

PARTICIPAÇÃO NO "THE 8TH INTERPOL
 TRAIN-THE-TRAINER WORKSHOP ON IT CRIME
 INVESTIGATION FOR ASIA AND SOUTH PACIFIC"



Hoje em dia a internet já atingiu um grande nível de desenvolvimento, a sua aplicação é muito extensa, no âmbito do uso individual (troca de informações, compras *on-line*, comunicação entre amigos e tratamento de dados pessoais) e comercial (transmissão de informações, transacções financeiras e análise da situação de mercado), a utilização do computador e da internet é um ponto fundamental na vida quotidiana. Devido ao seu uso cada vez mais alargado, a internet está a ser utilizada também por criminosos como meio para pôr em prática os seus actos, o que está a dar vida a vários tipos de crimes informáticos, tais como invasão de sistemas informáticos, burla na internet, uso não apropriado de dados alheios, etc. Assim, a internet reveste-se de uma característica transfronteiriça, acrescentando o facto que o desenvolvimento dos computadores e da tecnologia na rede, muda de dia para dia, isto tudo ajuda os criminosos para esconderem a sua identidade

nas suas actuações, tornando a investigação muito mais difícil. Por isso, a investigação e a recolha de provas relacionadas com crimes informáticos devem acompanhar o desenvolvimento tecnológico, bem como estar a par da actualidade do crime informático, das respectivas técnicas de investigação e da recolha de provas, para um combate mais eficaz.

Neste sentido, a Polícia Judiciária nomeou Lam Chon Cheng, investigador criminal de 2ª classe da Secção de Investigação de Crimes Informáticos, e Luís Hoi, técnico de 2ª classe da Divisão de Informática, para se deslocarem a Suva, Fiji, nos dias compreendidos entre 27 de Setembro e 5 de Outubro de 2009, e participarem na acção de formação "*The 8th Interpol Train-the-Trainer Workshop on IT Crime Investigation for Asia and South Pacific*". Este curso contou com a participação de 20 pessoas oriundas da região Ásia-Pacífico, os formadores são especialistas vindos de diferentes campos da informática, a saber, representantes da *Information, Communication and Technology Unit of Fiji Police Force*, da *Technology Crime Division of Commercial Crime Bureau of Hong Kong Police*, e do *Anti Cyber Terrorism Center of Korean National Police Agency*.

Os temas principais do curso foram: (1)

Perseguição dos autores de crimes perpetrados na internet, investigação sobre fontes de informações de websites e perseguição de serviços anónimos *on-line*. Após vários dias passados a simular situações reais, os participantes aprenderam como é que os criminosos adquirem ilegalmente dados de identificação de outrem (de cartões de crédito e contas bancárias), através de e-mail e websites falsificados, ou *social engineering*, utilizando depois dados ilegalmente obtidos para burlas directas ou indirectas. (2) Funcionamento e análise de e-mail. O E-mail é, hoje em dia, um dos meios de comunicação mais usados na rede, é também o meio mais utilizado na rede para burlas. Para conseguir saber o local de cometimento, pode-se analisar o *e-mail header*, examinar as vias de envio do e-mail de burla e procurar o endereço IP do emissor, utilizando depois diversos *Network Monitoring Tools* para localizar com exactidão o servidor em causa até chegar aos respectivos registos dos clientes na rede. (3) Análise de *Malware*, vírus e *Trojan Horse*. A rede está repleta de *Malware*, vírus e *Trojan Horses*. Ao navegar na internet, descarregar ficheiros ou usar um *Instant Messenger*, pode permitir-se a entrada no nosso computador, sem saber, de um *Malware* ou vírus, que conseguem evitar a detecção do antivírus, uma vez em acção, transmitem então dados pessoais, através da internet, para servidores controlados por criminosos, que os usam para burlar as pessoas. Neste *workshop* foi dada uma explicação sumária sobre diversos *Network Monitoring Tools* que podem efectuar um registo do movimento de todos os softwares constantes no computador, o processo de operações, bem como dados transmitidos entre computadores e internet. Depois da análise, pode-se perseguir a fonte dos *Malwares*, vírus e *Trojan Horses*. (4) Análise de websites falsificados, invasão de websites e *weblogs*. Estudaram-se as maneiras que os *hackers* usam na rede para copiar websites e falsificá-los, tornando-os semelhantes aos verdadeiros, nomeadamente websites de

bancos e de lojas *on-line*, bem como de *Social Networks*, no sentido de burlar os utentes, furtar depois os seus dados pessoais e desta maneira, ganhar lucros ilícitos. Foi também explicado como se analisa um *Sistem Log* e como se utilizam os *Network Monitoring Tools* para saber data e hora em que foi efectuada a entrada ilícita de um determinado website, bem como descobrir o endereço IP do website que a efectuou. (5) Como recolher provas relacionadas com o crime informático no local da ocorrência, recolha de provas e o uso de instrumentos tecnológicos para a recolha de provas. No decurso da investigação e recolha de provas relativas ao crime informático, para evitar a possível perda de provas electrónicas após desligado o computador, é necessário, às vezes, fazer a recolha das provas *in loco* num determinado computador ainda em funcionamento. Por isso, a utilização de instrumentos que garante a autenticidade e a eficácia ajuda a registar por completo todo o processo de cometimento do crime informático.

Através das explicações teóricas dadas pelos formadores especializados, combinadas com a prática e os debates em grupo efectuados neste *workshop*, o nosso pessoal aprendeu as técnicas de investigação mais actuais no âmbito do crime informático, bem como os procedimentos para o tratamento das provas electrónicas, foi ainda possível ter um conhecimento aprofundado sobre as características, técnicas de investigação e de recolha de provas seguras e efectivas em diversos tipos de crimes informáticos, atingindo o objectivo de melhorar a técnica e aumentar a eficiência do trabalho. Ao mesmo tempo, participantes e formadores compartilharam com entusiasmo experiências de trabalho e discutiram em conjunto soluções para ultrapassar as dificuldades encontradas no trabalho, isto contribuiu para melhorar as nossas capacidades no âmbito da investigação e da recolha de provas no que concerne ao crime informático.