Forbes.com

Security

The Top Countries For Cybercrime

Andy Greenberg, 07.16.07, 12:01 AM ET

Cybercrime, like every digital industry, is outsourcing. Though the U.S. still produces more malware, spam and viruses than any country in the world, illicit IT jobs are increasingly scattered across an anarchic and international Internet, where labor is cheap, legitimate IT jobs are scarce and scammers are insulated from the laws that protect their victims by thousands of miles. As Thomas Friedman might say, the criminal underworld is flat.

According to a Symantec report at the end of 2006, Beijing is now home to the world's largest collection of malware-infected computers, nearly 5% of the world's total. Research by the security company Sophos in April showed that China has overtaken the U.S. in hosting Web pages that secretly install malicious programs on computers to steal private information or send spam e-mails. And another report from Sophos earlier that month showed that Europe produces more spam than any other continent; one Polish Internet service provider alone produces fully 5% of the world's spam.

Cybercrime this geographically diverse isn't just hard to stop; it's hard to track. Common tactics like phishing and spam are usually achieved with "botnets," herds of PCs hijacked with malware unbeknownst to their owners. Botnet attacks can usually be traced only to the zombie computers, not to their original source. That means the majority of studies mapping botnet attacks point to every place in the world that has vulnerable PCs, with no real sense of where the attacks begin.

In Pictures: The Cybercriminals' Map Of The World

Researchers at Sophos Labs say they have a solution: They can roughly identify the host country of malicious software by tracing the default language of the computer on which it was programmed. According to their analysis of the default language linked with about 19,000 samples at the end of last year, Americans and other non-British English speakers still produce the most malware, more than a third of the world's total. Close behind is China, producing 30%, followed by Brazil, with 14.2%. Russia places fourth with 4.1% of the world's malware.

Bill Pennington of White Hat Security attributes these developing countries' bad behavior to an overabundance of technologically trained young people with low-paying jobs. "If you're in Russia or China and you have a computer science degree," he says, "You can either go work for nothing or you can make money using your skills for nefarious purposes."

Cybercrime isn't merely spreading to certain foreign countries, it's becoming cosmopolitan, says James Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies. As crime syndicates in Europe and Asia move into online scams, Lewis says that a single cybercrime operation can now be distributed among many different groups in several countries. One may create a "botnet" while another rents those computers to send credit scam e-mails and a third party transfers funds using the fraudulently obtained banking information. Sometimes each operation is on a different continent.

"The big problem here is political. It's sovereignty," Lewis says. "The FBI cannot go enforce American law without the consent of the country where cybercrime is being carried out. So even if U.S. laws were perfect, it wouldn't be enough to protect you." He describes a "Bonnie and Clyde" situation, where police stop at the edge of their jurisdiction rather than pursue criminals to their hideouts.

The growth areas of the malware industry aren't easily predicted. India, for instance, is one of the world's most

technologically booming developing countries, but ranks surprisingly low on Sophos' list. The U.K. and India together contribute only 1.3% of the world's malware--both use British English as a default language, so their samples couldn't be separated--and Sophos researchers say the majority of that criminal activity comes from the U.K. Eugene Kaspersky, Russian security guru and head of Kaspersky Labs, can only explain India's lack of cybercrime as a "cultural difference."

Nandkumar Saravade, director of cyber security for India's National Association of Software and Service Companies, says that India has so far avoided a cybercrime epidemic thanks to the success of its legitimate IT industry. "Today, it is a fact that any person in India with marketable computer skills has a few job offers in hand," he says.

But Saravade and Kaspersky both warn that security professionals should expect the subcontinent's malware contribution to grow in coming years. When it does, India likely won't be ready to contain the problem: The country's last major cybercrime law was created in 2000, long before botnets became an issue.

India isn't alone in being unprepared: Kaspersky says that the growing industry of malware professionals around the world hasn't been fully recognized by international legal bodies or the software industry, which continues to build vulnerable programs.

"We in the security industry need to attract the attention of government authorities, educate users and encourage changes in basic operating systems," he says. "Alone, we don't have a chance."

In Pictures: The Cybercriminals' Map Of The World