There’s been good news recently in the constant war on cybercrime. One of the services I subscribe to for computer crime news is run by Joe Mezzanini. His free Cybercrime Alerts service (subscription information at http://techPolice.com) provides several valuable articles a day on computer crime and forensics drawn from a variety of sources. In this newsletter and the next one, I relied entirely on Mezzanini’s service and have written abstracts that include key points made in the original articles. I’ve also added personal comments about some of the cases. Thanks, Joe: keep up the good work.

* * *

In May 2002, New York Attorney General Eliot Spitzer charged mega-spammer MonsterHut and its executives with fraud for claiming that its e-mail distribution lists consisted entirely of opt-in recipients. The spammers sent more than 500 million unsolicited commercial e-mail messages over the course of a year. [MK comment: Let’s hope that, if the accused are guilty, they are sentenced to read and delete 500 million unwanted commercial messages with misleading subject lines, bogus content advertising improbable enlargement of various body parts, and forged origination addresses – one by one. At 5 deletions per second 5 days a week for eight hours a day with two weeks off a year, that would keep them busy for, let’s see (tap, tap), 11 years <evil grin>.

* * *

Also in May, three employees of NEC Toshiba Space System Co., an aerospace firm in Japan, were arrested for hacking into National Space Development Agency (NASDA), the national space agency in that country in a quest for competitive intelligence about a rival firm, Mitsubishi Electric Corp. The illegal penetration allegedly took place in December 2001 and involved designs for a satellite antenna. Apparently the accused guessed a password; discovery followed discovery of an e-mail message supposedly from one of the perpetrators boasting about the hack; the message was sent to 80 recipients. NEC and Toshiba were both prevented from bidding on NASDA projects for one month. The accused will stand trial under Japan’s computer crime laws.

* * *

In June, agents of the U.S. Secret Service disclosed that several universities in AZ, CA, FL and TX may have been infiltrated by criminals who installed keystroke loggers to steal userIDs and passwords. The illicit software was apparently installed directly on individual computers in computer labs used by students but potentially open to interlopers. [At Norwich University, CIO Phil Susmann has instituted an excellent policy of disallowing software installations of any kind on University lab computers; in addition, each workstation is automatically reconfigured from a standard mirror file every night to reduce the number of system crashes expected for Windows systems that actually have users who run programs.]
Operation Candyman continued to rack up successes in finding child pornographers who use the Internet to satisfy their bizarre proclivities. In July, federal prosecutors in Manhattan and Brooklyn indicted ten people, including a “West Point Army sergeant, two former city police officers and a retired Yonkers firefighter.” [MK comment: I include this last detail because it is becoming clear that child pornographers include people from every walk of life. Remember, readers: in the USA and in most other countries, it is illegal to make, transmit or store child pornography (which is defined as depiction of children engaged in sexual activities). Report all occurrences of child pornography to the FBI (URL: ______________). If you find child pornography on your computer at work, report it to the security group; if you accidentally stumble on a child pornography site on the Web, report the incident to your supervisor in writing so you don’t get accused later of having deliberately downloaded the images that could be found on your hard disk during investigations.]

** For more information
MonsterHut
http://www.oag.state.ny.us/press/2002/may/may28a_02.html
NASDA
Child porn ring

**

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.