



Asia-Pacific  
Economic Cooperation



## **DRAFT Annotated APEC-OECD Malware Workshop Agenda TEL 35, Manila, The Philippines April 22 and 23, 2007**

### **Presentation of the workshop (orientation document and agenda overview)**

Many computer systems are compromised around the world everyday due to malicious code and malicious software, commonly known as “malware.” This combined with a reducing ability to detect and remove such malware leads to an increased proportion of compromised computers connecting to the Internet. In this context, governments, businesses, consumers and civil society are all concerned and need to take action. The Asia Pacific Economic Cooperation Telecommunication and Information Technology Working Group (APEC TEL) Security and Prosperity Steering Group (SPSG) and the Organisation of Economic Cooperation and Development (OECD) Working Party on Information Security and Privacy (WPISP) have decided to cooperate to better tackle the international dimension of information security risks such as malware and to examine options to address them.

This workshop is one of two inter-related components of joint APEC-OECD work on malware. The second component is an analytical report currently under development. The discussion and outcomes from the workshop are expected to further inform the report, a draft of which will be made available at the SPSG and APEC TEL 36 meetings.

### ***Objectives***

This workshop brings together representatives from the various communities addressing malware in order to inform policymakers of the issues and gain a better collective understanding of:

- the malware landscape, how it has changed and the most important issues of concern;
- the roles and responsibilities of various communities from governments to vendors to civil society in combating malware;
- the challenges to addressing malware and available mechanisms for combating it; and,
- how cooperation mechanisms, both domestic and cross-border, can be improved to better combat malware.

### ***Workshop format***

The workshop is organised to facilitate discussion among session participants and with the audience. Most sessions will begin with brief presentations followed by questions/answers with panellists and the audience.

A summary of the workshop discussion and outcomes will be made available.

## **Day 1 – April 22<sup>nd</sup>**

### **0900 – 0920 Introduction**

*This session sets the stage for the workshop.*

Society today is increasingly reliant on information systems and networks to conduct business, government and individual activities. Although data and statistics on malware growth and trends are not easily comparable in real and absolute terms, most sources and experts agree that the use of malware by malicious actors to compromise information systems and networks is on the rise.

There is no single explanation for the increased occurrence and use of malware. Rather, several factors contribute to this phenomenon including: the growing number of Internet users; the amount of services available online; the ability to make significant money with malware; the challenges faced by end users to securely manage their system; the demand for illegal services; the availability of malware that is easy to use; and, the number of vulnerabilities.

**Workshop Co-Chairs:** *Shamsul Jafni Shafie and Keith Besgrove*

➤ **Welcome Remarks by Philippines Commission on Information Communications and Technology (CICT)**

Commissioner Angelo Timoteo Diaz de Rivera

➤ **Welcome Remarks by TEL Chair**

Dr. Inuk Chung

➤ **Objectives of the Joint APEC-OECD Work on Malware and General Introduction to the Day**

Shamsul Jafni Shafie (Convenor, SPSG-APEC TEL) and Keith Besgrove (Chair, WPISP-OECD)

### **0920 – 1100 Session 1 - Trends & Overview: Why is Malware an Important Issue?**

*This session is designed to give workshop participants background information on the general issues concerning malware, including its rate of evolution and impact on various communities.*

Malware is a general term for software code or program inserted into an information system in order to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners. Malware is being used both as a primary form of cyber attack and to support other forms of cybercrime.

Malware is an effective and efficient means for attackers to compromise large numbers of information systems, which cumulatively, undermines and erodes trust in these systems. All users of information systems and networks can be affected by malware and therefore all should be concerned. The compromise of information systems can have national security implications for governments and severe financial implications for businesses and consumers.

In many cases, the consequences of inadequate security measures against malware are “external” or borne by others. For example, if one user is inadequately protected and allows their systems to become infected by malware, those can be used as a platform to launch attacks against other users’ systems. Thus, every computer user’s security directly impacts the security of other computer users.

**Moderator:** *Keith Besgrove*

➤ **Issues and problems, rate of evolution**

National Computer Network Emergency Response Technical Team Coordination Center (CNCERT/CC) – China

Dr. Yuejin Du

➤ **Impact on Business**

Association for Payment Clearing Services (APACS) – United Kingdom (UK)

Colin Whittaker

➤ **Impact on Government**

Department of Communications Information Technology and the Arts (DCITA) – Australia  
Sabeena Oberoi

➤ **Impact on Government**

Ministry of Internal Affairs and Communications - Japan

Mr. MURAKAMI Satoshi

Ministry of the Economy Trade and Industry - Japan

Mr. MURANO Masayasu

➤ **Impact on consumers**

Consumers Report WebWatch

Beau Brendler

**1100 – 1230 Session 2: Malware in Focus**

*This session is designed to explore more detailed aspects of malware including, how it works, how it is used, and who is behind malicious activities using malware.*

Malware is able to compromise computer systems due to a combination of factors including insecure operating system design, software vulnerabilities, poor user practices, and inadequate security policies and procedures. There are numerous types of malware that can be used separately or in combination to conduct a variety of attacks, usually some form of information theft or denial of service.

Many forms of malware require some level of user interaction to initiate the infection process (i.e. clicking on a web link in an email, opening an executable file attached to an email, or visiting a web site where malware is installed). Once the security of an information system has been breached with an initial infection, some forms of malware automatically install additional functionality, known as the payload. The payload could be a keylogger or other type of spyware, a backdoor, rootkit or anything else that the malicious actor wishes to install.

Some malware is distributed using botnets. A botnet is a group of “zombies” or bot infected computers compromised through malware and turned into malware that can be used to carry out attacks against other computer systems. These computers become compromised when a bot program, a type of malware, is installed on the system.

The growing complexity of information systems and networks has resulted in an increasingly complex community of malicious actors developing and deploying malware. Research shows that the range of malicious actors spans from malicious code innovators to amateurs seeking fame and media attention to serious organized cyber criminals. These malicious actors have various motivations from fame to financial gain.

**Moderator: Shamsul Jafni Shafier**

➤ **Malcode**

Computer Emergency Response Team / Coordination Center (CERT/CC)

Kevin Houle

➤ **Botnets**

Computer Emergency Response Team for the Dutch Government (GovCERT.NL) – The Netherlands

Douwe Leguit

➤ **Who is behind malware, their capabilities and activities?**

Postal and Communications Police Service - Italy

Sergio Staro

➤ **What are the challenges (all types) to combating malware?**

Microsoft UK

David Pollington

**1400 – 1620 Session 3: Identifying Counter Measures and Capabilities for Response to Cyber Attacks**

*This session is designed to discuss the mechanisms that exist within various communities for responding to cyber attacks using malware as well as to identify gaps to those responses. Following presentations from a panel of representatives from the CSIRT, anti-virus vendor, regulatory, law enforcement and domain name system communities, a case study will be presented and the panel will be invited to give “real world” reactions on how they would respond, what measures they would take, with whom they would coordinate etc. Participants in the audience will also be invited to react.*

A number of communities have varying levels of competence, resource, mandates and responsibility to prevent, detect and respond to malware attacks and malware-related cybercrime:

- Home users and SMEs who should be aware of the risks to information systems and should employ safeguards as a first line of defense for the protection of their information systems and networks.
- Public and private sector organisations who should be aware of the risks to information systems and should employ safeguards as a first line of defense for the protection of their information systems and networks.
- ISPs who manage the networks which the aforementioned groups connect to for access to the Internet and telecommunications regulators who develop policy and/or enforce how providers operate.
- Domain name registrars and regulators who determine if a domain is allowed to be registered and potentially have the power to deregister a domain that is registered purely for fraud or other criminal activity, including, for example, the distribution of malware.
- CSIRTs who have a role to play in coordinating nationally and internationally to detect and respond to cyber attacks affecting their constituency or emanating from their constituency and issuing security bulletins about the latest computer network threats or vulnerabilities associated with malware attacks.
- Anti-virus and software vendors whose products can avoid or limit potential harm from threat and vulnerabilities associated with malware.
- Information or cyber security agencies within governments, whose policies and procedures can impact the ability to prevent, detect and respond to malware.
- Law enforcement who investigate various forms of cybercrime.

**Moderator:** Keith Besgrove

➤ **Current counter-measures and responses by CERTs**

Korea Internet Security Center KrCERT /CC - Jeong, Hyun-Cheol

GovCERT.nl - Douwe Leguit – panellist only

➤ **Current counter-measures and responses by anti-virus vendors**

F-Secure – Finland - Patrik Runald

➤ **Current counter-measures and responses by regulators in partnership with Internet Service Providers (ISPs) and domain name registrars**

Philippine Internet Services Organization (PISO) - Horatio Cadiz

➤ **Current counter-measures and responses by law enforcement bodies, including through public private partnerships**

Department of Justice (DOJ) – United States of America (USA) - Anthony Teelucksingh

➤ **Current counter-measures and responses by domain name registrars**

### **CASE STUDY SCENARIO\***

#### ***Summary and objectives of the attack***

- series of related cyber attacks that occur over approximately a six month period
- in the public domain
- uses spam email to infect (compromise) the computers of many thousands of Internet users around the world
- country A is most affected although countries B, C, and D are also greatly affected
- principal attack tool is several variants of a multi-functional trojan and associated malware
- the trojan enables the system compromise of vulnerable computers
- captures and transfers passwords, other online access credentials, and web form data

#### ***Features of the attack include:***

- Compromised hosts using legitimate domains involved in the attack are located in several countries
- Registered fraudulent domains involved in the attack are registered in several countries
- 34,553 computers compromised (by unique IP address) around the world

*\* A list of questions for the panelists and audience will be distributed before this session of the workshop*

**Case Study moderator:** Graham Ingram - Australian Computer Emergency Response Team (AusCERT) – Australia

### **1620 – 1720 Session 4: Panel Discussion: Gaps and Challenges**

*Building on the discussion in the previous session, the purpose of this session is to help identify challenges and gaps to existing countermeasures and areas for improvement for fighting malware.*

Panellists are invited to consider the following broad topic areas to identify possible gaps in combating malware:

- Nationally coordinated user awareness raising programs
- Naming conventions
- The role of CSIRTs
- The role of ISPs and Domain Name Registrars
- The roles of the vendor community
- The role of government
- Law Enforcement
- Legal Frameworks
- Intellectual property concerns for the reverse engineering of malware
- Skills and capabilities
- Resources
- Information Sharing

**Moderator:** Shamsul Jafni Shafie

**Panellists:**

- Department of Homeland Security (DHS) US Computer Emergency Readiness Team (US-CERT), USA  
Josh Goldfarb
- DCITA, Australia  
Sabeena Oberoi
- CNCERT, China  
Dr. Yuejin Du
- Information & Communication Security Technology Center, Chinese Taipei  
Pei-wen Liu
- International Telecommunications Users Group (INTUG),  
Rosemary Sinclair
- Outblaze Limited, Hong Kong  
Suresh Ramasubramaniam
- Communications Technology Labs, INTEL  
Ravi Sahita

**Comments and wrap up of session and day 1**

Andy Purdy

## **Day 2 – April 23<sup>rd</sup>**

### **0900 – 1030 Session 5: Break Out Group Discussion**

*This session provides an opportunity for each community involved in fighting malware to discuss issues specific to their roles and responsibilities. A moderator will introduce the discussion. However, **all attendees** are encouraged to participate and propose ideas for how efforts to combat malware can be improved.*

Sample breakout group questions\*:

1. What is our community's role in combating malware?
2. What mechanisms exist for our community to combat malware?
3. What steps would be taken to respond to an attack using malware? Is it the same for attacks that may not employ malware (i.e., Phishing)?
4. Who would we coordinate with? Would we go across borders to other governments, organisations or entities to effectively respond?
5. Which mechanisms are the most effective? Which are the least effective?
6. Are there examples of successful cross-border cooperation for combating malware?
7. In an ideal world, what would we be able to do that we can not do today?

\*The discussion in each breakout group will be reported in plenary Session 6

#### ***Breakout group moderators:***

- **Break Out 1: How can vendor, CERT, ISPs, domain name registrars response be improved?**  
APACS – UK - Colin Whitaker  
Introduction to be provided by the Organization of Economic Cooperation and Development (OECD)  
- Peter Lübker
- **Break Out 2: How can government policy, law enforcement and regulatory response be improved?**  
Department of Justice (DOJ) – United States of America (USA) - Anthony Teelucksingh
- **Break Out 3: How can awareness, education, and training of individuals business – in particular SMEs – and users be improved?**  
INTUG - Ernie Newman
- **Break Out 4: How to address the economic impacts of malware?**  
Delft University – The Netherlands - Michel van Eeten

### **1100 – 1230 Session 6: Wrap Up and General Discussion**

*This session is designed to foster a general discussion on the findings of the workshop, including the breakout groups, with the objective of looking to the future (will the malware trend continue?), highlighting conclusions from the workshop (short term and long term solutions) and identifying areas for possible recommendations (both domestic and cross-border) for policymakers.*

**Moderators:** Shamsul Jafni Shafie and Keith Besgrove

- **Report by Break Out Groups moderators – suggestions for improvement - and comments from the wider workshop participants**
  - APACS – Colin Whittaker
  - DOJ – USA - Anthony Teelucksingh

- INTUG - Ernie Newman
- Delft University - Michel van Eeten
- **General discussion with the audience on how to improve government policy and international frameworks for cyber response/security and final wrap-up**  
Andy Purdy
- **Conclusions of the Workshop**  
*Shamsul Jafni Shafie and Keith Besgrove*