A logic bomb is a program which has deliberately been written or modified to produce results when certain conditions are met that are unexpected and unauthorized by legitimate users or owners of the software. Logic bombs may be within standalone programs or they may be part of worms (programs that hide their existence and spread copies of themselves within a computer systems and through networks) or viruses (programs or code segments which hide within other programs and spread copies of themselves).

An example of a logic bomb is any program which mysteriously stops working three months after, say, its programmer's name has disappeared from the corporate salary database.

In 1985, a disgruntled computer security officer at an insurance brokerage firm in Texas set up a complex series of Job Control Language (JCL) and RPG (an old programming language) programs described later as “trip wires and time bombs.” For example, a routine data retrieval function was modified to cause the IBM System/38 midrange computer to power down. Another routine was programmed to erase random sections of main memory, change its own name, and reset itself to execute a month later.

In 1992, a computer programmer was fined $5,000 for leaving a logic bomb at General Dynamics. His intention was to return after his program had erased critical data and get paid lots of money to fix the problem.

**Time bombs**

Time bombs are a subclass of logic bombs which “explode” at a certain time. Some of the first viruses, written in the 1980s, were time bombs. For example, the infamous Friday the 13th virus was a time bomb: it duplicated itself every Friday and on the 13th of the month, causing system slowdown. In addition, on every Friday the 13th, it also corrupted all available disks. The Michelangelo virus from the early 1990s – one of the first viruses to make it into public consciousness because of news coverage -- tried to damage hard disk directories on the 6th of March. The Win32.Kriz.3862 virus, discovered in 1999, detonates on Christmas day; its payload includes massive overwriting of data on all data storage units and also damage to the BIOS.

In 2000, a Stamford, CT, was indicted in NY State Supreme Court in Manhattan on charges of unauthorized modifications to a computer system and grand larceny. The defendant worked for Deutsche Morgan Grenfell Inc. from 1996 as a programmer. By the end of 1996, he became a securities trader. The indictment charged that he inserted a programmatic time bomb into a risk model on which he worked as a programmer; the trigger date was July 2000. The unauthorized code was discovered by other programmers, who apparently had to spend months repairing the program because of the unauthorized changes the defendant allegedly inserted.

**Arbitrary Code**

Logic bombs can be installed on a victim’s system from outside, too. Many buffer overflows allow what the alert agencies (e.g., CERT/CC) call “execution of arbitrary code.” It is possible
for malicious code (e.g., ActiveX, Java, and even HTML) to cause external code to be downloaded to a victimized machine; at that point, anything can happen. Malicious programs can not only take immediate action (e.g., sending spam with forged headers) but also lie quiescent until specific conditions are met; i.e., they can be logic bombs.

* * *

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.