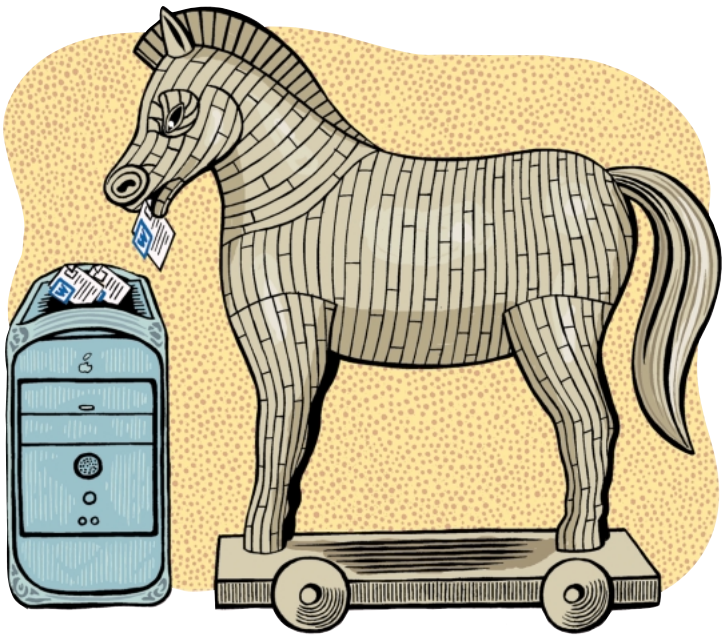

MICHAEL KUPPERMAN

For Love of Money

Malicious hacking takes an ominous turn

A well-known Israeli mystery writer, Amnon Jackont, found himself embroiled in a plot that could have come straight out of one of his novels. One day last year, he and his wife, Varda Raziel-Jackont, stumbled across a Web site that reprinted chapters from their cowritten—and not yet published—book. Until that moment, they thought that the book existed only as a file on their personal computer.

The thief? An estranged member of the family [see photo, "Culprit"]. With the police, the Jackonts figured out that the ex-husband of Raziel-Jackont's daughter had cracked their computer by e-mailing them a school registration form for their granddaughter with malicious software embedded.

The attack, of a kind known in software circles as a targeted Trojan horse, turned out to be the clue to a much bigger crime. When the local police got to the server where the culprit was thought to be storing the purloined novel, says Jackont, "they found a lot of people's stuff."

It emerged that the Jackonts' former son-in-law, Michael Haephrati, had made a business of selling his spy software and services to corporate leaders, who harvested competitors' secrets from destops. In due course, nearly 20 people—including executives at two cellphone companies, a major satellite television provider, and a Honda importer—found themselves in handcuffs and in Israeli tabloid headlines. Their victims included an Israeli telecommunications giant and a Volkswagen importer.

"To me," comments a programmer working in Israel's aerospace industry, "it was amazing how many legitimate firms bought into this action. Maybe I'm just naive."

The Trojan horse attack, in which an e-mailed attachment—like the Trojan horse of Greek myth—looks innocuous but conceals a dangerous cargo, has been an all-too-familiar part of the computer landscape for decades. In recent years,

CULPRIT: Michael Haephrati, an Israeli software specialist, developed a way of infiltrating computer systems. Seen here with his present wife, he was caught after using his methods to steal material from his former in-laws' computer.

however, a new and ever more prominent feature in that landscape has been the targeted Trojan, in which the e-mail subject line or message contains language calculated to lure a particular recipient into opening the attachment. Increasingly, targeted Trojan horses are being used to steal proprietary information, obtain intelligence to get an edge on rivals, and even, it seems, obtain access to sensitive military data.

The U.S. Department of Energy—keeper of the nation's nuclear secrets, among other responsibilities—revealed in July that it received several eerily personalized messages this summer. One e-mail, sent to a small group of DOE employees, appeared to come from a colleague and began with the convincing line, "In regards to today's meeting at 3 pm, I have attached a preliminary file for your reading." The attached file hid software that, if launched, would have allowed information to be extracted from the computer by remote control. (The DOE declined to answer questions about whether the targeted Trojan horses compromised any data.)

Customized Trojan-bearing e-mails likewise struck critical government and commercial offices in the United Kingdom and Canada. In a security briefing in June, the British government described this type of attack as an ongoing threat to national infrastructure. The Canadian and U.S. governments issued similar warnings.

No one knows exactly how often targeted Trojans strike, but they clearly represent a new twist in the way "malware" (malicious software) is distributed, says Johannes Ullrich of the SANS Internet Storm Center, a private organization in Bethesda, Md., that tracks security threats. Trojan horse software made up a third of the top malware complaints to Symantec Corp., a leading security company in

HAARETZ DAILY/AP PHOTO

"To me it was amazing how many LEGITIMATE FIRMS bought into this action. Maybe I'm just naive"—Israeli programmer

Cupertino, Calif., in the second half of 2004—double the proportion in the second half of 2003.

EARLY COMPUTER ATTACKS, such as the widespread Melissa virus of 1998, incapacitated computers or clogged mail servers with very heavy traffic. Such ploys inconvenienced victims but didn't enrich culprits. Now attackers increasingly go after valuable confidential information, whether credit card numbers or government documents. They're "hacking for fortune," as Symantec's Oliver Friedrichs puts it. Mystery writers like Jackont might prefer to say that the culprits have the classic motive—money. They also have means and opportunity.

The ubiquitous Windows PC, with its history of security problems, presents an enticing target. "A couple of years ago, or even last year, most of the attacks were basically targeting Web servers," says Ullrich. But as software companies and system administrators create better firewalls for servers, attackers are moving on to smaller but more vulnerable prey. Because many antivirus programs recognize only threats that security experts have already seen and defined, unique Trojans go undetected as they enter a system.

Once a Trojan has duped a user into allowing it onto a desktop, a well-configured firewall may later notice the Trojan intruder when it communicates with the outside world through unusual ports or addresses. But if a clever Trojan sends confidential information over the same port used for Internet access, no firewall can tell the difference between normal Web-surfing and nefarious activity.

The insidious Trojan attack is no longer a work of black art. When Trojan horses first appeared in the early 1970s, only programmers knew how to craft them. Now, however, crooks can just point and click to alter basic designs, thwarting antivirus software. They can add hidden instructions—"Get me passwords and anything called 'Top Secret'"—to ordinary files, be they Microsoft Word documents or PDFs. Crooks can even create Trojans that, by taking advantage of security flaws in Web browsers, install themselves automatically when a victim visits a deceptive Web site.

"So, should Company A decide that it doesn't have any scruples and wants to get something inside Company B," says Mark Sunner, chief technology officer of MessageLabs Ltd., an e-mail security company in Gloucester, England, "the tool kits...are now available to accomplish what three or four years ago would have been a very complex technical thing to pull off."

TO DETECT A TROJAN intruder lurking on a hard drive, it helps to make sure that firewalls are optimally configured, even if they can't be counted on to catch every targeted attack. Under development, says Symantec's Friedrichs, are methods of identifying Trojans by tell-tale file modifications and other suspicious behavior. A common clue for users is a computer's suddenly performing ordinary tasks much more slowly than normal.

To stop a Trojan from breaking and entering in the first place, companies have recourse to proxy servers. They essentially download files for a test run before passing them on to a user's desktop, scanning each attachment for potentially malicious software.

Yet truly avoiding infection, says Ullrich, "really comes down almost exclusively to user education." Users should regularly install software update patches offered by software suppliers to minimize the flaws that Trojan horses and other threats sometimes take advantage of. Of course, it also helps to avoid keeping valuable information on Internet-connected machines. Most important, they should steer clear of unsolicited attachments, links, and even disks and CDs.

Ordinary computer users may not enjoy greeting every e-mail with skepticism. Pain, regrettably, often proves to be the most effective teacher. Not long after the Jackonts' novel appeared prematurely on the Internet, their former son-in-law mailed Amnon a disk that supposedly came from a student in Jackont's writing class. "This disk, I never put in my computer," Jackont says. "I gave it to the police." **—LAUREN AARONSON**