As I mentioned in the first of these two articles, Joe Mezzanini’s 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. This newsletter is the second to abstract and comment on articles distributed by Mezzanini. I recommend that anyone interested in keeping up with investigations and prosecutions of computer crime subscribe to his service. You can often find interesting nuggets that are perfect for your security-awareness materials and courses. Nothing perks up a mandatory security-policy class like some juicy recent crime cases.

* * *

On August 1st, the New York State Grand Jury delivered indictments against four people in a crackdown on a major identity-theft gang. According to the official press release from the Office of the Attorney General of NY, the accused are alleged to have used their access privileges as employees to steal personal details such as Social Security Numbers, credit-card numbers and bank account details from “New York State Insurance Fund, the Social Security Administration, Empire State College, WNYC radio, Hollywood Video, Worldcom Wireless and American Express.” The gang impersonated the victims to order merchandise (including “hundreds of computers and more than a thousand cellular telephones”) by phone; the loot was then sold on the black market by a large number of “fences.” A member of this conspiracy who had worked at the NY State Insurance Fund was convicted of grand larceny in July 2001 and is currently in jail for at least two and up to nine more years. [MK comment: always check your credit-card statement carefully as soon as you receive it. Immediately report unknown charges to the credit-card company and check with your bank to verify the status of your bank accounts.]

* * *

In mid-December 2001, four children from northern Israel were arrested for allegedly writing and distributing the Goner worm (aka “Pentagone” and “Gone”). In August, a group including four senior high school students (grades 10 and 11) and an eighth-grader were charged with violations of Israeli computer-crime laws. One of these script-kiddies allegedly wrote the worm in Visual Basic; the others are accused of posting the “screen saver” to various Internet sites. The worm spread rapidly by commandeering MS Outlok e-mail address books and ICQ instant messaging; it caused system crashes at NASA and other organizations. The five children were charged in August. [MK comment: yes, parents, your very own little darlings may be hacking NASA and writing the next misery-causing worm. How will you know unless you pay attention to what they are actually doing with that nifty computer you put in their bedroom last year?]

* * *

In Italy, 14 people were arrested in August on suspicion of being the criminal hackers from the “Mentor” and “Reservoir Dogs” gangs who are thought to have carried out thousands of illegal penetrations including data thefts from US government and military sites. Mathew Broersma,
writing for CNET News.com, stated that the suspects “included four minors, the security manager of a large Italian Internet service provider, a network security manager for a computer consulting company, and several information technology consultants.” The list of criminal activities in which the suspects allegedly participated includes the following:

- using stolen credit-card numbers;
- cracking the satellite TV encryption codes;
- making and selling illegal copies of DVDs;
- keeping the content of the DVDs on university servers they had penetrated;
- giving themselves unauthorized access on their own clients’ systems;
- installing back doors on their clients’ systems.

[MK comment: who will guard the guards? Use personnel security management techniques to spot unusual behavior before your systems are corrupted by dishonest employees or contractors. Verify the bona fides of “security experts” who offer their services to “strengthen” your security. Don’t hire criminal hackers as security staff.]

***

For more information:
ID theft http://www.oag.state.ny.us/press/2002/aug/aug01a_02.html
http://www.oag.state.ny.us/press/2002/aug/aug01a_02.html
Goner virus http://tinyurl.com/xnq

***

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.