley**  
*Research Fellow & Director of  
Malware Intelligence, CISSP FBCS  
CITP, ESET*

**The Power of US**

**Dr. Igor Muttik**  
*McAfee Labs Senior Architect*



**Weightwatching: Why prevalence and persistence matter in Anti-malware testing**

**Andrew Lee**  
*Chief Technology Officer, K7  
Computing*



**The Current State of Sample and Metadata Sharing**

**Dmitry Gryaznov**  
*Sr. Research Architect,  
McAfee Labs*



Welcome to 13th AVAR International Conference in Bali, Indonesia, the leading anti-malware conference in Asia-pacific. As the conference organizer for AVAR2010, it is my pleasure to extend to you an invitation to participate in the AVAR2010 conference. The last 12 years AVAR has grown from a small event to an international recognized conference adding to the awareness of and fight against cybercrime.

to meet industry experts and professionals from across the globe to share and to learn the latest information and techniques in the battle against cybercrime. That cybercrime is a growing problem will not be a surprise for anyone, but this is the time to prepare for the battle in the future. AVAR2010 is the ideal event for this and I look forward meeting you there.

## Righard J. Zwienberg

*AVAR2010 Conference Chair  
Norman Data Defense Systems*



**China Cybercrime and Government Enforcement – the Oriental Dragon Launches Alliance to Improve its Threat Landscape**

**Wei Yan**  
*Security Solution Architect,  
HS USA*



**Adobe: The currently most exploited software in the world**

**Roel Schouwenberg**  
*Senior anti-virus researcher  
Global Research & Analysis  
Team, Kaspersky Lab*

# Conference Program

17 November 2010

Wild List Meeting 09.00-12.00  
AVPD Meeting 13.00-15.45  
AVAR Director Meeting 16.00-18.00

## Day 1 Main Stream | 18 November 2010

Time	Program
08.00-08.50	Registration
08.50-09.15	<b>Welcome Speech</b> Presenter <b>Seiji Murakami</b> , AVAR Chairman <b>Righard Zwieneberg</b> , Conference Chairman <b>Alfons Tanujaya</b> , CEO Vaksin.com
09.15-10.15	<b>Keynote Speaker: State of the Net</b> Presenter <b>Mikko H. Hypponen</b> , F-Secure
10.15-11.00	<b>Buckle up Security Belt When Enjoying Ride on Internet of Things</b> Presenter <b>Peter Wei</b> , Senior Software Architect, Trend Micro <b>Liang-Seng Koh</b> , Trend Micro Inc
11.00-11.15	Coffee/Tea
11.15-12.00	<b>Using Memory Forensics for Identification and Attribution of Malware</b> Presenter <b>Scott Mann</b> , Director, Invest-e-gate Pty
12.00-12.45	<b>Adobe: The currently most exploited software in the world</b> Presenter <b>Roel Schouwenberg</b> , Kaspersky Lab
12.45-13.30	Lunch
13.30-14.15	<b>The rise of icon attacks</b> Presenter <b>Cristian Lungu</b> , Senior Virus Researcher Heuristic Research Team, Proactivity and Kernel Research Department, BitDefender
14.15-15.00	<b>The Fileless Whitelisting and False Positive Testing</b> Presenter <b>Kyu-Beom Hwang</b> , AhnLab, Inc.
15.00-15.45	<b>Getting rich with mobile malware: the how, the where, and the \$\$\$</b> Presenter <b>Denis Maslennikov</b> , Kaspersky Lab
15.45-16.00	Coffee/Tea
16.00-16.45	<b>The Difference Between False Positives and False Positives in Testing</b> Presenter <b>Mark Kennedy</b> , Symantec Corporation
16.45-17.30	<b>Metamorphic Virus: Is it Amenable for Algorithmic Detection?</b> Presenter <b>N.V. Narendra Kumar</b> , Tata Institute of Fundamental Research <b>Vivek Goswami</b> , Dhirubhai Ambani Institute of Information and Communication Technology <b>Richya Bansal</b> , National Institute of Technology
17.30-18.15	<b>An insight into managed downloaders</b> Presenter <b>Scott Molenkamp</b> , Microsoft Corp
19.30-20.00	Drinks before dinner
20.00	Dinner and Entertainment

## Day 1 Back-2-Back | 18 November 2010

Time	Program
11.00-11.15	Coffee/Tea
11.15-11.55	<b>Risking the Symbian OS</b> Presenter <b>Marchelle David</b> , Technical Lead - CA Malware Research, HCL Technologies Ltd.
12.05-13.30	<b>Mobile Malware: Status and Countermeasure</b> Presenter <b>Shihong Zou</b> , Vice President Research Center, NetQin Mobile Inc.
12.45-13.30	Lunch
13.30-14.10	<b>Ready to launch 'Sandbox' now?</b> Presenter <b>Jie Zhang</b> , Manager, Antivirus Team, Fortinet Inc. <b>Raul Alvarez</b> , Fortinet, Inc.
14.20-15.00	<b>High Speed JavaScript Malware Sandbox</b> Presenter <b>Rajesh Mony</b> , Webroot
15.05-15.45	<b>So, what is the government doing?</b> Presenter <b>Hirotake Hayashi</b> , Representative of Ministry of Economy, Trade and Industry (METI), Japan
15.45-16.00	Coffee/Tea
16.00-16.40	<b>Cloudy with a Chance of Malicious URLs</b> Presenter <b>Wing Fei, Chia</b> , F-Secure Labs
16.50-17.30	<b>Portable Document Format or Pretty Dangerous File?</b> Presenter <b>Kazumasa Itabashi</b> , Symantec Corporation
17.35-18.15	<b>Weightwatching: Why prevalence and persistence matter in Anti-malware testing</b> Presenter <b>Andrew Lee, K7</b> <b>Lysa Meyer</b> , West Coast Labs <b>Matt Garrad</b> , West Coast Labs <b>Michael Parsons</b> , West Coast Labs

## Day 2 Main Stream | 19 November 2010

Time	Program
09.15-10.00	<b>China Cybercrime and Government Enforcement - the Oriental Dragon Launches Alliance to Improve its Threat Landscape</b> Presenter <b>Wei Yan</b> , Security Solution Architect, HS USA <b>Fengmin Gong</b> , Chief Scientist, HS USA
10.00-10.45	<b>Network detection of PE structural anomalies and linker characteristics</b> Presenter <b>Gary Golomb</b> - Principal Security Researcher, NetWitness Corporation
10.45-11.00	Coffee/Tea
11.00-11.45	<b>Test Files and Product Evaluation: the Case for and against Malware Simulation</b> Presenter <b>David Harley</b> , CISSP FBSC CIPP, ESET <b>Lysa Myers</b> , West Coast Labs <b>Eddy Willems</b> , G Data's Security Labs
11.45-12.30	<b>Malware Paradox - Persistent Cross Interface Attacks</b> Presenter <b>Aditya K Sood</b> , PhD Candidate Michigan State University <b>Richard J Enbody</b> , Associate Professor, Michigan State University
12.30-13.30	Lunch
13.30-14.15	<b>Is Spam Dying</b> Presenter <b>Rowland YU</b> , SophosLabs, Australia
14.15-15.00	<b>Image spam filtering by optical pattern matching</b> Presenter <b>Evgeny Smirnov</b> , Kaspersky Lab
15.00-15.15	Coffee/Tea
15.15-16.00	<b>Surviving Targeted Attacks: Beyond Today and Tomorrow</b> Presenter <b>Stefan Tanase</b> , Kaspersky Lab <b>Costin G. Raiu</b> , Kaspersky Lab
16.00-16.45	<b>Don't Touch My Winny</b> Presenter <b>Moti Joseph</b> , Former Senior Security Researcher at Websense Security Labs & Check Point
16.45-17.45	<b>Panel: Rogue, anything rogue!?!</b> Panelchair <b>Righard Zwieneberg</b> , Norman Panelist <b>Andrew Lee, K7</b> Panelist <b>Lysa Meyers</b> , West Coast Labs Panelist <b>David Harley</b> , ESET Panelist <b>Tony Lee</b> , Microsoft
17.45	Closing Ceremony
18.00	AVAR Members Meeting

## Day 2 Back-2-Back | 19 November 2010

Time	Program
09.15-09.55	<b>Sponsor Presentation: Hot Topics in Modern Malware</b> Presenter <b>Andrew Lee, K7</b>
10.05-10.45	<b>The Power of US</b> Presenter <b>Dr. Igor Muttik</b> , McAfee Labs Senior Architect
10.45-11.00	Coffee/Tea
11.00-11.40	<b>An Automated Malware Processing Lab</b> Presenter <b>Jim Cai</b> , Fortinet, Inc.
11.50-12.30	<b>The Current State of Sample and Metadata Sharing</b> Presenter <b>Dmitry Gryaznov</b> , McAfee Labs
12.30-13.30	Lunch
13.30-14.10	<b>Behavior-Based Detection for file infectors</b> Presenter <b>Rajesh Nikam</b> , Quick Heal Technologies Pvt Ltd
14.20-15.00	<b>Cleanup to Damage Recover -Solution for PE Virus Infection and Beyond</b> Presenter <b>Zhihe Zhang</b> , Trend Micro, Inc.
15.00-15.15	Coffee/Tea

## Reserve Papers

Title	Speaker
Targeting your Source Code: Stuxnet, Aurora, Induc and New Attack Vectors targeting global brands	<b>Moderator</b> : <b>Mario Vuksan</b> <b>Panelists</b> : <b>Randy Abrams</b> (Eset) <b>Jonathan Poon</b> (Microsoft) <b>Jamz Yaneza</b> (Trend Micro) <b>Roel Schouwenberg</b> (Kaspersky) <b>Righard Zwieneberg</b> (Norman) <b>Possible Panelist</b> : <b>Zhang Jian</b> (Tianjin CCCERT)

# More Information

## Conference Venue; Grand Hyatt Nusa Dua, Bali

Grand Hyatt Bali Hotel is the crown jewel of resorts in Nusa Dua, the luxury stretch of magnificent beachfront on the island of Bali.

Grand Hyatt Bali was conceived as a water palace with lakes, landscape gardens and five lagoon or river pools surrounding low-rise Balinese style buildings. Our Bali resort offers the comfort of a world class hotel with the relaxing tranquillity of a secluded beach resort. Recreational facilities include the 24-villa Kriya Spa designed as an exotic water palace, Bali Golf & Country Club 5 minutes away and a variety of water activities.

The resort is just a short distance from Sanur, Kuta and the city of Denpasar, while Ngurah Rai Airport is only 12 km away.

## Book Your Accommodation

To book your hotel room, please visit the hotel's website at :

<http://www.aavar.org/avar2010/venue.html>



## Some Information about BALI

Bali is an Indonesian island that is rich in indigenous culture. A lot of people say that Bali culture is unique and that the people of Bali have always been contented with the "now." If you ask a Balinese person what heaven is like, the probable answer will be "Just like Bali". This only goes to show that most Balinese people are happy to be where they are and never worry.

Hinduism is the main religion in Bali. The Bali culture is based on a form of this religion, which is called "Hindu Dharma". This religion reached the island during the eleventh century. Most of the family customs and traditions as well as community lifestyles of the Balinese people are influenced by this. The religious influence even expands widely into the arts, which makes Bali distinct from the rest of Indonesia.

In spite of the influx of tourists to the island, Balinese people have managed to preserve their culture. Almost every native of Bali is an artist in some form or another. Parents and villagers have passed on their skills to their children, who all seem to have inclinations either to music, dance, painting and decor.

Indeed, Bali has a rich culture, making it distinctive from the rest of the islands in Indonesia. Bali is renowned for its diverse and sophisticated art forms, such as paintings, sculptures, woodcarvings, handicrafts and performing arts. Balinese percussion orchestra music, known as gamelan, is highly developed and varied. Balinese performing arts often portray stories from Hindu epics such as the Ramayana but with heavy Balinese influence. Famous Balinese dances include pendet, legong, baris, topeng, barong, gong kebyar, and kecak (the monkey dance). Bali boasts one of the most diverse and innovative performing arts cultures in the world, with paid performances at thousands of temple festivals, private ceremonies or public shows.



## Visa Information

A Tourist Visa is for tourists who are visiting Indonesia. During their stay in Indonesia, the tourist visa cannot be extended and cannot be converted into another type of visa. The maximum stay for tourist visa is 30 days.

Since May 3, 2006, the government has new visa system with 3 categories:

### 1. Pay for Visa-On-Arrival system. This system is for citizens of:

Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Egypt, Emirates Arab, Finland, France, Germany, Holland, Hungary, India, Iran, Ireland, Italy, Japan, Kuwait, Luxembourg, Maldives, New Zealand, Norway, Oman, Poland, Portugal, Qatar, P.R.China, Russia, Saudi Arabia, Spain, South Africa, South Korea, Sweden, Switzerland, Taiwan, United Kingdom, USA

The Visa-On-Arrival facility will only be available at the following airports: Bali, Jakarta, Medan, Manado, Padang, Pekanbaru and Surabaya.

The cost of 30-day tourist visa is USD. 25,- per person.

### 2. Visa-Free facility which is valid for 30-day is granted to the citizens of 11 countries:

Brunei Darussalam, Chile, Hongkong Special Administrative Region, Macao Special Administrative Region, Malaysia, Morocco, Peru, Philippines, Singapore, Thailand, Vietnam

### 3. Citizens of other countries NOT on the Pay Visa-on Arrival or Visa-Free facility lists will be required to apply for a visa at the Indonesian Embassy overseas in their home country before entering Indonesia.

## Registration

17 November 18:00  
18 November 08:00

Wednesday  
at Lagoon Pool, Grand Hyatt  
Nusa Dua - Bali

## Cocktail Welcome Reception

17 November

Wednesday  
at Lagoon Pool, Grand Hyatt  
Nusa Dua - Bali  
19.00 - 21.00

## AVAR 2010 REGISTRATION

<http://www.aavar.org/avar2010/registration.html>

## For more details please visit

AVAR official webpage <http://www.aavar.org>

AVAR 2010 official webpage <http://www.aavar.org/avar2010/>

AVAR 2010 official email address [avar2010@aavar.org](mailto:avar2010@aavar.org)

## AVAR2010 Organizing Committee

PT. Vaksincom

Phone: +62 21 345 6850, Fax: +62 21 345 6851

Email: [avar2010@aavar.org](mailto:avar2010@aavar.org)

Mail: Tanah Abang III / 19 E - Jakarta 10160

Web: <http://www.vaksin.com>