# Networking: Virus writing for profit

September 26 2005

Unscrupulous e-mail marketers are collaborating with criminal virus writers to combine selling questionable goods and services online with attempting to steal information from consumers, experts told United Press International's Networking.

"Spammers are now paying virus writers to make new viruses that create zombie networks that are used to send fraudulent or phishing e-mails," said John Dickinson, author of the book, "The New Anti-Virus Formula: How to Use Multilayered Security to Defeat Viruses."

Dickinson added, "The so-called phishing variant induces people to turn over the keys to their financial accounts, leading to outright theft."

Kaspersky Lab, an Internet-security company in Moscow, reports increasing evidence of criminal activity in this field since December 2004. Over the past year, company researchers have found, the virus-writing community has moved from pranksters to pros, with the result that between 70 percent and 90 percent of all malware detected by Kaspersky Lab has been written for criminal purposes, instead of the previous aim of gaining the virus writer international notoriety.

Shane Coursen, Kaspersky Lab's senior technical consultant in the United States who recently published a scholarly paper called "The Changing Threat," said virus writing is becoming a for-profit endeavor, with goals as varied as personal-identity theft to corporate espionage.

"The threat in its mildest forms -- which too often defy successful

criminal prosecution -- results in disruption of day-to-day business, taking a significant toll on the profitability of companies of all sizes," Coursen said.

Other experts said collaborations between virus writers and spammers constitute a natural, symbiotic partnership.

"Anyone can send spam or a phishing e-mail," said Patrick Peterson, chief technology officer at IronPort, an IT security technology developer in San Bruno, Calif. "There are two magic ingredients to economic success on a large scale. The first is in controlling a large enough network of open proxies and compromised hosts to blast e-mail without having your footsteps traced. This is accomplished with viruses."

Next, Peterson continued, the criminals need to be able to transform stolen credit-card numbers and online bank-account numbers into cash.

"This is uniquely aligned with organized crime," he said. "Organized criminals have aggressively inserted themselves into the e-mail fraud ecosystem and play the primary role in networks like carderplanet.com and shadowcrew, which steal millions of credit-card numbers every year."

One of the fastest-growing markets for these criminal collaborators is overseas, experts said. For example, South American banks are considered a prime target for online fraud criminals. On a daily basis, according to MessageLabs, an IT-security company in New York City, approximately 20 Web sites are discovered that harbor malware aimed at compromising predominantly South American banks.

Authorities recently arrested 15 suspects from Spain, Argentina, Italy and Romania who were targeting customers in South America with illegal spam-virus combos.

According to Alex Shipp, senior anti-virus technologist at MessageLabs, the banking system in South American countries is generating a lot of interest in Internet banking, even more so than in the United States or Europe.

"This makes online banks a prime target for the high-tech gangs operating in the region who can get rich quick by selectively targeting local economic interests," Shipp said.

One tactic used by the spammers and virus writers is sending virtual postcards. In Brazil there is a massive craze for virtual-postcard sites, which allow people to send e-cards to loved ones and friends.

Shipp said, however, that these sites also provide an easy social-engineering opportunity for criminals wanting to steal users' confidential details.

"By tricking victims into downloading a Trojan instead of an electronic postcard, they can then start to monitor internet traffic with the goal of stealing usernames and passwords," he said.