Crime organizado no Ciberespaço: rastreando a sua estrutura

Marcos Carazai

A estrutura dessas organizações criminosas é diferente das organizações tradicionais de crime organizado. As atividades criminosas geralmente são realizadas em redes criminosas virtuais multifacetadas, porém, quando necessário, são planejadas em reuniões *on-line*. Essas redes são estruturadas de forma "autônoma", uma vez que os membros raramente se encontram pessoalmente. Esta estrutura sofisticada, juntamente com o acesso às operações básicas concedidas apenas a associados confiáveis, impede que sejam detectados por infiltrados virtuais ligados às autoridades policiais.

Ferramentas e modelos das atividades criminosas

O crime organizado empresta e copia modelos de negócios do setor da economia legítima. Os cibercriminosos empregam modelos similares ao B2B (business-to-business) para suas operações, como os altamente sofisticados modelos C2C (criminal-to-criminal), que utilizam ferramentas muito eficazes disponíveis através de redes digitais. As vulnerabilidades e softwares dos sistemas informáticos são explorados para criar *crimeware*, como vírus, *trojans, keyloggers*. Essas ferramentas *crimeware* oferecem aos grupos criminosos a flexibilidade de controlar, roubar e comercializar dados. O desenvolvimento de *botnets*, redes de computadores comprometidos, que executam programas sob controle externo, transformaram alguns tipos de cibercrimes, como o phishing, no ecossistema subterrâneo mundial administrado pelo crime organizado. O ganho financeiro estimado desses grupos criminosos varia entre dezenas de milhares

e dezenas de milhões de dólares. O comércio de *botnets* também se tornou uma atividade de alta receita que também está ligada ao crime organizado. Os custos dos *botnets* são relativamente baixos em comparação com o ganho financeiro dos delinquentes e com os danos causados a consumidores e empresas individuais, bem como à saúde financeira, à reputação e à confiança nas transações *on-line* como um todo. O *Crimeware* também é usado para implantar modelos de negócios *Crime-as-a-Service* que representem o sistema de negociação e entrega de ferramentas de *crimeware*. Os modelos de fornecimento de dados também são usados para compartilhar as ferramentas dos crimes cibernéticos. Por exemplo, ao criar sistemas de "clientes", onde os instrumentos estão disponíveis sob demanda, o integrante da organização faz o *login* no servidor da mesma e escolhe as ferramentas adequadas para fraude, *phishing* e subtração de dados. Quando os dados dos usuários são "*roubados*", criminosos usam servidores de *Crimeware, com base nesses dados,* para cometer ataques organizados. Os servidores *Crimeware* permitem controlar computadores comprometidos e gerenciar todos os dados subtraídos.