

10ª CONFERÊNCIA - ÁSIA E OCEÂNIA - SOBRE TÉCNICAS DE INVESTIGAÇÃO DO CRIME INFORMÁTICO

Para conhecer as últimas tendências da evolução do crime informático na zona Ásia-Pacífico, e para actualização das técnicas de combate a este crime, especialmente no que concerne à investigação e recolha de provas, a PJ enviou Che Ka Kin, técnico superior, e Leong Kin Wai, investigador criminal, para participarem na 10ª Conferência - Ásia e Oceânia - sobre Técnicas de Investigação do Crime Informático que teve lugar em Tóquio entre 8 e 12 de Setembro de 2009. Nesta conferência, realizada pela *National Police Agency* do Japão, contou-se com a participação de 29 representantes, da Interpol, de Fiji, Índia, Indonésia, Coreia do Sul, Malásia, Nova Zelândia, Filipinas, Singapura, Tailândia, Vietname, China com as R.A.E. de Hong Kong e Macau etc., num total de 15 países.

A conferência foi dividida em duas partes, “*Workshop* sobre as Técnicas de Investigação e Análise do Crime Informático” e “Conferência sobre as Técnicas de Investigação do Crime Informático”. No primeiro dia, realizou-se o “*Workshop* sobre Técnicas de Investigação e Análise do Crime Informático” no qual foi criado um ambiente informático para simular casos reais e explicar como os *hackers* invadem um *website* usando, por exemplo, *SQL injection* para atacarem a base de dados (sistema destinado à preservação de dados pessoais de clientes ou sistema de bases de dados concernentes a transacção de mercadorias na rede), ou usurparem e modificarem, com maus propósitos,

dados informáticos sem autorização, na sessão também se falou das medidas contra a invasão e técnicas de investigação e de análise. Para além disso, através deste *workshop*, foi explicado como o *software* “*Malware analysis*” prejudica os dados dos clientes e a segurança patrimonial sendo um dos graves problemas do crime informático actual, os organizadores falaram das características deste *software*, analisaram o seu funcionamento e os vestígios da invasão, apresentaram as técnicas para examinar *malwares* adoptando instrumentos como “*SysAnalyzer, FileMon, FakeDNS, WireShark*” e técnicas de recolha de provas. Do ponto de vista da investigação e recolha de provas, no *workshop* também se discutiram casos reais referentes ao crime informático, como a invasão de um servidor, ataque de *Botnet* etc.

Nos seguintes dois dias realizou-se a segunda parte, ou seja, a “Conferência sobre as Técnicas de Investigação do Crime Informático” que focou o combate a este tipo de crime adoptando medidas eficientes, bem como o reforço das relações cooperativas entre os estados-membros por meio do CTINS (*Cybercrime Technology Information Network System*). Nesta sessão, vários representantes apresentaram a actualidade desta área e casos reais no seu próprio país, por exemplo, crime financeiro utilizando a rede, divulgação de mensagens que prejudicam a segurança do público através da entrada ilegal na rede sem fio, divulgação, de forma criminosa, de

softwares específicos que usurpar informações confidenciais, apostas ilegais na rede etc. Durante a conferência, os participantes partilharam experiências de investigação e estudos sobre o combate ao crime informático discutindo vários temas inclusive a construção de um ambiente para gerir as provas electrónicas e na larga utilização deste tipo de provas na investigação, falou-se das técnicas de investigação do *Instant Messenger*, funcionamento de *softwares* comuns de transmissão P2P (*Peer-to-Peer*) como *BitTorrent*, *eMule* e *eDonkey*), técnicas de recolha de provas em telemóveis etc .

A *National Police Agency* do Japão fez um balanço da aplicação e optimização do sistema *CTINS (Cybercrime Technology Information Network System)*, como plataforma destinada aos estados-membros da Ásia e da Oceânia na troca de informações relacionadas com o combate ao crime informático, na recolha de prova, serão implementadas novas funções como:

1. Base de gestão de documentos: partilha de documentos de referência sobre a investigação destes crimes, acções de formação, análise informática forense etc., com vista a adquirir experiências avançadas de investigação e peritagem actuais, informações sobre formação e

actualização sobre o desenvolvimento tecnológico em todo o mundo;

2. Forum de discussão: irão criar-se foruns sobre vários temas, tendências do crime informático e medidas preventivas, informática forense, peritagem de telemóveis, cursos de formação, etc. Isto favorecerá a aquisição de experiência tanto para os investigadores como para os peritos, possibilitando a colaboração no combate a este tipo de crime.

3. *Software* para recolha de provas e análise: A *National Police Agency* do Japão pôs a disposição um *software* para a recolha de provas e análise criado de propósito por eles, para que os vários países membros possam estudá-lo e trocar opiniões.

4. Correio electrónico encriptado: os países membros podem comunicar entre eles através deste meio bem como receber mensagens divulgadas regularmente pela *National Police Agency* do Japão.

Este sistema apresenta características de encriptação e autenticação electrónica que garantem aos membros o contacto num ambiente electrónico seguro que promove, com eficácia, a colaboração.

