Call for Interest for the INTERPOL Digital Crime Centre – 2nd round (area of advanced technology required for the Malware/BotNet analysis)

(CFI-12-IGCI-02)

Background

INTERPOL recognizes that police worldwide are facing an increasingly challenging operational landscape as criminals take advantage of new technology, the ease of international travel and the anonymity of doing business virtually. As criminal phenomena become more aggressive and elusive, notably in the area of cybercrime committed through the exploitation of technology, INTERPOL has embarked on a programme of innovation, which will see the opening of the INTERPOL Global Complex for Innovation (IGCI) in May 2014 in Singapore.

Complementing the General Secretariat Headquarters in Lyon, France, the purpose of the INTERPOL Global Complex for Innovation is to enhance INTERPOL's capability to tackle the crime threats of the 21st century and strengthen international policing worldwide.

The INTERPOL Digital Crime Centre will be the driving force of the Complex. Its activities will cover a range of areas essential to the assistance of national authorities: cybercrime investigation support, research and development in the area of digital crime, and digital security.

Two of the core elements of the Centre, and the subject of this Call for Interest, are the Digital Forensic Lab and the Cyber Fusion Centre.

Digital Forensic Lab:

The lab is expected to be a centre of excellence for forensic technology in the law enforcement community. The Lab has been allocated approximately 60-80m² in the Complex and is expected to be staffed by approximately 5 IT experts and investigators seconded from member countries and other external entities. It does not, however, aim to centre on academic research on cybercrime and cyber security; rather it will focus on practical technology that provides investigators with the capacity to better coordinate and conduct national and regional investigations.

The activities of the Lab can be broken down into 4 key areas which will, in conjunction with one another, provide the tools, intelligence and expertise required, as identified by law enforcement stakeholders themselves, to more effective combat cybercrime.

Trend Analysis

- The Lab will conduct strategic trend monitoring, and analysis of emerging crimes and threats to digital security through the employment of appropriate scientific methodologies.

- The Lab will engage strategic stakeholders, including the law enforcement community, research laboratories and institutions, academia, and the public and private sectors, to conceptualize and design state-of-the-art technological innovations that address current and future cybercriminal activities.

Testing Forensic Tools

- The Lab will identify, using Open Source Intelligence (OSInt) and partnership contacts, commercial and non-commercial Digital Forensic tools developed by private sector, academia and national level research laboratories.

- The Lab will drive, initiate and co-ordinate collaborative test-bedding of cutting edge IT tools, services and protocols that push the frontiers of cybercrime fighting and digital security, as well as advance the use of digital identity technologies and digital forensics.

Development of Best Practices

- The Lab will drive, initiate and coordinate collaborative research projects in innovative IT solutions with the view of improving digital-forensics capability and the use of digital identity technologies and other policing IT tools.

- The Lab will identify, develop and share Best Practices for cyber-incident preparedness and prevention as well as for incidence response activities.

- By using the results of the evaluation of digital forensic tools and techniques, and analytical reports regarding trend analysis, Standard Operating Procedure (SOP) for crime investigation shall be developed and shared with member countries.

Capacity Building and Training

- The Lab will develop and provide career development trainings for examiners, investigators and other first responders to ensure that they possess the latest knowledge of cybercrime trends, and the usage of digital forensic tools and techniques.

- The Lab will develop multi-level training modules/courses and materials with categorized core skill-sets and competencies for examiners and investigators.

- The Lab will operate a knowledge bank of modules/courses and materials to be accessed from member countries in order to facilitate information-sharing and maintain momentum of cyber security capacity-building.

<u>Cyber Fusion Centre</u>

The Fusion Centre will provide essential assistance to the Cybercrime Investigative Support (CIS) sub-directorate so that INTERPOL's member countries receive the intelligence and expertise required to effectively investigate cases of cybercrime.

The Fusion Centre will function in a manner similar to INTERPOL's Command and Coordination Centre, providing real-time monitoring of the network and analysis of malicious Internet activities. The Fusion Centre is expected to be housed in approximately 100-150m² and staffed by approximately 10 people.

The functions of the CFC will be divide into two complementary areas: Intelligence and Law Enforcement (L.E.) Action.

Intelligence

The Intelligence function of the Fusion Centre will be supported by personnel from Law Enforcement, Industry and Academia. The Intelligence function will:

- Conduct real-time analysis of threat feeds supplied by industry, package data, network activity, and other information and intelligence from open and friendly sources (such as IMPACT) in order to provide a holistic overview of malicious Internet activity, evaluate threats and action the information as needed.

- Generate analytical reports for member countries on the threats and actual problems identified in their countries to encourage discussion and multistakeholder efforts to improve the situation and thereby prevent crime.

- Produce an INTERPOL Cybercrime Treat Assessment or white papers from a the law enforcement perspective, which will identify cybercrime threats and encourage global action by pinpointing the cybercrime hotspots around the world.

- Supply relevant operational data to the L.E. Action personnel.

L.E. Action

Activities will be conducted by Law Enforcement personnel allowing for case-oriented analysis drawn from the Intelligence side of Fusion Centre to be turned into solid, intelligence driven identification of criminals.

- Consolidate criminal analysis of crime trends and turn this analysis into concrete operational action.

- Provide cybercrime expertise to national cybercrime units during investigations or coordinate cross border cybercrime investigations when there is not sufficient capacity.

- Deploy investigative support teams to assist national law enforcement agencies during investigations following a serious cybercrime incident.

Support Sought

INTERPOL has already identified some of the equipment, resources and information needed for the establishment and effective operation of the Lab and Fusion Centre. INTERPOL requests that interested parties take into consideration these requirements but also provide other additional proposals that will allow the Lab and/or Fusion Centre to fulfil its core activities, in particular, INTERPOL focuses upon the area of advanced technology required for the Malware/BotNet analysis. Identified items include:

Equipment and Tools

Contributions towards the furnishing of the DFL and CFC could be in-kind or purely financial.

- High specification computer workstations and servers
- Hardware and software for real-time monitoring and visualisation of network conditions, threat levels, incidents and network infections.
- Data storage and analysis facilities
- Licences and maintenance for Windows (XP, Vista or 7) and Virtual (VM) operating systems

- Licences and maintenance for essential word processing and analytical software packages
- Forensic tools, including: Encase, FTK, H/W & S/W type HDD Duplication devices,/tool, Sandbox or equivalent virus testing environment, mobile exploitation forensic tools
- Non-IT specific forensic tools: Video Surveillance/monitoring system, biometric devices (Facial, DNA, iris and other recognition)

Human Resource Support

- Software Examiners: duties would include malware and botnet analysis, testing of forensic tools, compilation of reports and development of best practices.
- Criminal Intelligence Analysts: trend analysis of cybercrime operandi and cyber security-related technology, and open source intelligence (suspects and incidences) collection.
- Technical Support: Assistance in configuring computers/networks/devices, trouble-shooting, and emergency response assistance when required.

Information and Intelligence Gathering

- Provision of cybercrime and security-related intelligence with regards to cybercrime and incidents; and emerging threats, including vulnerabilities and hot-fixes.
- Access to security-related data or databases: access to database storing raw packet data, and malicious packet collections for analytical purposes.

~~~~~~

INTERPOL invites interested companies and technological institutions to assist in the design, establishment, maintenance and partial-operation of the Digital Forensics Lab and/or Cyber Fusion Centre for a period of at least 3 years by providing technical equipment and tools, technical assistance and expert human resources[1].

INTERPOL is soliciting interested parties to produce their own proposals for the establishment of the Digital Forensics Lab and/or Cyber Fusion Centre, or to offer to collaborate on the creation of these functions with other interested parties.

INTERPOL will ultimately decide whether to select one company to assist in the design, establishment, maintenance and partial-operation of the Digital Forensic Lab and/or Cyber Fusion Centre, or to select a consortium of private sector companies and technological institutions to do so.

Call for Interest Objectives

INTERPOL announces a Call for Interest (CfI) to companies specializing in information technologies, as well as technological institutions, to obtain an indication of their interest to assist in the design, establishment, maintenance and partial-operation[2] of the Digital Forensic Lab and/or Cyber Fusion Centre in the INTERPOL Digital Crime Centre in Singapore by providing technical equipment and tools, technical assistance and expert human resources at no cost to INTERPOL for at least 3 years.

[1] Human Resources would be expected to be assigned linked to a Resources Assignment Agreement (RAA) unless otherwise agreed between INTERPOL and an interested party. RAAs may be concluded to obtain temporary additional human resources from institutions such as universities, private companies, foundations, law enforcement agencies and other national administrations. RAAs shall be concluded for a minimum duration of 2 weeks and a maximum of 12 months. The Organization shall not be responsible for emoluments, health insurance, welfare scheme and pension payments.

[2] Partial operation would refer to instances where any human resources might be detached from a private company to work in either the Lab and/or Fusion Centre.
~~~~~~

More specifically, any party interested to provide the abovementioned assistance for the Digital Forensic Lab and/or Cyber Fusion Centre to INTERPOL can opt to respond to the following two options:

1) By submitting your company, consortium or institution's interest to assist in the design, establishment, maintenance and partial-operation of the Digital Forensic Lab and/or Cyber Fusion Centre (*to be specified within the proposal*) as the sole vendor for the complete product by including your proposed concept functionalities, technologies, expertise, etc. and time for completion for the establishment of unit.

2) By agreeing to participate in the design and establishment of the Digital Forensic Lab and/or Cyber Fusion Centre containing specialized equipment, including advanced technology required for the Malware/BotNet analysis or expertise from your company that could be incorporated in the Lab and/or Fusion Centre, founded with the assistance of one of the participating consortium companies.

Additional Conditions

a. Any interested company/institution or consortium thereof would be required to do all the design and development on its own and to absorb all costs related thereto.

b. Any interested company/institution or consortium thereof would be required to collaborate with the architects and interior design companies already contracted to design and build the INTERPOL Global Complex for Innovation. No modifications to structural design or layout would be permitted unless otherwise agreed with INTERPOL beforehand.

c. Any interested company/institution or consortium thereof would be required to provide installation and maintenance in Singapore, and provide an functioning product before the INTERPOL Global Complex for Innovation becomes operation in May 2014.

d. Following the acceptance of a party's proposal, INTERPOL can be consulted to give input along the way to review draft designs of the Lab and/or Fusion Centre.

e. Prior to entering into an agreement, any interested company/institution or consortium thereof would be required to have all key Officers and Board Member to be subject to national and INTERPOL background checks. INTERPOL reserves the right to apply other due diligence procedures prior to entering into a commercial agreement.