ONAL CRIMINAL POLICE ORGANIZATION
ACIÓN INTERNACIONAL DE POLICÍA CRIMINAL

ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE
المنظمة الدولية للشرطة الجنائية

INTERPOL

Invitation

To Heads of NCBs
Directors/Heads of Cybercrime Units

Date 4 December 2017

Our Ref. 2017/350/I/IGCI/CD/DIS/SS/jg

Contact Mr. HONG Sung Jin
Mr. Javad GANJALI
Digital Crime Officers
Cybercrime Directorate

Subject INTERPOL Advanced Malware Analysis Training on 19-23 February 2018 in Manila, Philippines and on 26-30 March 2018 in Lyon, France

Dear colleagues,

Following the two well-received training sessions on Malware Analysis in 2017, the INTERPOL Cybercrime Directorate is pleased to present two more training sessions on Advanced Malware Analysis to be held in 2018 to meet the huge demand of member countries:

- Session 1 to be held on 19-23 February 2018 in Manila, Philippines
- Session 2 to be held on 26-30 March 2018 in Lyon, France

The above two training sessions have similar contents and structure, and will be supported by Trend Micro in capacity of partner of INTERPOL, with their extensive expertise in the area of cyber security and malware analysis.

1. Aims & Objectives

The aim of this training is to offer an advanced level of knowledge on malware analysis tools and techniques. The training course will focus on establishing knowledge and skillsets on:

- Malware classification
- Static malware analysis tools and techniques
- Behavioral malware analysis tools and techniques
- Attack scenarios and techniques
- Ransomware and behavioral analysis
- Online banking malware
- PoS malware
- Countermeasures

A significant part of the training course will focus on practical exercises on above topics.

2. Prerequisites for participants

This training course will be an advanced training; participants should be practitioners in cybercrime investigation and possess the following skills:

- Internet fundamentals
  - Can explain illegal activity and harmful information in internet.
  - Can explain the following mechanisms of Internet:
    - IP address, DNS (including WHOIS)
    - Access of web site, e-mail sending/receiving, role of servers
    - Internet connections (mobile, Wi-Fi, ISP)
    - Encrypted connections (HTTPS/SSH), P2P connections
  - Can understand overview of network from standard specification document.
  - Can assessment network by the command of Ping/ traceroute/ ipconfig/ telnet.
  - Can trace network traffic with extracted network packets
  - Can evaluate re-transmission packets by tools
  - Can explain credibility of information, when identify IP address as "send from".
  - Can record software service by banner grabbing.
- Open Source Intelligence (OSINT)
  - Can search with Boolean operation on search engines.
  - Can search with Wild card on search engine
  - Can analyze the fact for identification from multiple data sources such as social network, blog/forum, geo-locational information, image/video and so on.
  - Can trace back to the fact from forged contents.
- Malware Analysis
  - General knowledge on malware classification.
  - Understand basic activities and behaviors of malware.
  - Can evaluate and analyze malware behavior with comparing difference between before/after.
  - Can analyze malware against camouflaged deceiving.
  - Know auto-start mechanisms (such as RUN, Task schedule in Windows) for programs.

3. Language

The training will be conducted in English only. Please note that there will be no interpretation services provided.

4. Participants

Participants must be from law enforcement agencies that deal with the investigations of cybercrime or other technology enabled crimes or specialists in digital forensics that meet the requirements outlined above.

5. Capacity

The capacity is limited to 20 slots for Manila session and 18 slots for Lyon session, and registration will be handled on a first-come first-served basis.

If there is more than one nomination from a member country, the acceptance of the second and subsequent nominations will be subject to capacity after the deadline of registration.

A confirmation of acceptance or rejection to the registration will be sent to NCB and the applicant.

We may transfer participants registered for Manila session to Lyon session given it is agreeable by participants if we reached the maximus capacity for Manila session.

Pre-assessment of trainees

pre-assessment will be conducted to assess applicants' technical skill and vet appropriate participants. Once receive the application, a web link will be sent to applicant's personal Email address indicated in the registration form to proceed the pre-assessment.

7. Expenses

Participants will be responsible for covering the costs of their own travel to and from the venue, accommodation, meals and any additional or incidental expenditure they incur including any medical costs/insurance.

8. Visa Requirement

All participants are required to have a passport valid for the duration of their intended stay. The responsibility to obtain travel visas (if applicable) remains with the participants. Should you require a supporting letter from INTERPOL for your visa application, please contact Mr. Javad **GANJALI**.

9. **Venue, date and hotel reservations**

The Manila session will be held from 19th to 23th February 2018 at 8/F The Rockwell Business Center Tower 2 Ortigas Avenue, Pasig City, Metro Manila Philippines 1600.

The Lyon session will be held from 26th to 30th March 2018 at the INTERPOL General Secretariat, 200 Quai Charles de Gaulle, 69006 LYON, FRANCE.

According to our circular N°.13/DI/AGN/99 of 31 January 2000, the INTERPOL General Secretariat no longer makes hotel reservations for participants. However, in order to help participants to make these reservations themselves, please find enclosed the lists of recommended hotels for the two training sessions.

10. Registration

Please find attached the registration form to send in your nomination with a scanned copy of the participant's passport via e-mail to EDGCI-CD@interpol.int, by 20th January 2018 for Manila session and by 26th February 2018 for Lyon session.

Participants will be provided with further details regarding the training such as the agenda in due course. It would be highly appreciated if you could support this event and send your representatives to the INTERPOL Advanced Malware Analysis Training.

For further consultation, please contact **Mr. Sung Jin HONG** or **Mr. Javad GANJALI**, Digital Crime Officers, INTERPOL Cyber Crime Directorate, at EDGCI-CD@interpol.int .

Yours faithfully,

Silvino SCHLICKMANN Junior
Director
Cybercrime Directorate
INTERPOL

INTERPOL

REGISTRATION FORM

INTERPOL Advanced Malware Analysis Training, Manila and Lyon 2018

Note

- Each applicant should send a duly completed Pre-Registration Form by e-mail to the Cybercrime Directorate, IGCI, at EDGCI-CD@interpol.int
  - For Manila Training before 20TH January 2018
  - **For Lyon Training before 26TH February 2018**
- Each applicant should fill in the Pre-Registration Form by word processor and submit it as a Word document. Handwriting should be avoided.
- Each applicant should fill in his/her name in the Pre-Registration Form exactly as it is written on his/her passport.

- I would like to attend in □Manila Training □Lyon Training
- If the registration for Manila Training reached the maximum capacity, I agree to be transferred to the Lyon training list.

YES□ NO□

Personal details	Given name (forename) *(exactly as written on passport)*:		
	Family name *(exactly as written on passport)*:		
	Date of birth:		*(dd/mm/yyyy)*
	Place of birth:	Town/city:	
		Country:	
	Current nationality:		
	Other nationality(-ies):		
	Please attach a photocopy of your passport to this form		

Contact details at work	No. and Street:	
	Zip/Postcode:	
	Town/city:	
	Country:	
	Telephone (with country and city code):	
	Mobile phone No.:	
	Fax:	
	E-mail:	

Professional Experience	*List positions held in reverse order (starting with the current/latest one),* ***highlighting your involvement in cybercrime-related operations/investigations.*** *Please continue overleaf if necessary.*		
	Total number of years' experience in the area of cybercrime:		
	Organization:		
	Current position:		
	Rank/grade:		
	Job title:		
	Date	From:	*(mm/yyyy)*
		Please indicate date of next transfer, if known:	
	Description of your duties and responsibilities:		
	Previous position:		
	Job title:		
	Date	From:	*(mm/yyyy)*
		To:	*(mm/yyyy)*
	Description of your duties and responsibilities:		