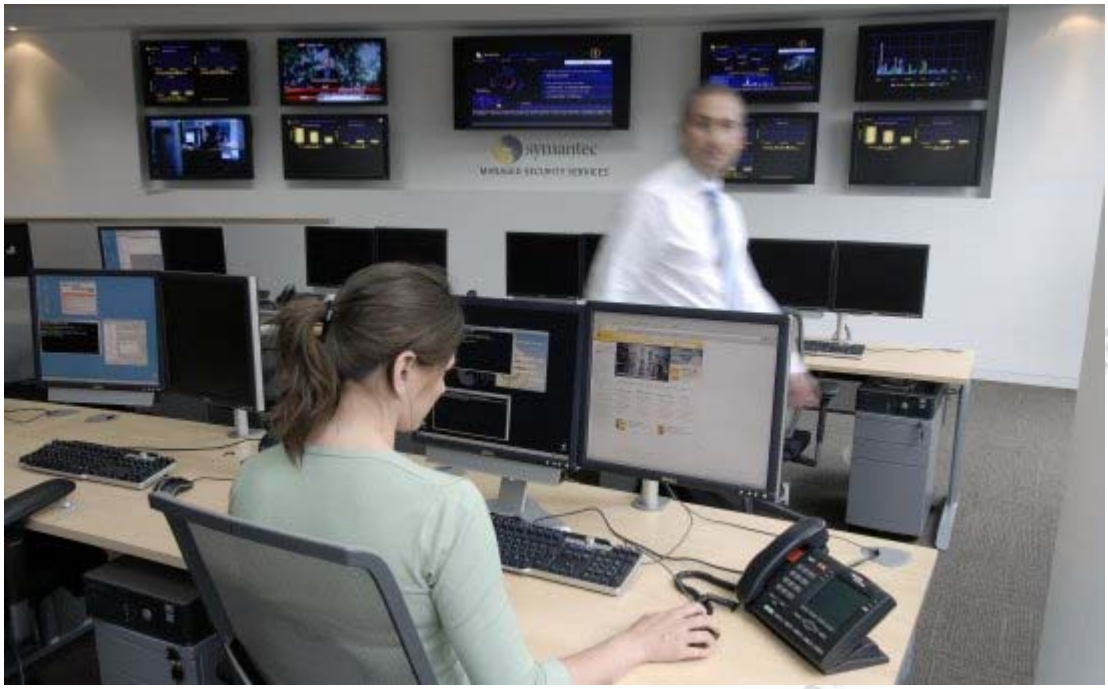
The evolution of CyberCrime Inc.
Doreen Carvajal



Technicians at work in a Symantec computer operations center. (Symantec)

There is no storefront or corporate headquarters for Cybercrime Inc., but savvy salesmen in a murky, borderless economy are moving merchandise by shilling credit card numbers - "two for the price one."

"Sell fresh CC," promised one salesman who offered teaser credit card numbers for samples in New Jersey and Canada. "Visa, MasterCard, Amex. Good Prices. Many countries!!!!!"

Electronic crime is maturing, according to security experts, and with its evolution, clever criminals are adopting conventional approaches that reflect cold business sense - from supermarket-style pricing to outsourcing to specialists acting as portfolio managers, coders, launchers, miners, washers and minders of infected "zombie" computers.

"It's a remarkable development of a whole alternative business environment that's occurred over the last couple years," said Richard Archdeacon, a senior director of global services for Symantec, an Internet security company with 11 research centers around the world tracking crime trends. "What's been so astonishing is the speed with which it's developed and the effect with which the market has grown and matured."

In the United States alone, victims of reported Internet fraud lost $239 million in 2007, with average losses running about $2,530 per complaint recorded by a special Web-based hot line operated by the FBI and the National White Collar Crime Center, a nonprofit corporation focusing on electronic crime.

The most common frauds were fake e-mail messages and phony Web pages and the crimes were organized from the United States, England, Nigeria, Canada, Romania and Italy, according to an FBI report issued last week.

Yet despite the increasing sophistication and elusiveness of e-criminals, judges remain reluctant to order much jail time for computer crime, according to some national law enforcement officials and such major companies as Microsoft.

A case in point is Owen Thor Walker, a self-taught computer wizard from New Zealand who, at 18 years old, pleaded guilty last week to criminal charges arising from his development of a

vast international network of individual computers that he had hijacked and infected with hidden software or "malware" and remotely controlled.

In the parlance of the trade, he was a "bot herder" who offered his "robot network" for hire to a company in the Netherlands to covertly install their adware. Walker's borderless network first surfaced in an FBI investigation of a computer attack in 2006 that caused the crash of a computer server at the University of Pennsylvania in the United States. The FBI singled out a Pennsylvania student in the attack who ultimately led investigators to Walker, nicknamed Akill.

Walker's sentencing is scheduled for late May, but the judge on the case indicated that he would consider community detention and work release or some home detention for punishment of the teenager, who suffers from Asperger Syndrome, a mild form of autism marked by poor social skills and compulsive behavior.

"Most of the time it's very difficult for a judge to understand what's going on and what the risks are," said Eric Loermans, chief inspector of a Dutch high-tech crime unit, noting though that private companies that are not satisfied can also take civil action against offenders.

Loermans was part of the Council of Europe's cybercrime forum in Strasbourg last week to develop guidelines for closer international cooperation between law enforcement and Internet service providers. More than 200 people representing government agencies and private companies from the Europe, the United States, Africa and South America participated in the conference.

Many came from countries where the police are regrouping: like India, where officers in New Delhi are being sent for cybercrime training in e-mail tracking and digital fraud; or the Netherlands, where the government is spending €14 million, or $22 million, over the next four years on its fight against cybercrime.

The Dutch plainclothes high-tech unit now numbers about 25 people, but the police are also in the process of developing training programs for everyone on the staff down to the officer on the beat, according to Loermans.

"Years ago, we saw cybercrime as a speciality," he said. "Now we have added cybercrime in every form of police training, so we are raising the level of the entire Dutch police force. There's no crime anymore where there are no digital components built in."

The aim is to keep up with an age-old game of cat-and-mouse that is accelerating, with newly emerging tools like the "fast flux" that allows cybercriminals to hide the national location of spamming and phishing Web sites, which surface for minutes on a bot computer in one country before moving within minutes to another infected bot in another country. Phishing is a method of fraudulently acquiring sensitive information, like passwords and credit card numbers, using digital communication.

The advantage of fast flux, according to experts, is that attackers can register a child-pornography site or a fake bank that is not tied to a single domain that can be tracked and shut down. The flux techniques were used in phishing frauds this year that targeted bank customers in England where criminals created fake bank sites mimicking Barclays and Halifax banks and requested personal information.

David Roberts, chief executive of the Corporate IT Forum, which represents 150 companies in Britain, said his group was pressing for a single confidential channel where corporate security chiefs could report cybercrimes. The Conservative Party in Britain has lately seized on the issue, promising a dedicated "e-crime" police unit and the creation of a new government position, a "cybercrime minister."

As it is now, Roberts said that major companies rarely reported crimes because they wanted to protect their own reputation. And he said they might deal with it discreetly in other ways, perhaps by simply paying nuisance attackers to go away.

"Their only recourse at the moment is to quite literally go to their nearest police station and report the crime to the local police constable," Roberts said, adding that the local police are "very good on physical criminals and household thefts and burglaries, but electronic crime is not part of their curriculum."

The fast-flux technique, Roberts said, was a further illustration of how online crime has evolved. "They are professional, large, well organized and they are best called companies."

Microsoft, which has its own teams of private investigators to monitor and combat cyberthreats to the company, is now taking a more "holistic" approach to confront electronic fraud by financing conferences and training programs.

"It's just not sufficient to bring cases to police," said Jean-Christophe Le Toquin, an Internet safety director for Microsoft in Europe, the Middle East and Africa. "It's not sufficient to have conferences on cybercrime. What you have to do is both of these things and then offer training to judges on cybercrime so that the parliament, the police, the judges are all trained at the same time."

Microsoft is also turning its lawyers toward another flaw in e-commerce called typosquatting by challenging individuals for trademark infringement who register domain names with misspelled versions of the Microsoft name to make money from unsuspecting computer users through pay-per-click advertisements.

Last year, according to the company, it recovered more than 2,000 names.

Disponível em: <http://www.iht.com>. Acesso em 7/4/2008.