INTERPOL

GLOBAL COMPLEX FOR INNOVATION

国际刑警网络情报公私营合作模式

刘肇邦

国际刑警组织数字犯罪中心专家

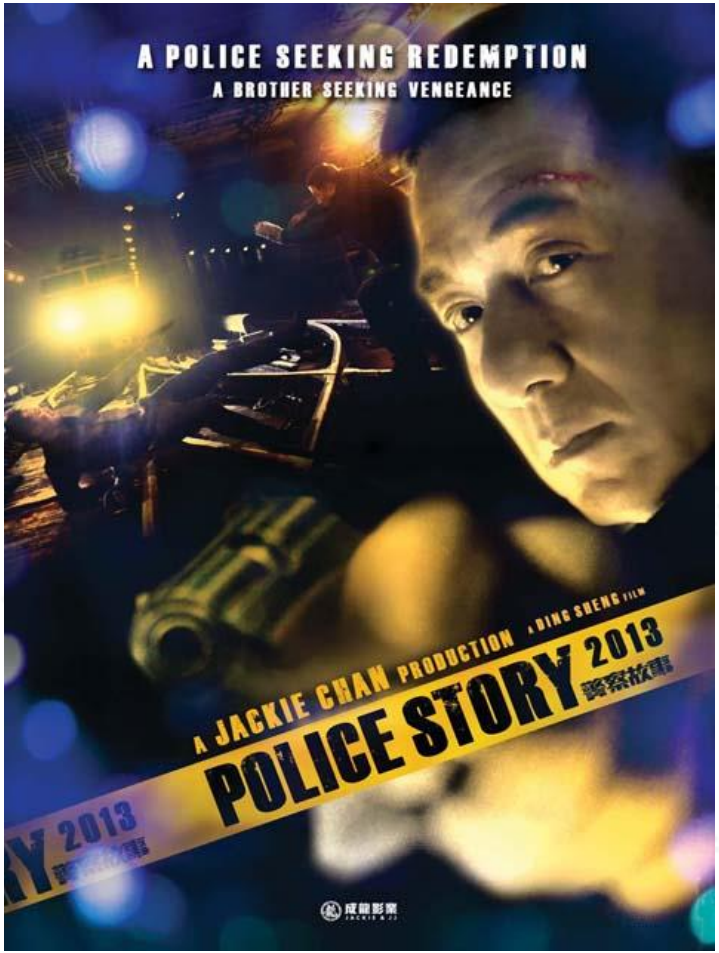
Louis LAU

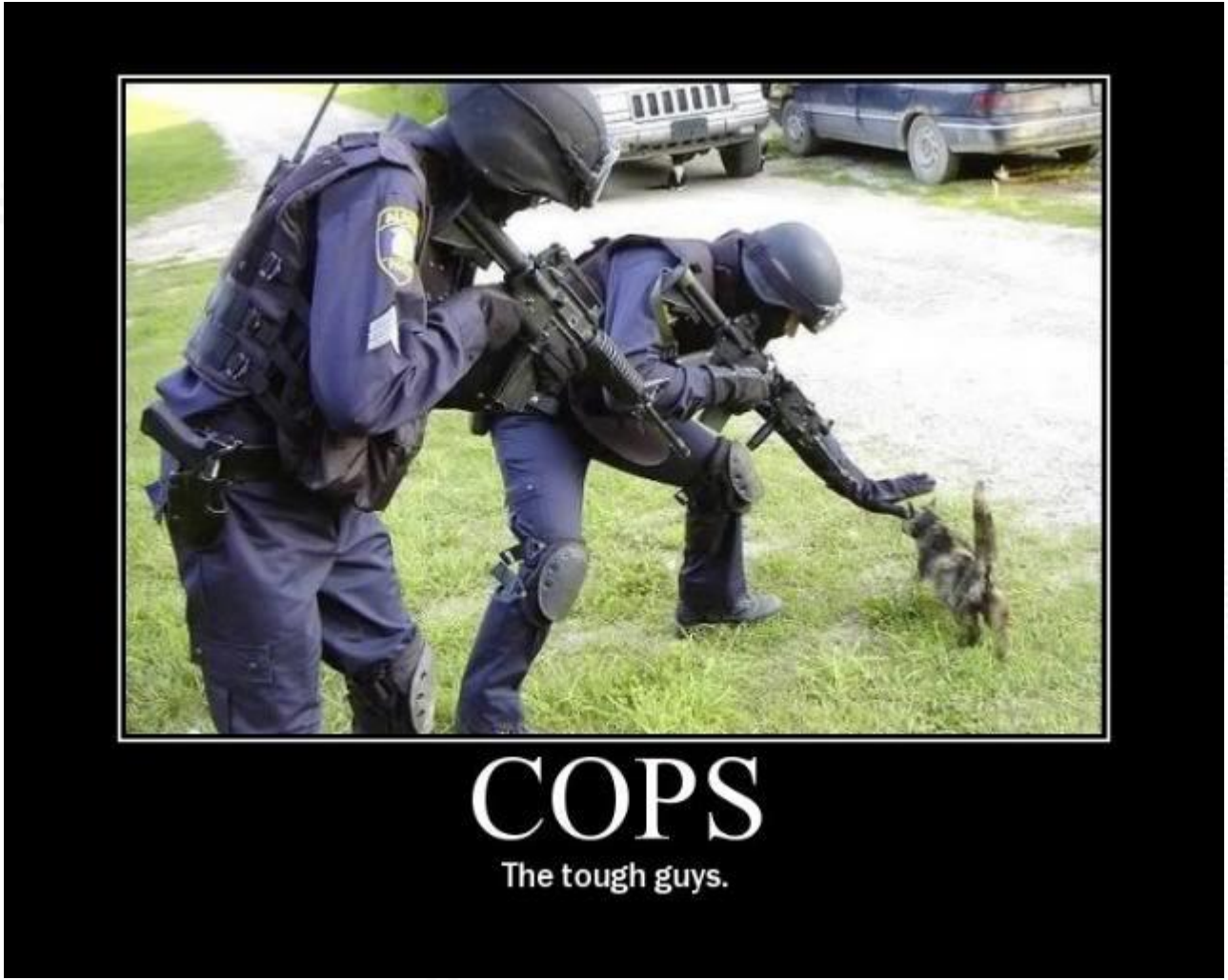
Digital Crime Officer

Cybercrime Directorate

INTERPOL Global Complex for Innovation

INTERPOL





国际刑警是...

A 联合国的一个分支

B 总部位于美国

C 一支跨国的警察队伍

D 总部位于法国

国际刑警是...

A 联合国的一个分支

B 总部位于美国

C 一支跨国的警察队伍

D 总部位于法国

01

IPSG LYON

02

IGCI SINGAPORE

03

3.1 RB SAN SALVADOR
3.2 RB BUENOS AIRES
3.3 RB ABIDJAN
3.4 RB YAOUNDE
3.5 RB HARARE
3.6 RB NAIROBI
3.7 LO BANGKOK

04

4.1 UN OFFICE
4.2 EU OFFICE

下面那一项有关国际刑警是正确的？

A 可拘捕罪犯

B 拥有自己的监狱

C 为全球警队
提供一个内部网络

D 是一个情报组织

下面那一项有关国际刑警是正确的？

A 可拘捕罪犯

B 拥有自己的监狱

C 为全球警队
提供一个内部网络

D 是一个情报组织

国际刑警的座右铭为：

A 建立一个
更安全的世界
连系全球警队

B 捍卫领土

C 立足未来

D 成为全球情报中心

国际刑警的座右铭为：

A 建立一个
更安全的世界
连系全球警队

B 捍卫领土

C 立足未来

D 成为全球情报中心

下面那一项不是国际刑警的法定语言？

A 英语

B 法语

C 阿拉伯语

D 西班牙语

E 德语

下面那一项不是国际刑警的法定语言？

A 英语

B 法语

C 阿拉伯语

D 西班牙语

E 德语

虽然国际刑警不会发出拘捕令，但会发出：

A 红色通报

B 网络活动报告 *(Cyber Activity Report) ("CAR")*

C 紫色通报

D 黄色通报

E 以上皆是

虽然国际刑警不会发出拘捕令，但会发出：

A 红色通报

B 网络活动报告 (Cyber Activity Report) (“CAR”)

C 紫色通报

D 黄色通报

E 以上皆是

拉登的红色通缉令是由以下那个国家要求发出的：

A 沙地阿拉伯

B 美国

C 利比亚

D 巴基斯坦

拉登的红色通缉令是由以下那个国家要求发出的：

A 沙地阿拉伯

B 美国

C 利比亚

D 巴基斯坦

以下那个是国际刑警的成员？

A 台湾

B 北韩

C 梵蒂冈

D 所罗门群岛

以下那个是国际刑警的成员？

A 台湾

B 北韩

C 梵蒂冈

D 所罗门群岛

INTERPOL

Secretary General

秘书处

Executive Dir.
Resource Management

Executive Dir.
Police Service

Executive Dir.
Strategy and Governance

Executive Dir.
Global Complex for Innovation

国际刑警全球创新科技中心

网络犯罪部门

Cybercrime

Innovation Centre

创新部门

Capacity Building and Training

培训部门

Governance


INTERPOL | 경찰청
ISCR 2016
4th INTERPOL Eurasian Working Group Meeting
on Cybercrime For Heads of Units
2016 국제 사이버범죄대응 심포지엄
ISCR 2016

INTERP

东盟『网络突破』行动时序

Timeline of ASEAN Cyber Surge Operation

第四届欧亚工作组会议

第四届欧亚工作组会议

- 会后总结：
  - 网络犯罪是无国界的
  - 网络犯罪的数量不断上升，对经济的影响亦日益增多
  - 国际合作是打击及预防网络犯罪的其中一个最重要的环节
- 会上建议：
  - 国际刑警继续协调跨国联合行动
  - 为东盟地区举办一个为期一周，打击网络罪犯及打击网络基建的行动

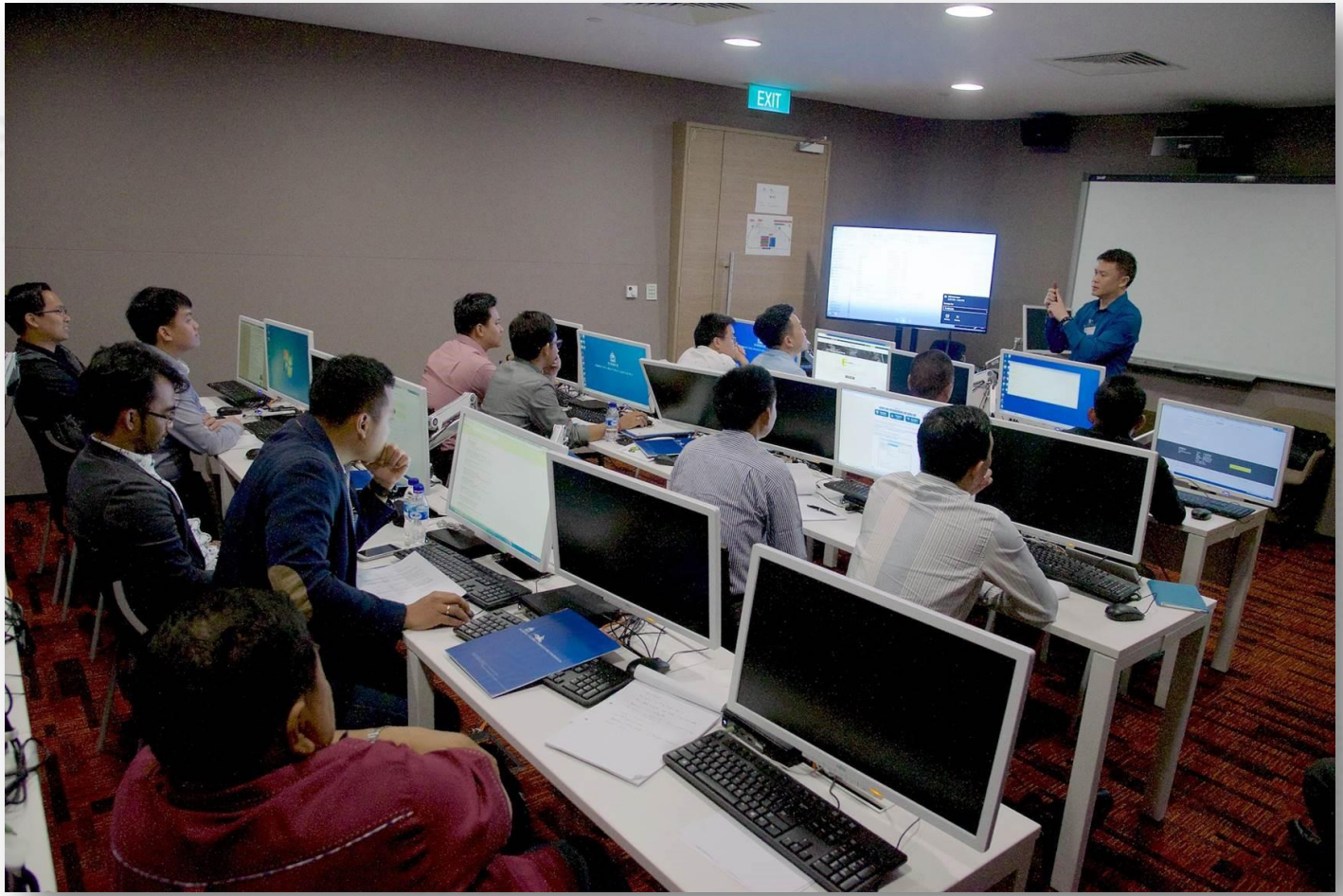
东盟『网络突破』行动 - 预备会议

预备会议

- 八国参与，包括：柬埔寨，印度尼西亚，马来西亚，缅甸，菲律宾，新加坡，泰国和越南
- 会上：
  - 谈及是次行动的背境及理念
  - 圆桌讨论 – 各国的情况
  - 简报：
    - 区内的恶意网站（Malicious Website）
    - 恶意软件追踪（Malware Tracing）
    - 『No more ransom』 运动

东盟『网络突破』行动 - 培训

INTERPOL



培训 (2017年1月9-13日)

- 15名参加者
- 来自八国东盟国家，包括柬埔寨，印度尼西亚，马来西亚，缅甸，菲律宾，新加坡，泰国和越南
- 培训项目包括:
  - IP地址基础概念
  - 网域名称系统(DNS)的滥用
  - 执法人员
    - 网上调查的能力
    - 追查在网上匿名人士的能力
    - 社交媒体的调查能力
    - 保存网上证据的能力
    - 实习

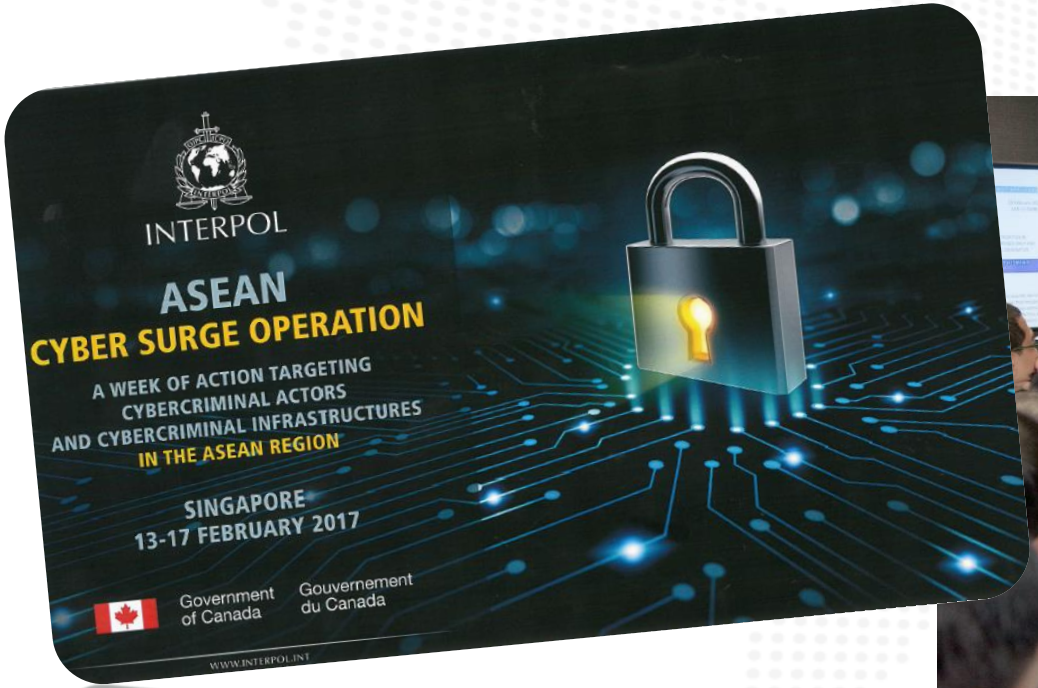
东盟『网络突破』行动 - 最后准备会议

INTERPOL

- **网络活动报告(CAR)的内容围绕:**
  - 网页窜改及其相关活动
  - 恶意网站及钓鱼网站
  - 网上交易区/讨论区及疑犯
  - C2 基建 及 相关的恶意软件家族(malware families)
  - 各国的网络罪犯所进行的地下买卖活动
- **『网络融合中心(CFC)』 与以下七间公司合作:**
  - Trend Micro, Kaspersky Lab, Cyber Defense Institute, Booz Allen Hamilton, Palo Alto Networks , BT.
- **东盟+3成员国亦有参与**

东盟『网络突破』行动 - 一周行动

东盟『网络突破』行动


INTERPOL
ASEAN
CYBER SURGE OPERATION
A WEEK OF ACTION TARGETING
CYBERCRIMINAL ACTORS
AND CYBERCRIMINAL INFRASTRUCTURES
IN THE ASEAN REGION
SINGAPORE
13-17 FEBRUARY 2017
Government of Canada
Gouvernement du Canada
WWW.INTERPOL.INT

东盟『网络突破』行动 - 总结

新闻发布
(2017年4月24日)

Search : Keyword English

INTERPOL

CONNECTING POLICE FOR A SAFER WORLD

WANTED PERSONS

MISSING PERSONS

HOME | ABOUT INTERPOL | NEWS AND MEDIA | MEMBER COUNTRIES | INTERPOL EXPERTISE | CRIME AREAS

Media room
News
Speeches
Events
Publications
Videos
Photos
Social media
Visits

All news

Share | Print

Photos : 2

24 April 2017

INTERPOL-led cybercrime operation across ASEAN unites public and private sectors

SINGAPORE – An INTERPOL-led operation targeting cybercrime across the ASEAN region has resulted in the identification of nearly 9,000 Command and Control (C2) servers and hundreds of compromised websites, including government portals.

The operation, run out of the INTERPOL Global Complex for Innovation (IGCI), brought together investigators from Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam to share information on specific cybercrime situations in each country. Additional cyber intelligence was also provided by China.

Experts from seven private sector companies - Trend Micro, Kaspersky Lab, Cyber Defense Institute, Booz Allen Hamilton, British Telecom, Fortinet and Palo Alto Networks - also took part in pre-operational meetings in order to develop actionable information packages.

Information provided by the private sector combined with cyber issues flagged by the participating countries enabled specialists from INTERPOL's Cyber Fusion Centre to produce 23 Cyber Activity Reports. The reports highlighted the various threats and types of criminal activity which had been identified and outlined the recommended action to be taken by the national authorities.

Analysis

Analysis identified nearly 270 websites infected with a malware code which exploited a vulnerability in the website design application. Among them were several government websites which may have contained personal data of their citizens.

A number of phishing website operators were also identified, including one with links to Nigeria, with further investigations into other suspects still ongoing. One criminal based in Indonesia selling phishing kits via the Darknet had posted YouTube videos showing customers how to use the illicit software.

The threats posed by the 8,800 C2 servers found to be active across eight countries included various malware families including those targeting financial institutions, spreading ransomware, launching Distributed Denial of Service (DDoS) attacks and distributing spam. Investigations into the C2 servers are ongoing.

IGCI Executive Director Noboru Nakatani said the operation was a perfect example of how the public and private sectors can work efficiently together in combating cybercrime.

"With direct access to the information, expertise and capabilities of the private sector and specialists from the Cyber Fusion Centre, participants were able to fully appreciate the scale and scope of cybercrime actors across the region and in their countries," said Mr Nakatani.

"Sharing intelligence was the basis of the success of this operation, and such cooperation is vital for long term effectiveness in managing cooperation networks for both future operations and day to day activity in combating cybercrime," added Mr Nakatani.

Chief Superintendent Francis Chan, Chairman of INTERPOL's Eurasian cybercrime working group and Head of the Hong Kong Police Force's cybercrime unit said the operation helped develop capacity and expertise of officers in the participating countries.

SEE ALSO

- Cybercrime
- INTERPOL Global Complex for Innovation
- Partners

行动结果

- 一共发出了23个网络活动报告(CAR)
- 识别了最少三个设立钓鱼网站的网络罪犯
- 向两个在暗网上进行不法交易的集团进行卧底渗透行动
- 就着发现的近九千个指令及控制服务器，进行一个有系统的清除行动

回应

- 提高针对网络犯罪的认知
- 是一个崭新的学习过程
- 对区内各国的法规有更深入的认识
- 由于网络犯罪很多时并不能找出受害人，所以各国应该更主动及积极的展开调查

建议

- 语言
- 数据源
- 获得情报的方法
- 调查建议

نشكركم جزيل الشكر على انتباهكم

Thank You-Merci-Gracias

多谢!

l.lau@interpol.int

INTERPOL