A few weeks ago I watched the entire six-movie Star Wars series. I wish that malware writers could be turned away from the Dark Side, but I don’t see anything likely to achieve even the terminal redemption that Anikin Skywalker experience just before he dies. It’s a pity, because we have to admit that malware is getting smarter. Here are some developments from 2005.

In June, the Department of Homeland Security (DHS) Daily Report had this interesting summary of a New Scientist report: "An emerging breed of computer virus that keeps hackers informed about the latest weaknesses in computer networks has been discovered by security experts. The viruses infect a computer network, scan for security vulnerabilities and then report back to hackers through an Internet chatroom. Armies of computers infected with 'bot' viruses are routinely controlled via a chatroom connection and are used to knock for denial of service attacks or as a conduit for sending out spam e-mail. However, the ability of some bots to scan their hosts for unpatched security holes and report their findings back to hackers has gone largely unnoticed until now. The emerging class of malware or malicious software -- known as vulnerability assessment worms -- 'phone home' to allow hackers to fine-tune further attacks or perhaps even target an individual PC within a network. This pernicious form of program is just one of a growing number of new viruses identified each month, says computer security expert Bruce Schneier. 'The virus trend doesn’t look good,' Schneier writes in the June 2005 edition of the Association for Computing Machinery journal, Queue." <http://www.newscientist.com/article.ns?id=dn7500>

Worms have been using social engineering techniques to trick naive users into opening messages or attachments; however, a report in January provided depressing evidence of yet more imagination on the part of malware
writers. Someone created the W32/Crow-A worm which collects "subject lines, message content and attachment names from headlines gathered in real-time from the CNN Website.... [Its] subject line and attachments share the same name, but continually change to mirror the front-page headline on the CNN news site...." (from the DSH Daily Report). The worm installs a keylogger function that sends collected information to remote sites. < http://tinyurl.com/byeoy >

The Kelvir.HI instant messaging (IM) worm checks the configuration of infected Windows systems and adapts its social-engineering message ("haha I found your picture!") to the configured language -- any of Dutch, English, French, German, Greek, Portuguese, Spanish, Swedish, or Turkish. The worm installs the W32.Spyboot program. < http://tinyurl.com/alev7 >

The IM.Myspace04.AIM worm actually converses with users in an ELIZA-like way (see < http://en.wikipedia.org/wiki/Eliza > if you are not familiar with the computer program ELIZA). The AOL Instant Messenger (AIM) worm sends an instant message: "lil thats cool" and points to a vector for a malware file called clarissa17.pif. Apparently the worm responds to user queries by incorporating elements of their question into its answer much as the ELIZA program did. Because it has no artificial intelligence engine but merely a parser, it does make stupid responses, though. The DHS Daily reported that when users sent a query asking if the attachment contained a virus, the worm responded, "lol no its not its a virus." Still, its a disturbing development that someone will undoubtedly use as a proof of concept and then elaborate upon. < http://tinyurl.com/c87vr >

Copyright (c) 2006 M. E. Kabay. All rights reserved.